UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

Implantación del Reglamento General de Protección de Datos y adaptación al Esquema Nacional de Seguridad de manera integrada en el Sistema de Gestión de Seguridad de la información basado en la ISO 27001.

Pablo Jiménez Gómez

Tutor: Carlos Hernández Franco

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2018-19

Valencia, 16 de agosto de 2019

Escuela Técnica Superior de Ingeniería de Telecomunicación
Universitat Politècnica de València
Edificio 4D. Camino de Vera, s/n, 46022 Valencia
Tel. +34 96 387 71 90, ext. 77190
www.etsit.upv.es

VLC/ CAMPUS
VALENCIA, INTERNATIONAL CAMPUS OF EXCELLENCE

EMAS
Gestión ambiental verificada
REG.NO. ES-CV- 000030

Agradecimientos

A mi familia por darme el apoyo y el cariño necesarios para superar todos los momentos difíciles que surgen en el camino. A mis compañeros de clase, en especial a César, por unos años inolvidables, en los cuales nunca faltó el compañerismo y el apoyo mutuo. A Andrea por tener la paciencia necesaria para aguantarme y darme ánimo en los peores momentos, haciendo siempre más fácil llevar la presión del día a día. A mis compañeros de prácticas de empresa por acogerme como a uno más desde el primer día y enseñarme todo lo que ha estado en su mano para empezar a sumergirme en el mundo laboral.
Y a la Universidad Politécnica de Valencia y su profesorado, por haber puesto en disposición todo lo necesario para ensalzar el desarrollo tanto profesional como personal.

Resumen

El uso generalizado de las TIC ha llevado a múltiples empresas a experimentar una adaptación constante a ellas, siendo así capaces de ofrecer sus servicios mediante tecnología accesible por el ciudadano. Tan pronto se han modernizado estos servicios, han surgido problemas relativos a la "seguridad de la información" que manejan, ocasionando graves pérdidas y sanciones críticas para la continuidad del negocio.

El presente trabajo tiene como finalidad mitigar los riesgos que afectan a la seguridad del "Sistema de Gestión de Seguridad de la Información" (SGSI) de una empresa que ofrece un servicio de transporte público y la gestión de forma telemática de bonos de transporte. Para ello, se realizará un análisis de riesgo cualitativo de su SGSI basado en la "metodología Magerit", analizando el estado actual de la organización para, poder así, identificar los activos que la sustentan y las amenazas por las que se ven afectados, continuando con una medición de los riesgos potenciales que afectan al sistema. Una vez esclarecida la situación de la organización, se procederá a la gestión de dichos riesgos elaborando un plan que sirva, tanto para implantar el nuevo "Reglamento General de Protección de Datos" que comenzó a ser de aplicación el 25 de mayo de 2018, como para adecuar a la empresa al "Esquema Nacional de Seguridad", basando todo ello en la norma "ISO 27001" para la gestión de la "seguridad de la información". Como soporte al análisis de riesgos, se hará uso de la herramienta proporcionada por el "Centro Criptológico Nacional (CCN)", PILAR, destinada al "análisis y la gestión de riesgos de un sistema de información" bajo la "metodología Magerit".

Resum

L'ús generalitzat de les TIC ha portat a múltiples empreses a experimentar una adaptació constant a elles, sent així capaços d'oferir els seus serveis mitjançant tecnologia accessible pel ciutadà. Tan aviat s'han modernitzat aquests serveis, han sorgit problemes relatius a la seguretat de la informació que manegen, ocasionant greus pèrdues i sancions crítiques per a la continuïtat del negoci.

El present treball té com a finalitat mitigar els riscos que afecten la seguretat del "Sistema de Gestió de Seguretat de la Informació (SGSI)" d'una empresa que ofereix un servei de transport públic i la gestió de forma telemàtica de bons de transport. Per a això, es realitzarà una anàlisi de risc qualitatiu del seu SGSI basat en la metodologia MAGERIT, analitzant l'estat actual de l'organització per, poder així, identificar els actius que la sustenten i les amenaces per les quals es veuen afectats, continuant amb una mesurament dels riscos potencials que afecten el sistema. Un cop aclarida la situació de l'organització, es procedirà a la gestió d'aquests riscos elaborant un pla que serveixi, tant per implantar el nou "Reglament General de Protecció de Dades" que va començar a ser d'aplicació el 25 de maig de 2018, com per adequar a l'empresa a "l'Esquema Nacional de Seguretat", basant tot això en la norma "ISO 27001" per a la gestió de la seguretat de la informació. Com a suport a l'anàlisi de riscos, es farà ús de l'eina proporcionada pel Centre Criptològic Nacional (CCN), PILAR, destinada a l'anàlisi i la gestió de riscos d'un sistema d'informació sota la "metodologia MAGERIT".

Abstract

The widespread use of ICT has led multiple companies to experience constant adaptation to them, thus being able to offer their services through technology accessible by the citizen. As soon as these services have been modernized, problems related to the security of the information they handle have arisen, causing serious losses and critical sanctions for business continuity. The purpose of this paper is to mitigate the risks that affect the security of the Information Security Management System (ISMS) of a company that offers a public transport service and the management of transport vouchers electronically. For this, a qualitative risk analysis of its ISMS will be carried out based on the "MAGERIT methodology", analyzing the current state of the organization in order to be able to identify the assets that sustain it and the threats for which they are affected, continuing with a measurement of the potential risks that affect the system. Once the situation of the organization has been clarified, the risks will be managed by preparing a plan that will serve both to implement the new "General Data Protection Regulation" that began to be applicable on May 25, 2018, and to adapt the company to the "National Security Scheme", basing all this on the "ISO 27001" standard for the management of information security. As a support to the risk analysis, the tool provided by the National Cryptological Center (CCN), PILAR, will be used for the analysis and risk management of an information system under the "MAGERIT methodology".

Índice

Capítulo 1. Introducción

1.1 Introducción al "Reglamento General de Protección de Datos"

El continuo desarrollo tecnológico ha traído una serie de cambios relevantes en la manera en la que se desenvuelven las sociedades. El uso de éstas en el día a día es una realidad para los ciudadanos, que cada vez disponen de más medios telemáticos a su disposición destinados a le gestión de todo tipo de trámites. De esta forma, la cantidad de información y datos personales prestados a diferentes tratamientos es cada vez mayor, por lo que nace la necesidad de proteger dicha información en favor del ciudadano. La aparición de la "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)", surge del incremento de vulnerabilidad que supone el constante desarrollo de las tecnologías de la información. Dicha Ley Orgánica tiene por objeto, según el Boletín Oficial del Estado, "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". [1]

Actualmente, la LOPD ha sido reemplazada por la vigente "Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que adapta la legislación española al Reglamento General de Protección de Datos de la Unión Europea (RGPD), de aplicación desde el 25 de mayo de 2018".

Al tratarse de una normativa a nivel de Unión Europea, cualquier empresa, que trate con información personal de cualquier ámbito, tiene la obligación de acogerse a ésta.

La introducción del RGPD en la Unión Europea también supone para el ciudadano un nuevo conjunto de derechos digitales a los que acogerse. El creciente aumento del valor de los datos personales a nivel económico tiene como efecto dotar de aún más importancia a los nombrados derechos digitales.

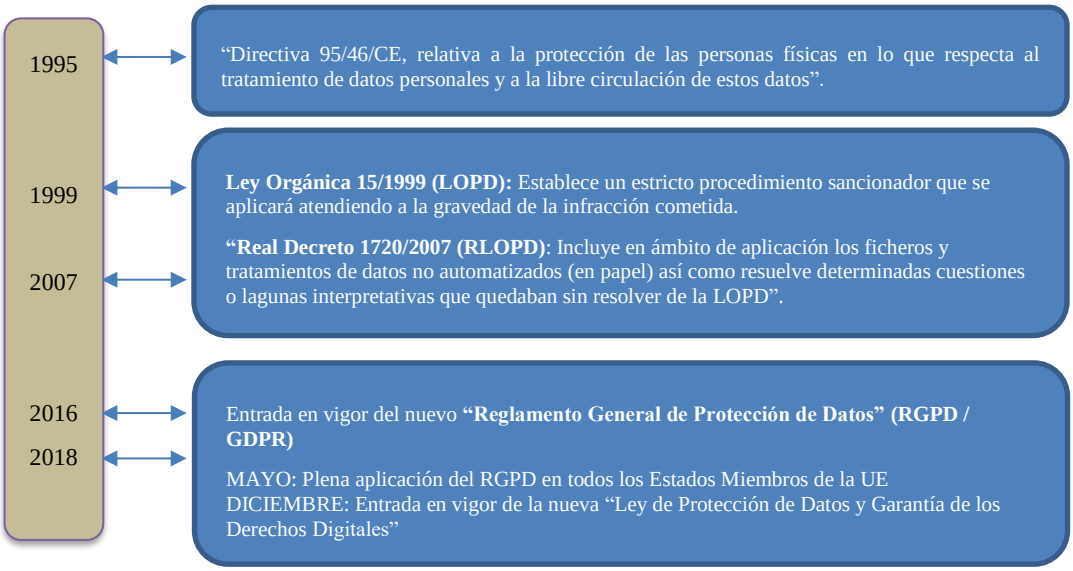


Figura 1. Cronología RGPD.

1.2 Introducción al "Esquema Nacional de Seguridad"

El "Esquema Nacional de Seguridad (Real Decreto 3/2010, de 29 de enero)", en adelante ENS, surge como una necesidad para garantizar la seguridad entre información y tecnologías públicas:

"El ENS desarrolla el artículo 42.2 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, con unas finalidades comunes frente a la utilización de los medios electrónicos de los ciudadanos en sus relaciones con las Administraciones Públicas": [2]

- "*Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos*".
- "*Aportar confianza la hora de utilizar soportes electrónicos, implantando las medidas oportunas para garantizar la integridad de los derechos, con especial hincapié en los relacionados con datos personales*".
- Establecer cercanía al ciudadano con las Administraciones Públicas y tratar de agilizar procedimientos y hacerlos de forma más eficiente.
- Cumplir con las garantís legales mínimas exigidas.
- "*Aportar nuevos mecanismos para el crecimiento de la sociedad de la información*".

El ENS tiene como finalidad principal garantizar y crear las condiciones necesarias de confianza en el uso de los medios electrónicos en las relaciones con la Administración, estableciendo las medidas y requisitos de seguridad que aseguren "una adecuada protección de la información en términos de confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad".

1.3 Introducción al estándar ISO/IEC 27001

"ISO 27001" es un estándar de ámbito internacional preparado con el objetivo de fortalecer un "sistema de gestión de la información" en todas sus dimensiones. Fue aprobado y publicado como estándar internacional en octubre de 2005 por "International Organization for Standardization" y por la comisión "International Electrotechnical Commission".

La normativa "ISO 27001" define un "sistema de gestión de la información" (SGSI) como "el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar de una forma eficiente la accesibilidad de la información. Tiene como objetivo garantizar la accesibilidad a la información, cumpliendo con los principios de confidencialidad, integridad y disponibilidad, minimizando los riesgos de seguridad de la información". [3]

En su anexo A, estándar ISO/IEC 27002, se contempla una lista con los objetivos y controles definidos como guía de buenas prácticas recomendables en cuanto a "seguridad de la información".

La versión de la ISO 27002:2013 establece catorce dominios principales y dentro de cada uno de ellos se especifican los objetivos a obtener para la "seguridad de la información".

Las organizaciones que implanten los controles de la normativa pueden certificar su SGSI a través de una entidad certificadora externa. Mediante una auditoria de los sistemas se determina el grado de conformidad con la ISO/IEC 27001 y, en caso de una correcta implantación, se emite el correspondiente certificado. [4]

1.4 Contexto normativo

1.4.1 Principios básicos RGPD

El alcance de la regulación aplica a cualquier organización que obtenga datos de personas residentes en la Unión Europea. La alta dirección debe garantizar que la organización tome las medidas adecuadas para cumplir con todas las leyes y regulaciones aplicables, de modo que los riesgos para la organización se administren de manera efectiva. El "Reglamento General de Protección de Datos" (RGPD), con sus requisitos específicos relacionados con la protección de datos personales de ciudadanos y residentes europeos y las sanciones administrativas importantes, lo convierte en una prioridad para la alta dirección de las organizaciones.

La entrada en vigor del nuevo reglamento establece, además de los anteriores derechos ARCO ("Acceso, Rectificación, Cancelación y Oposición"), dos nuevos derechos, el derecho a la "***portabilidad de los datos***" y el "***derecho al olvido***". Así los derechos del interesado serían [5]:

"Información: derecho a obtener información sobre cómo se van a tratar/están tratando nuestros datos personales".

"Acceso: derecho a obtener confirmación de si tus datos personales se están tratando y acceder a dichos datos".

"Rectificación: derecho a rectificar los datos personales incorrectos o incompletos".

"Supresión (olvido): derecho a pedir a los responsables del tratamiento que borren todos los datos personales sin demora indebida en determinadas circunstancias".

"Toma de decisiones automatizadas: derecho a la oposición de la toma de decisiones automatizadas que nos afecten, incluida la elaboración de perfiles".

"Limitación del tratamiento: derecho a limitar el tratamiento de tus datos personales".

"Portabilidad: derecho a obtener una copia de tus datos personales para tu uso interno o para transferirlos a una tercera compañía".

"Oposición: derecho a oponerse al tratamiento de tus datos personales en determinadas circunstancias".

Además, el RGPD introduce tres principios a los que las organizaciones deben acogerse:

- **"Principio de responsabilidad"**. Toda organización tiene el deber de demostrar el cumplimiento de la normativa vigente y las exigencias que conlleva, mediante el desarrollo de políticas, controles y procedimientos [6].

- **"Principios de protección de datos por defecto y desde el diseño"**. Se deben aplicar medidas que garanticen el cumplimiento de la norma en todo proceso que implique tratamiento de datos personales [7].

- **"Principio de transparencia"**. Se pretende facilitar la comprensión de políticas y avisos legales, haciéndolos más inteligibles [8].

Del mismo modo, nacen nuevas obligaciones para empresas y administraciones. Entre ellas, se destacan las siguientes [9]:

- **"Designación de un Delegado de Protección de Datos (DPO)"**, interno o externo, capaz de ayudar en las tareas propias de la nueva normativa.
- **"Plazo máximo de 72 horas en el informe de brechas de seguridad"**, tanto a las autoridades como a afectados, en casos de gravedad crítica. En España, la autoridad de control es la "Agencia Española de Protección de Datos (AEPD)".
- **"Protección de datos sensibles"**: se amplían los datos considerados de sensibilidad, incluyendo datos de carácter genético y biométrico.
- **"Selección de encargado de tratamiento de datos personales"** que garantice el cumplimiento de la normativa.
- **"Sellos y certificaciones"** de cumplimiento para reforzar el principio de responsabilidad.
- **"Sanciones"**: Aumento cuantitativo en las sanciones derivadas del incumplimiento de la norma, alcanzando los "20 millones de euros o el 4% de la facturación global anual".

De forma más específica, el nuevo "Reglamento General de Protección de Datos" ejercerá mayor impacto en cuatro bloques diferenciados dentro de cada organización.

El primero de ellos será el aspecto **legal,** de modo que, según la interpretación y aplicación de la legislación aplicable, serán necesarias medidas tales como:

- Revisión y actualización de la política de privacidad y clausulas (entorno webs).
- Revisión y actualización de cláusulas en formularios de obtención de datos.
- Revisión y actualización de contratos (p.e. empleados, proveedores).

En lo relativo al **modelo de negocio,** se evaluará el impacto en el negocio**:**

- Identificación y análisis de los flujos de datos que dan soporte a los procesos de negocio.
- Análisis y validación de los consentimientos obtenidos sobre los datos existentes.
- Definición de los plazos de conservación de los datos (abonados potenciales, abonados dados de baja…).

En cuanto a **tecnología**, se seleccionarán los mecanismos adecuados:

- Validar que los mecanismos implementados minimizan adecuadamente los riesgos potenciales.
- Evaluar aquellas tecnologías utilizadas y consideradas muy intrusivas sobre la privacidad (biometría).
- Evaluar entornos o soluciones en cloud.

Además, en lo que se refiere a **organización**, se deberá implementar una cultura de cumplimiento:

- Designar figura de "Delegado de Protección de Datos" (DPO).
- Identificar figuras equivalentes en aquellos proveedores que traten datos en nombre de la compañía.
- Procedimentar la privacidad desde el diseño y por defecto.

- El RGPD se compone de 10 capítulos, divididos cada uno de ellos en artículos, sumando un total de 99 [10].

LOPD	RGPD
1. Consentimiento entendido como "manifestación de voluntad".	1. Consentimiento entendido como "clara acción afirmativa".
2. Ficheros inscritos.	2. "Registro de actividades de tratamiento de datos".
3. Documento de seguridad y auditoría biaunal.	3. Principio de responsabilidad activa y transparencia.
4. Reglamento de medidas de seguridad básicas, medias y altas.	4. Evaluación de Impacto (EIPD) y seguridad desde el diseño.
5. Derechos ARCO.	5. Nuevos derechos (olivdo, portabilidad y perfilado).
6. Sanciones de hasta 600.000 € (muy graves).	6. Sanciones de hasta el 4% del volumen de negocio.
7. Responsable de Seguridad.	7. "Delegado de Protección de Datos" (DPD).
8. Obligación de registrar internamente las incidencias con afectación a datos personales.	8. Obligación de notificar ocurrencia de brechas de seguridad.
9. Obligaciones del responsable de tratamiento.	9. Obligaciones de los encargados de tratamiento.
10. Período de almacenamiento de datos personales ilimitado.	10. Política de conservación de datos personales.

Tabla 2. Novedades RGPD.

La completa aplicación del reglamento requiere de una plantilla de profesionales especializados en diferentes áreas, tales como legal, financiera e informática. De cara al presente trabajo, el capítulo sobre el que adaptaremos las medidas necesarias en la compañía será el cuarto; "responsable del tratamiento y encargado del tratamiento", sección segunda; "Seguridad de los datos personales; Artículo 32, Seguridad del tratamiento".

El artículo 32 indica "las medidas técnicas y organizativas que responsable y el encargado del tratamiento aplicarán para garantizar un nivel de seguridad adecuado al riesgo", incluyendo de esta forma [11]:

a) "La seudonimización y el cifrado de datos personales".

b) “La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia 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”.

1.4.2 Principios básicos “Esquema Nacional de Seguridad”.

El cumplimiento con el ENS se añade a otras normas de aplicación en la Administración relativas a “seguridad de la información”, como son la LOPD, RGPD, “ISO 27001” /27002 u otras.

Así mismo, se propone la evaluación de estos controles de acuerdo con un modelo de madurez en líneas con las mejores prácticas del mercado, por ejemplo, “CMMI (Capability Maturity Model Integration) modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software”.

El ENS dispone de los siguientes principios y elementos básicos para conseguir aumentar la seguridad y la confianza en el uso de dispositivos electrónicos [12]:

- Política de Seguridad: Compromiso de la más alta dirección mediante documento de alto nivel que define lo que significa “Seguridad de la Información” en una organización.
- Funciones y Responsabilidades: Asignar funciones y responsabilidades en materia de “Seguridad de la Información”, como son:
    - Responsable de la Información. Determina los requisitos de la información tratada, persona de Gobierno.
    - Responsable del Servicio/Sistema. Responsable del ciclo de vida del sistema que determina los requisitos del sistema de información.
    - Comité de Seguridad / Responsable de Seguridad / Técnico / Organizativo / Legal. Define un rol de supervisor, para la regulación de las medidas establecidas.
- Proceso de Gestión de la Seguridad (SGSI): Similar a lo dispuesto en la “ISO 27001”, desplegar un proceso integral de seguridad basado en un ciclo continuo Plan-Do-Check-Act.
- Gestión de Riesgos: Gestionar la seguridad y las medidas que se aplican en base a sus riesgos, aplicando el principio de proporcionalidad.
- Medidas/controles de seguridad en función de la clasificación de la información: A partir de la clasificación de la información que se tratan en las diferentes relaciones con la administración, se seleccionarán unas medidas de seguridad u otras.
- Reevaluación periódica de la seguridad: Realización de revisiones (autoevaluaciones) y auditorías cada dos años por una parte independiente.
- Plan de Adecuación al ENS. Aún transcurridos el plazo previsto de 12 meses, es necesario redactar por el Responsable de Seguridad y aprobar el Plan de Adecuación.

El ENS establece 5 dimensiones en la clasificación de la información: Confidencialidad, Integridad, Autenticidad, Trazabilidad y Disponibilidad. Y sus correspondientes niveles ALTO, MEDIO y BAJO. Así como la elección de controles/medidas de seguridad de acuerdo a la clasificación (valoración) de la información que se trata en las relaciones con las administraciones [13].

1.4.3 Principios básicos ISO/IEC 27001

En base a los requerimientos y preocupaciones que se deben cubrir con esta prestación de servicios de carácter informático**, se propone el marco de seguridad que ofrece la serie internacionalmente reconocida ISO 27000**. Se considera que este marco de trabajo **permitirá cubrir más que todos los aspectos requeridos, proporcionando una visión completa de la seguridad.**

En concreto, la ISO 27002 supone el código de buenas prácticas para garantizar los pilares básicos de:

Confidencialidad. La información únicamente debe ser accesible por aquellos usuarios o empleados autorizados.

Integridad. Tiene en cuenta la precisión y completitud de la información y sus métodos de cálculo.

Disponibilidad. Por otra parte, el acceso a la información y los activos tecnológicos deben estar garantizados cuando éstos lo requieran.

Por otra parte, la ISO/IEC 27001:2013 "establece las especificaciones normativas para establecer, operar, mantener y mejorar un "Sistema de Gestión de Seguridad de la Información" (SGSI), y de esta manera permitir una gestión de la seguridad de manera más adecuada y eficiente. El "Sistema de Gestión de Seguridad", según "ISO 27001", proporciona mecanismos para dedicar recursos y esfuerzos a la seguridad de manera proporcional a la importancia de los riesgos identificados a la organización".

El SGSI está basado en un "Modelo de Mejora Continua, Model PDCA (Plan-Do-Check-Act), denominado ciclo de Deming, estando totalmente alineado con otros sistemas de gestión como ISO 9000 (calidad) e ISO 14000 (medioambiente)".

Figura 2. Modelo de Mejora Continua.

"ISO/IEC 27002 - Código de Buenas Prácticas" establece 35 objetivos de control y 114 controles agrupados en 14 dominios (5-18), los cuales proporcionan una visión completa de la seguridad, cubriendo así todos los requerimientos del diagnóstico. [14]

Figura 3. Dominios "ISO 27001" /27002:2013.

Capítulo 2. Objetivo de este documento

El cumplimiento del Reglamento General de Datos es de carácter obligatorio para cualquier empresa que ejerza su actividad económica dentro de la Unión Europea, es por ello que el objetivo principal es el asesoramiento y soporte para la adecuación e implantación del RGPD, de manera integrada en el "Sistema de Gestión de Seguridad de la Información" (SGSI) basado en la "ISO 27001".

La organización objeto del trabajo, resulta ser una empresa de ámbito público que ofrece al ciudadano un servicio telemático de gestión de bonos de transporte, por lo que está sujeta al ámbito de aplicación del "Esquema Nacional de Seguridad". El desarrollo del proyecto se fundamentará en la confección de un Marco de Convergencia Normativa, como catálogo único de controles, cuyo cumplimiento garantice alcanzar un grado de "seguridad de la información" adecuado. Se considera la forma más eficiente de alinear las diferentes normativas, buenas prácticas y legislaciones vigentes. Como consecuencia, se obtendrán los niveles de "seguridad de la información" requeridos para la compañía, optimizando tiempo, esfuerzo y dinero. Asimismo, se garantizará la completa adaptación de la compañía al "Reglamento General de Protección de Datos", al que será más sencillo adecuarse bajo las medidas de seguridad propuestas tanto por la "ISO 27001" como por el ENS.

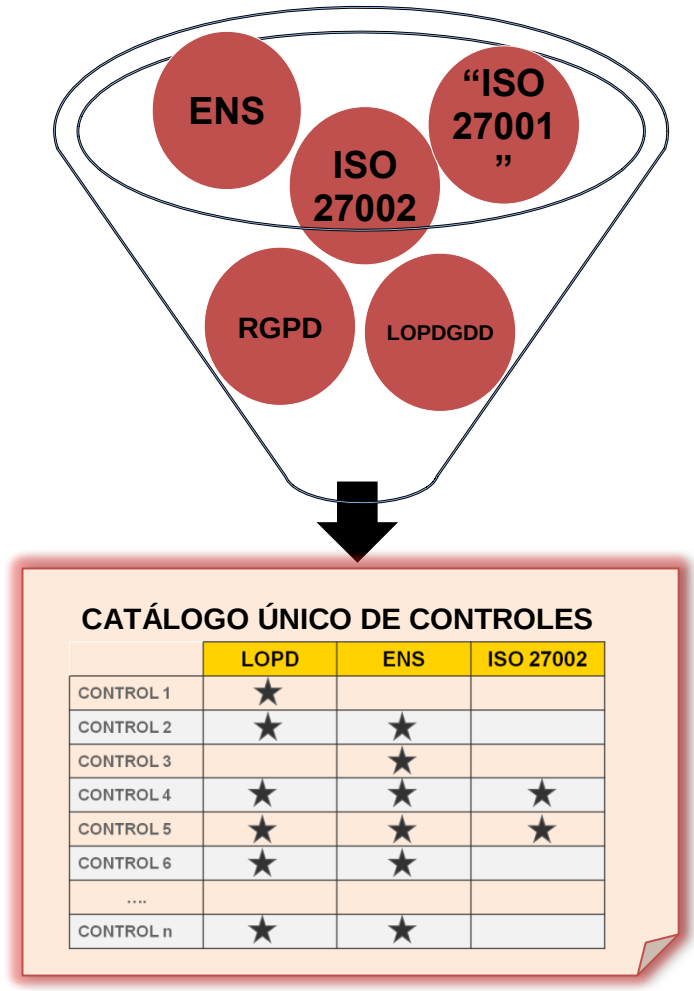


Figura 4. Convergencia Normativa.

2.1 Metodología seguida en el proyecto

Con el fin de poder mejorar los niveles de seguridad de la organización, se estructurará el trabajo en fases que deben cubrir la correcta prestación del servicio, las cuales se alinean con las 4 fases del ciclo Deming (Plan-Do-Check-Act), ciclo en el que se basa la operación de cualquier sistema de gestión y en concreto un SGSI, de tal manera que facilite la integración en el SGSI de la compañía.

En primer lugar, en la **planificación** del proyecto, se estudiará cada uno de los procesos de negocio de la organización y su relación con su "sistema de gestión de la información", averiguando, mediante entrevistas con cada uno de los responsables de cada departamento que constituye la empresa, el tipo de datos que se tratan y cómo se gestionan. De esta forma se identificarán los procesos de negocio que se encuentren bajo el alcance del "Esquema Nacional de Seguridad". Una vez identificados los sistemas a los que se aplica el ENS, el siguiente paso será categorizarlos atendiendo a la **valoración de la información** que se maneja y de los servicios que se prestan.

Una vez realizado el estudio de los procesos de negocio de los que hace uso la empresa y su relación con el tratamiento de datos personales, la herramienta PILAR, proporcionada por el "Centro Criptológico Nacional", será de ayuda para realizar un **análisis de riesgo** en primera estancia sobre el estado actual de los niveles de "seguridad de la información" de la organización.

PILAR realiza un análisis de riesgos basado en la "metodología Magerit", consistente en garantizar las cinco dimensiones de seguridad que propone; confidencialidad, integridad, autenticidad, disponibilidad y trazabilidad. La herramienta es capaz de analizar los niveles de seguridad de la empresa en base a los activos que componen los procesos principales de la compañía.

De este modo, se propondrá un plan de gestión de riesgos que ayude a la organización a mejorar sus niveles de seguridad, asesorando a la compañía en la **implantación de las medidas** oportunas.

Como última fase del proyecto, se propone el asesoramiento para el **soporte y el mantenimiento** de las normativas aplicadas.

Figura 5. Fases planificación.

Capítulo 3. Desarrollo de las fases del proyecto

3.1 Plan inicial

El objetivo principal de esta fase es identificar y planificar los recursos necesarios para desarrollar el trabajo de la manera más eficaz y eficiente, con el fin de cumplir los objetivos del proyecto. Por otra parte, en esta fase también se identificarán los interlocutores adecuados para realizar el trabajo de campo.

3.1.1 Identificación inicial de los principales interlocutores

El primer paso del proyecto ha de ser conocer la estructura interna de la compañía que desea adecuar sus sistemas a las normativas propuestas. De este modo, se establecerán sesiones de entendimiento con los departamentos relacionados con el tratamiento de datos personales.

Este proceso va a servir para conocer al completo la operativa de la compañía y averiguar el tipo de datos personales que manejan y cómo hacen uso de ellos.

Como resultado, se obtienen los diferentes departamentos de la empresa y los responsables de cada uno de ellos:

Figura 6. Áreas y responsables.

Una vez identificados los responsables de tratamiento, el siguiente paso será la elaboración de entrevistas con cada uno de ellos para conocer las actividades de tratamiento de datos que manejan.

El cuestionario que se va a seguir en cada una de las entrevistas tiene un enfoque tanto de adecuación a RGPD como de seguridad en los medios electrónicos.

La información por destacar en un enfoque sobre el RGPD en las entrevistas es la siguiente:

1. Breve descripción del área o departamento en el que habitualmente desempeña sus funciones, así como aquellas aplicaciones donde se traten datos de carácter personal.
2. La ubicación física de los servidores que soportan las aplicaciones informáticas.
3. Existencia de proveedor externo que preste el servicio de soporte y/o mantenimiento cuando las aplicaciones y/o dispositivos sufren problemas técnicos.
4. Procedimientos para solventar problemas detectados en aplicaciones y/o dispositivos informáticos.
5. Terceros que tengan acceso a datos de carácter personal.
6. En el momento de la recogida de los datos personales, el tipo de información se proporciona a los afectados.
7. Existencia de datos especialmente protegidos en el área en cuestión (salud, religión, ideología, orientación sexual, etc.), o en su defecto datos relativos a menores. En caso de manejar este tipo de datos, procedimiento que detalle cómo la organización garantiza su protección, de conformidad con lo establecido en la normativa aplicable en materia de datos personales.
8. Medidas de las que la organización hace uso cuando se les proporcionan datos de carácter personal para cualquier servicio que preste al ciudadano.
9. Procedimientos de los que dispone la empresa para notificar a las autoridades de control y/o a los afectados, una violación de la seguridad de los datos personales.
10. Metodología que usa el departamento para que los datos personales tratados se mantengan actualizados (periódicamente), precisos, completos y limitados a las finalidades del tratamiento para las cuáles se han recabado.
11. El departamento trata datos personales con la finalidad de elaborar perfiles basados en actitudes sistemáticas o automatizadas. En caso afirmativo, medidas de las que se dispone para salvaguardar dichos datos.
12. Aplicación de medidas de seguridad (por ejemplo, nombres de usuario, contraseñas, pseudoanonimización, etc.) sobre los sistemas y/o aplicativos con los que habitualmente trabaja cada departamento. Así como la protección sobre los datos en papel.
13. Categorización del nivel de cumplimiento de las medidas de protección de datos de las que dispone la compañía en cada departamento.
14. Existencia de procedimiento en virtud del cual los interesados puedan ejercer sus derechos (“acceso, rectificación, cancelación, oposición,” etc.).
15. Ubicaciones de almacenamiento de datos personales y periodos de conservación de estos.

De forma análoga, se realiza un cuestionario de la ISO 27000 para conocer el estado de los sistemas de información, del que se concluyen los siguientes puntos:

1. Ubicaciones físicas de los servidores que soportan las aplicaciones informáticas.
2. Medidas de seguridad aplicadas para el acceso a los sistemas y/o aplicativos utilizados por la organización y política de contraseñas.
3. Medidas de protección sobre la información recabada en papel.
4. Evidencias de que la información confidencial solo es accesible por personal autorizado.
5. Existencia de una lista de los usuarios con accesos privilegiados.

6. Posibilidad de extraer listados de cambios técnicos aplicados sobre las aplicaciones de la organización.
7. Listado de las personas encargadas de:

I. Solicitar y autorizar el desarrollo de programas y/o los cambios a programas
II. Desarrollo de los cambios a programas
III. Paso del cambio al entorno de producción
IV. Monitorización del proceso de cambios

8. Procedimientos de seguridad llevados a cabo a la hora de implantar cambios (política de buenas prácticas).
9. Medidas para proteger la red y crear un entorno de comunicación seguro. (áreas DMZ, VPN, proxys, etc.).
10. Herramientas de control de dispositivos móviles.
11. Procedimientos para solventar deficiencias detectadas en el desempeño de funciones en medios electrónicos.

Por último, se realiza un cuestionario sobre el marco de control que establece el "Esquema Nacional de Seguridad", del que se extrae:

1. Medidas de seguridad utilizadas para acceder a los centros de procesamiento de datos (CPDs).
2. Medidas de seguridad implantadas en las infraestructuras (SAI, grupo electrógeno, suelo técnico, etc.).
3. Sincronización respecto a un mismo reloj.
4. Disposición de un "Plan de Continuidad de Negocio".
5. Políticas de seguridad definidas.
6. Inventario de activos de información.
7. Relación detallada de los servicios que se prestan en la organización con los responsables designados.
8. "Política de seguridad que defina los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información".
9. Categorización y clasificación de los sistemas de información.
10. Firmas electrónicas y certificados.

Tras las entrevistas con los responsables, la información obtenida queda recogida en el análisis GAP (*apartado 3.3*) y el resumen de la fase de planificación quedaría de la siguiente forma:

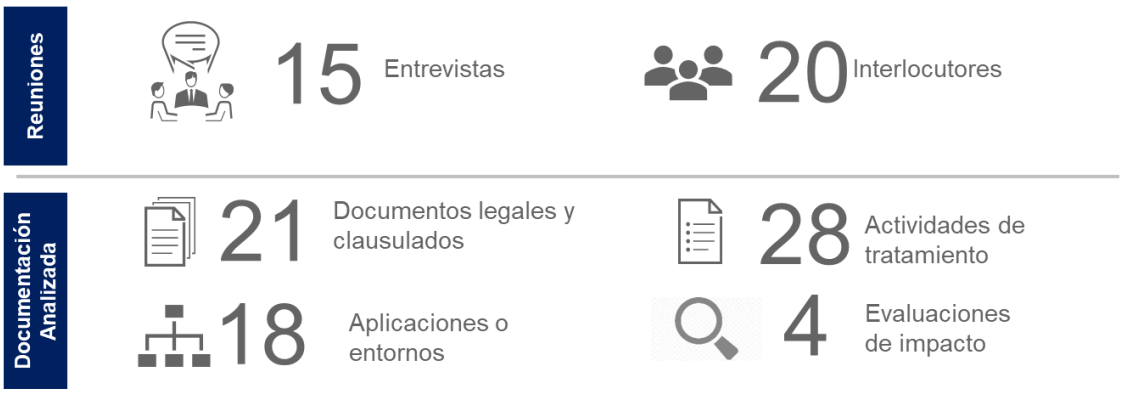


Figura 7. Resumen entrevistas.

3.2 Identificación de procesos y tratamientos de datos

Como resultado de las entrevistas de entendimiento mantenidas con los distintos departamentos de la empresa, se ha completado un inventario de procesos de negocio y tratamientos de datos propios de la compañía.

Se considera tratamiento de datos personales "toda operación o conjunto de operaciones realizadas sobre los datos personales, ya sea a través de procedimientos automatizados o no" [9]. Así, tras las entrevistas se elabora un Registro de Actividades de Tratamiento que pueda ser facilitado a las autoridades en el supuesto de que así lo requieran:

#	Nombre del tratamiento	#	Nombre del tratamiento
AT.01	Gestión de compras	**AT.15**	Seguimiento de la recaudación
AT.02	Facturación	**AT.16**	Vigilancia de la Salud y Prevención de Riesgos Laborales
AT.03	Gestión de cobros y devoluciones online	**AT.17**	Gerencia
AT.04	Gestión de la recaudación	**AT.18**	Organización del servicio
AT.05	Gestión de títulos personales	**AT.19**	Gestión de siniestros
AT.06	Registro de títulos no personales	**AT.20**	Líneas de trabajadores
AT.07	Estudio uso de tarjetas	**AT.21**	Gestión línea diversidad funcional
AT.08	Gestión de quejas y reclamaciones	**AT.22**	Gestión de servicios especiales
AT.09	Objetos perdidos	**AT.23**	Control de acceso
AT.10	Captación de personal	**AT.24**	Geolocalización de vehículos
AT.11	Período de prueba conductores	**AT.25**	Videovigilancia
AT.12	Gestión de pago de nóminas, adelantos y finiquitos	**AT.26**	Campañas publicitarias en RRSS
AT.13	Estudio de rendimiento de los trabajadores	**AT.27**	Uso de imágenes con fines publicitarios
AT.14	Gestión laboral de los empleados	**AT.28**	Contratación

Tabla 2. Actividades de tratamiento.

De forma análoga, para conocer los Sistemas de información aplicables al ENS, se procede a la identificación de los procesos de negocio de la compañía, clasificados según su afectación a las distintas normativas aplicables, así como las aplicaciones que intervienen en los mismos:

#	Procesos de Negocio	#	Procesos de Negocio
PN.01	Gestión de Proveedores	**PN.08**	Registro de entrada
PN.02	Gestión de cobro a clientes	**PN.09**	Gestión servicio autobuses
PN.03	Reporte de Cuenta de Resultados al Registro Mercantil	**PN.10**	Control de acceso a instalaciones
PN.04	Gestión de títulos	**PN.11**	Geolocalización de vehículos
PN.05	Atención a la ciudadanía	**PN.12**	Videovigilancia
PN.06	Gestión personal laboral	**PN.13**	Acciones publicitarias
PN.07	Proceso de servicio de prevención de riesgos laborales y vigilancia de la salud	**PN.14**	Contrataciones y licitaciones

Tabla 3. Procesos de negocio.

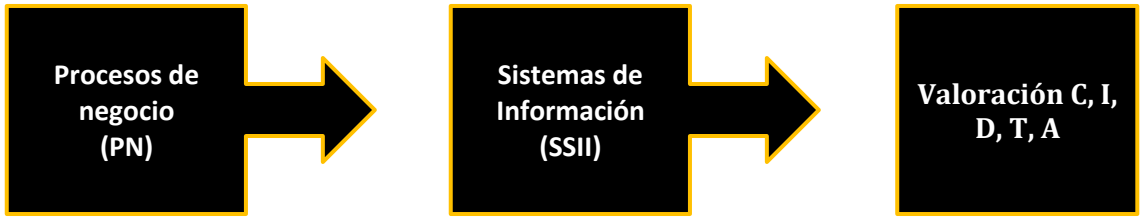
Por otra parte, se distinguen las aplicaciones sobre las que cada departamento realiza su labor. En las reuniones con cada responsable se detalla el nivel de seguridad establecido en cada una de ellas. También es necesario conocer si las aplicaciones son desarrolladas por la propia compañía o son una solución comercial gestionada por un tercero. Este aspecto es de especial relevancia, dado que supondrá que la gestión de accesos, cambios sobre la aplicación y copias de seguridad se gestione de una forma u otra.

Sistema de Información	Descripción	Sistema	Nivel de seguridad
PREVEN Riesgos	Gestiona datos de Salud de los Empleados	Base de Datos	
Ap. Nómina y Recursos Humanos	Gestión de empleados, Nómina, Seguros y Recursos humanos	BDD desarrollada por la compañía	
Ap. Operaciones	Gestión de empleados, Nómina, Seguros y Recursos humanos	BDD desarrollada por la compañía	
Ap. Equipamiento	Gestión de trabajos en el Área Técnica	BDD desarrollada por la compañía	
BBDD propietaria	Gestiona datos de clientes de la compañía	BDD desarrollada por la compañía	
Lotus Notes	Sistema de Comunicación y Base Documental	Comunicación personal	
Microsoft Office	Aplicaciones ofimáticas para la generación de documentos.	Suite Ofimática	
Advanced Tempo	Control Horario	Control Presencia	
Gestión Documental	Gestión Documental	Repositorio documental	
Cuadro de Mando	Cuadro de Mando y organización Empresa	Base de Datos	
SAE	Gestión de la flota de autobuses	Base de Datos	
Usuarios	Usuarios registrados	Base de Datos	
Pases	Gestión de pases	Base de Datos	
Ficha empleados	Consulta de datos de empleados	BBDD vía web	
Prisma 3	Gestión de almacén, proveedores y taller	Base de Datos	
Facebook	Usuario corporativo para información al cliente	Red Social externa	
Twitter	Usuario corporativo para información al cliente	Red Social externa	

Whatsapp	Usuario corporativo para atención al cliente	Red Social externa	
Telegram	Usuario corporativo para atención al cliente	Red Social externa	
EXPERT	ERP contabilidad	SaaS	
EPS	BBDD clientes	Base de Datos	
EPESI	Organización, procesado y almacenamiento de información	Base de Datos	
DataWarehouse	BBDD autobuses y conductores	Base de Datos	
CTI	Sistema de validación entre la cantidad de tickets vendidos y el importe recaudado de la caja del autobús contado por cajeros auto-liquidadores.	Base de Datos	
CCTV	Cámaras de videovigilancia. Circuito cerrado de televisión para supervisar diferentes actividades.	Base de Datos	

Tabla 4. Listado de aplicaciones.

Para conocer los sistemas de Información aplicables al ENS, primero se han identificado los procesos de negocio que corresponden con trámites ofrecidos a los ciudadanos por parte de la compañía.



Una vez identificados los Sistemas de Información bajo el alcance del ENS, se ha valorado su criticidad con respecto a los dominios de seguridad: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad.

Para ello, se ha calificado de "alto", "medio" o "bajo" la criticidad de estos dominios para cada caso, revisando los siguientes aspectos sobre cada uno de ellos:

	Bajo	Medio	Alto
· Según pérdidas económicas	< 2 M€	2 M€ < x < 5 M€	> 5 M€
· Según tiempo de recuperación(RTO)	> 1d	1d > x > 5h	< 5h
· Según protestas generadas	Indivudal	Pública	Masiva
· Según daño causado al servicio	Perjuicio leve	Grave pero subsanable	Grave y de imposible reparación
· Según incuplimiento de leyes o normas	Leve	Material o formal	Grave
· Según daño a la reputación	Leve	Importante	Grave

Tabla 5. Criterios de criticidad ENS.

De esta forma, los procesos identificados bajo la aplicabilidad del ENS son los indicados en las siguientes tablas:

PN.02 Gestión de cobro a clientes	
Departamento	Administración
Área	Facturación
Descripción general	Trámites necesarios para el cobro a clientes, incluyendo la devolución de pagos pertinentes (pago electrónico y liquidación del efectivo recaudado).
Información obtenida	1. Número de tarjeta transporte y número de VISA. 2. Número de cuenta. 3.Nombre y apellidos del cliente. 4. IP del cliente. 5. País de procedencia del cliente. 6. Importe a recargar. 7. Datos de los conductores (trabajadores) que liquidan. 8. Datos liquidación: cuantía y periodo en el que se ha realizado (fuera o dentro de plazo). 9. Número de tickets vendidos. 10. Código QR que contiene el arqueo del servicio diario
Canales de entrada de la información	▪ Correo electrónico ▪ Contrato firmado con el cliente (si aplica)
Sub-procesos bajo alcance del ENS (trámites)	Gestión de cobros y devoluciones a través de plataformas web.
Sistemas afectados ENS	▪ “Sistemas de Información accesibles electrónicamente por los ciudadanos”. ▪ “Sistemas de Información para el ejercicio de derechos”: Plataformas web (página web y app), correo electrónico
Valoración CIATD	C: M, I: M, A: B, T: B, D: B

Tabla 6. PN.02.

PN.04 Gestión de títulos	
Departamento	Relación con personas usuarias
Área	Desenvolupament
Descripción general	Emisión de títulos personales y no personales, además modalidades en las oficinas de atención al cliente de la compañía.
Información obtenida	1. Nombre. 2. Dirección de correo electrónico. 3. Nº tarjeta transporte. 4. Teléfono. 5. DNI. 6. Foto.
Canales de entrada de la información	▪ "Formulario de emisión de título. ▪ Correo electrónico. ▪ Teléfono. ▪ Página web y aplicaciones móviles.
Sub-procesos bajo alcance del ENS (trámites)	▪ Gestión de títulos personales a través de plataformas web (recargas, anulaciones, consultas de saldo, notificaciones al cliente) ▪ Registro de títulos no personales
Sistemas afectados ENS	▪ "Registros electrónicos": Plataformas web (página web y app), correo electrónico
Valoración CIATD	C: B, I: B, A: B, T: B, D: B

Tabla 7. PN.04.

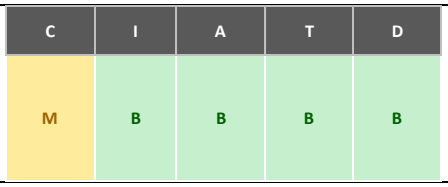
PN.05 Atención a la ciudadanía	
Departamento	Relación con personas usuarias
Área	Desenvolupament
Descripción general	Conjunto de actividades y servicios ofrecidos por la compañía en los que interactúa con los clientes (quejas y reclamaciones, objetos perdidos, comunicación por RRSS).
Información obtenida	1. Nombre del cliente. 2. Domicilio 3. Teléfono. 4. Dirección de correo electrónico. 5. Puesto y nombre del trabajador (en caso de estar involucrado) 6. Nombre de cuenta en RRSS de los clientes.
Canales de entrada de la información	▪ Correo electrónico (attcliente@valencia.es) ▪ Plataformas web (página web y app) ▪ Formulario de quejas y reclamaciones ▪ Redes Sociales ▪ Correo electrónico / Gestión Documental ▪ Teléfono
Sub-procesos bajo alcance del ENS (trámites)	Gestión de consultas, quejas y reclamaciones a través de plataformas web (portal web, correo electrónico, RRSS).
Sistemas afectados ENS	▪ "Sistemas de Información para el ejercicio de derechos": Plataformas web (página web y app), correo electrónico
Valoración CIATD	

Tabla 8. PN.05.

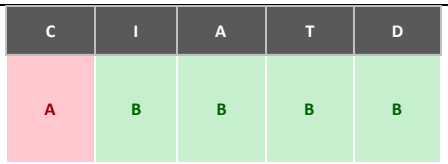
PN.09 Organización del servicio	
Departamento	Operaciones
Área	Gestión servicio autobuses
Descripción general	Organización de las líneas de autobuses que componen los servicios prestados por la compañía y asignación del personal a cada caso.
Información obtenida	1. Datos de trabajadores (nombre, apellidos, daños sufridos -si existen). 2. Número de matrícula. 3. Puesto de trabajo. 4. Línea y número de autobús. 5. Datos de los afectados (Nombre, apellidos, DNI, daños sufridos, matrícula coche -si existe-).
Canales de entrada de la información	▪ Parte de accidente. ▪ Informes médicos. ▪ Contratos ▪ Foro del empleado ▪ Teléfono ▪ Correo electrónico ▪ Formulario de reclamación
Sub-procesos bajo alcance del ENS (trámites)	▪ Gestión de la línea diversidad funcional (línea 96). ▪ Gestión de servicios especiales.
Sistemas afectados ENS	▪ "Registros electrónicos": ▪ Sistema de gestión documental, nóminas y aplicación de organización del servicio"
Valoración CIATD	

Tabla 9. PN.09.

3.3 Análisis GAP (RGPD, ENS E ISO 27002)

Una vez identificados y conocidos cada uno de los procesos y actividades de tratamiento de datos personales, el siguiente paso consistirá en conocer el nivel de cumplimiento técnico de la compañía con el marco de controles aplicables en materia de "seguridad de la información".

Este tipo de análisis nos permite conocer el nivel de seguridad existente en la compañía con respecto al nivel de seguridad óptimo aconsejado en las normativas de aplicación.

En primera instancia, se ha definido un marco de convergencia entra las normativas aplicables, de modo que los cuestionarios definidos en el apartado anterior sean de utilidad para la evaluación de madurez de cada una de las normas.

Para cada convergencia se ha establecido una relación de cumplimiento, que regula el nivel de similitud de una norma con otra.

Siendo la relación la siguiente:

Descripción del grado de cumplimiento	
0	Cubierto Siempre conviene validar que se contemplan los detalles específicos del ENS
1	Probablemente cubierto Hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea marginal
2	Probablemente se necesite completar Hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea significativo
3	No cubierto Son aspectos que no se cubren en los controles de la norma 27002 ni en los requisitos de la norma 27001, por lo que deberán ser objeto de una auditoría específica

Tabla 10. Descripción del grado de cumplimiento.

Para el desarrollo del trabajo sólo se mostrarán los controles relativos a la "seguridad de la información" y el tratamiento de datos personales, ya que la parte jurídica es desempeñada por un abogado. Cada uno de los controles que se muestran en el cuestionario han sido relacionados con la aplicación del sistema de información al que afectan. De esta forma se asigna un nivel de madurez de seguridad a cada aplicación en función de la media obtenida en el cuestionario.

La relación de controles converge como se muestra en las tablas:

			Relación ENS-ISO								
CONTROLES			RGPD	Controles ISO 27002			Controles ENS				
ID	Dominio	Descripción	Artículo	Dominio	Sub-dominio	Descripción control	Bloque	Sub-bloque	Descripción control	Relación de cumplimiento	Transversal
Q.014	Seguridad del tratamiento de datos personales	¿Existe un responsable de seguridad, así como una política de seguridad para la compañía?	Art. 32	6. Organización de la "seguridad de la información"	6.1 Organización interna	6.1.1. "seguridad de la información", Roles y Responsabilidades	[ORG] MARCO ORGANIZATIVO	[ORG.1] POLÍTICA DE SEGURIDAD		[ORG.1] - 1	SÍ
Q.015	Seguridad del tratamiento de datos personales	¿Existen políticas de acceso a la información de carácter personal por los principios: need-to-know y least priviledge?	Art. 32	6. Organización de la "seguridad de la información"	6.1 Organización interna	6.1.2 Separación de deberes	[OP] MARCO OPERACIONAL		[OP.ACC.3] SEGREGACIÓN DE FUNCIONES Y TAREAS	[OP.ACC.3] - 0	SÍ
Q.016	Seguridad del tratamiento de datos personales	¿La función de "seguridad de la información" está integrada en el ciclo de vida de desarrollo de los proyectos (especialmente los que impliquen tratamiento de datos de carácter personal)?	Art. 32	6. Organización de la "seguridad de la información"	6.1 Organización interna	6.1.5 "seguridad de la información" en Gestión de Proyectos	[OP] MARCO OPERACIONAL	[OP.EXP] EXPLOTACIÓN	[OP.EXP.7] GESTIÓN DE INCIDENCIAS	[OP.EXP.7] - 0	SÍ
Q.017	Seguridad del tratamiento de datos personales	¿Se les comunica a los trabajadores que se incorporan a la compañía la política de privacidad y las normas en materia de "seguridad de la información"? ¿Queda constancia formal de ello?	Art. 32	7.Seguridad de los Recursos Humanos	A.7. 1 antes de asumir el empleo	A.7.1.1 "Selección" A.7.1.2. "Términos y condiciones del empleo"	[OP] MARCO OPERACIONAL	[OP. CONT] CONTINUIDAD DEL SERVICIO	[OP.CONT.1] ANÁLISIS DE IMPACTO OP.CONT.2] PLAN DE CONTINUIDAD	[OP.CONT.1] - 0 [OP.CONT.2] - 0	SÍ
Q.018	Seguridad del tratamiento de datos personales	¿Existe un plan formativo en materia de "seguridad de la información" dirigido a los trabajadores de la Compañía y terceros que tengan acceso a datos personales?	Art. 32	7.Seguridad de los Recursos Humanos	A.7.2. Durante la ejecución del empleo. A.7.3. Terminación y cambio de empleo	A.7.2.2. "Toma de conciencia, educación y formación"de la "seguridad de la información". A.7.2.3."Proceso disciplinario". A.7.3.1."Terminación o cambio de responsabilidades de empleo".	[MP] MEDIDAS DE PROTECCIÓN	[MP.PER] GESTIÓN DEL PERSONAL	[MP.PER.2] DEBERES Y OBLIGACIONES [MP.PER.3] CONCIENCIACIÓN	[MP.PER.2] - 0 [MP.PER.3] - 0	SÍ
Q.019	Seguridad del tratamiento de datos personales	¿Existe un inventario actualizado de activos? ¿Existe una actualización periódica de este registro?	Art. 32	A.8. Gestión de Activos	A.8.1. Responsabilidad por los Activos	A.8.1.1. "Inventario de Activos". A.8.1.2. "Propiedad de los activos". A.8.1.3. "Uso aceptable de los activos".	[ORG] MARCO ORGANIZATIVO [OP] MARCO OPERACIONAL	[ORG.2] NORMATIVA DE SEGURIDAD [OP.PL] PLANIFICACIÓN	[OP.PL.2] ARQUITECTURA DE SEGURIDAD	[OP.PL.2] - 1	SÍ

Q.020	Seguridad del tratamiento de datos personales	¿Existe una política de clasificación de la información? ¿Tiene criterios de privacidad? ¿Se definen las medidas de seguridad que deben aplicarse para cada uno de los niveles de clasificación de la información? Para cada nivel de privacidad, ¿se han definido las medidas de seguridad que se deben cumplir a distintos niveles?	Art. 32	A.8. Gestión de Activos	A.8.2. Clasificación de la información	A.8.2.1. "Clasificación de la Información". A.8.2.2. "Etiquetado de la Información". A.8.2.3. "Manejo de Activos". A.8.2.4. "Devolución de Activos".	[ORG] MARCO ORGANIZATIVO [MP] MEDIDAS DE PROTECCIÓN	[ORG.4] PROCESO DE AUTORIZACIÓN [MP.PER] GESTIÓN DEL PERSONAL [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN [MP.INFO] PROTECCIÓN DE LA INFORMACIÓN	[MP.INFO.2] CALIFICACIÓN DE LA INFORMACIÓN [MP.SI.1] ETIQUETADO [MP.PER.2] DEBERES Y OBLIGACIONES	[MP.INFO.2] - 0 [MP.SI.1] - 0 [MP.PER.2] - 0	SÍ
Q.021	Seguridad del tratamiento de datos personales	¿Cómo se controla la información que es extraída de la compañía a través de medios extraíbles?	Art. 32	A.8. Gestión de Activos	A.8.3. Manejo de medios de soporte	A.8.3.1. "Gestión de medios de Soporte Removibles". A.8.3.2. "Disposición de los medios de soporte". A.8.3.3. "Transferencia de medios de soporte físicos".	[ORG] MARCO ORGANIZATIVO [MP] MEDIDAS DE PROTECCIÓN	[ORG.4] PROCESO DE AUTORIZACIÓN [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN	[MP.SI.1] ETIQUETADO [MP.SI.2] CRIPTOGRAFÍA [MP.SI.3] CUSTODIA [MP.SI.5] BORRADO Y DESTRUCCIÓN	[MP.SI.1] - 0 [MP.SI.2] - 1 [MP.SI.3] - 0 [MP.SI.5] - 0	SÍ
Q.022	Seguridad del tratamiento de datos personales	¿Existe una política de control de acceso a los sistemas de información de la compañía en todos sus niveles (red, sistema operativo, aplicación...)? ¿La compañía tiene implementada una política de contraseñas robusta? ¿Existe un proceso de gestión de accesos de usuario (altas, bajas, modificaciones)? ¿Existen revisiones periódicas de los usuarios con acceso a los sistemas? ¿Los usuarios administradores son los mínimos necesarios y autorizados? ¿Existe una política de auditoría por la cual se registren los accesos de usuario a los sistemas de información?	Art. 32	A.9.Control de Acceso de Usuarios.	A.9.2. Gestión de Acceso de Usuarios. A.9.4. Control de Acceso a Sistemas y Aplicaciones	A.9.2.1. "Registro y cancelación del registro de usuarios". A.9.2.2. "Suministro de acceso de usuarios". A.9.4.1. "Restricción de acceso a información". A.9.4.3. "Sistema de Gestión de Contraseñas". A.9.2.3. "Gestión de derechos de acceso privilegiado". A.9.2.6. "Retirada o adaptación de los derechos de acceso"	[OP] MARCO OPERACIONAL	[OP.ACC] CONTROL DE ACCESO	[OP.ACC.1] IDENTIFICACIÓN [OP.ACC.4] PROCESO DE GESTIÓN DE DERECHOS DE ACCESO [OP.ACC.2] REQUISITOS DE ACCESO [OP.ACC.5] MECANISMO DE AUTENTICACIÓN	[OP.ACC.1] - 1 [OP.ACC.2] - 1 [OP.ACC.4] - 1 [OP.ACC.5] - 3	SÍ
Q.023	Seguridad del tratamiento de datos personales	¿Existe un perímetro de seguridad física para proteger las zonas que contienen información crítica en formato digital? ¿Se controla el acceso a dichos espacios? ¿Y para el formato en papel?	Art. 32	A.11. Seguridad Física y Ambiental	A.11.1. Áreas Seguras	A.11.1.1. "Perímetro de Seguridad Física". A.11.1.2. "Controles Físicos de entrada". A.11.1.3. "Seguridad de oficinas, salones e instalaciones".	[MP] MEDIDAS DE PROTECCIÓN	[MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS	[MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO [MP.IF.2]	[MP.IF.1] - 0 [MP.IF.2] - 0	SÍ

						A.11.1.6. “Áreas de despacho y carga”.			IDENTIFICACIÓN DE LAS PERSONAS		
Q.024	Seguridad del tratamiento de datos personales	¿Se toman medidas de seguridad con los equipos que son susceptibles de salir de las instalaciones de la compañía?	Art. 32	A.11. Seguridad Física y Ambiental	A.11.2. Equipos	A.11.2.1. “Ubicación y protección de los equipos”. A.11.2.5. “Retiro de activos”. A.11.2.6. “Seguridad de equipos y activos fuera de las instalaciones”. A.11.2.7. “Disposición segura o reutilización de equipos”. A.11.2.8. “Equipos sin supervisión de los usuarios”. A.11.2.9. “Política de escritorio limpio y pantalla limpia”.	[MP] MEDIDAS DE PROTECCIÓN	[MP.IF] PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS [MP.EQ] PROTECCIÓN DE LOS EQUIPOS [MP.SI] PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN	[MP.IF.1] ÁREAS SEPARADAS Y CON CONTROL DE ACCESO [MP.IF.7] REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO [MP.SI.4] TRANSPORTE [MP.SI.5] BORRADO Y DESTRUCCIÓN [MP.EQ.1] PUESTO DE TRABAJO DESPEJADO [MP.EQ.2] BLOQUEO DEL PUESTO DE TRABAJO	[MP.IF.1] - 0 [MP.IF.7] - 0 [MP.SI.4] - 0 [MP.SI.5] - 0 [MP.EQ.1] - 0 [MP.EQ.2] - 0	SÍ
Q.025	Seguridad del tratamiento de datos personales	¿Existen en la compañía políticas de gestión de cambios a programa que asegure la “seguridad de la información”? ¿Son autorizados los cambios adecuadamente? ¿Son testeados los cambios desarrollados? ¿Son monitorizados los cambios una vez se trasladan al entorno de producción? ¿Existe una correcta segregación de funciones en el proceso de implantación de cambios a programa?	Art. 32	A.12. Seguridad de las Operaciones	A.12.1. Procedimientos operacionales responsabilidades	A.12.1.2. “Gestión de cambios”. A.12.1.4. “Separación de los ambientes de desarrollo, ensayo y operación”.	[OP] MARCO OPERACIONAL [MP] MEDIDAS DE PROTECCIÓN	[OP.EXP] EXPLOTACIÓN [MP.SW] PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS (SW)	[OP.EXP.5] GESTIÓN DE CAMBIOS [MP.SW.1] DESARROLLO DE APLICACIONES [MP.SW.2] ACEPTACIÓN Y PUESTA EN SERVICIO	[OP.EXP.5] - 1 [MP.SW.1] - 0 [MP.SW.2] - 1	SÍ
Q.026	Seguridad del tratamiento de datos personales	¿Existe una adecuada protección antivirus? ¿Se encuentra instalado en todos los equipos? ¿Existe una correcta gestión del mismo? ¿Se actualiza debidamente?	Art. 32	A.13. Seguridad de las Comunicaciones	A.13.1. Gestión de Seguridad de redes	A.13.1.2. “Seguridad de los servicios de red”	[ORG] MARCO ORGANIZATIVO [OP] MARCO OPERACIONAL	[ORG.4] PROCESO DE AUTORIZACIÓN [MP.COM] PROTECCIÓN DE LAS COMUNICACIONES	[MP.COM.1] PERÍMETRO SEGURO [MP.COM.2] PROTECCIÓN DE LA CONFIDENCIALIDAD [MP.COM.3]	[MP.COM.1] - 2 [MP.COM.2] - 1 [MP.COM.3] - 1 [MP.INFO.3] - 2 [OP.ACC.7] - 1 [OP.MON.1] - 2	SÍ

							[MP] MEDIDAS DE PROTECCIÓN	[MP.INFO] PROTECCIÓN DE LA INFORMACIÓN [OP.ACC] CONTROL DE ACCESO [OP.MON] MONITORIZACIÓN DEL SISTEMA	PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD [MP.INFO.3] CIFRADO DE LA INFORMACIÓN [OP.ACC.7] ACCESO REMOTO (REMOTE LOGIN) [OP.MON.1] DETECCIÓN DE INTRUSIÓN		
Q.027	Seguridad del tratamiento de datos personales	¿Existe algún procedimiento de copias de respaldo de la información? En caso de contingencia, ¿la información es recuperable a partir de las copias de backup? ¿Es monitorizado el proceso de copias de seguridad?	Art. 32	A.12. Seguridad de las Operaciones	A.12.3. Copias de Respaldo.	A.12.3.1. "Copias de respaldo de la información"	[MP] MEDIDAS DE PROTECCIÓN	[MP.INFO] PROTECCIÓN DE LA INFORMACIÓN	[MP.INFO.9] COPIAS DE SEGURIDAD (BACKUP)	[MP.INFO.9] - 0	SÍ
Q.028	Seguridad del tratamiento de datos personales	¿Existe alguna política y/o mecanismos para proteger la transferencia e intercambio de información?	Art. 32	A.13. Seguridad de las Comunicaciones	A.13.2. Transferencia de información	A.13.2.3. "Mensajes electrónicos"	[MP] MEDIDAS DE PROTECCIÓN	[MP.S] PROTECCIÓN DE LOS SERVICIOS	8.8.1. [MP.S.1] PROTECCIÓN DEL CORREO ELECTRÓNICO (E-MAIL)	[MP.S.1] - 0	SÍ
Q.029	Seguridad del tratamiento de datos personales	¿Se gestiona la "seguridad de la información" en las relaciones con terceros? ¿A la hora de subcontratar un servicio se identifican los requisitos de seguridad que el proveedor debería cumplir? ¿Existe una monitorización del servicio prestado desde el punto de vista de seguridad? ¿Desde la compañía tiene la facultad de auditar a sus proveedores (preferiblemente por contrato)?	Art. 32	A.15 Relaciones con los proveedores	A.15.1. "seguridad de la información" en las relaciones con los proveedores. A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.1.1. "Política de seguridad de la información para las relaciones con proveedores". A.15.2.1. "Seguimiento y revisión de los servicios de los proveedores".	[ORG] MARCO ORGANIZATIVO [OP] MARCO OPERACIONAL	[ORG.2] NORMATIVA DE SEGURIDAD [OP.EXT] SERVICIOS EXTERNOS	[OP.EXT.1] CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO [OP.EXT.2] GESTIÓN DIARIA	[OP.EXT.1] - 1 [OP.EXT.2] - 1	SÍ
Q.030	Seguridad del tratamiento de datos personales	¿Existen procedimientos que aseguren una rápida respuesta frente a incidentes en la "seguridad de la información"? ¿Se informa de dichos incidentes a través de los canales de gestión apropiados de forma rápida y eficiente?	Art. 32	A.16 Gestión de incidentes de "seguridad de la información"	A.16.1. Gestión de incidentes y mejoras en la "seguridad de la información"	A.16.1.1. "Responsabilidades y procedimientos". A.16.1.2. "Informe de eventos de seguridad de la información". A.16.1.3. "Informe de debilidades de seguridad de la información".	[ORG] MARCO ORGANIZATIVO [OP] MARCO OPERACIONAL	[ORG.2] NORMATIVA DE SEGURIDAD [ORG.3] PROCEDIMIENTOS DE SEGURIDAD [OP.EXP] EXPLOTACIÓN	[OP.EXP.7] GESTIÓN DE INCIDENCIAS	[OP.EXP.7] - 0	SÍ

Q.031	Seguridad del tratamiento de datos personales	¿En la compañía existe un plan que asegure la continuidad de sus operaciones? ¿Existe un plan de recuperación de desastres?	Art. 32	A.17. Aspectos de "seguridad de la información" de la gestión de continuidad de negocio	A.17.1. Continuidad de "seguridad de la información"	A.17.1.2. "Implementación de la continuidad de la seguridad de la información"	[OP] MARCO OPERACIONAL	[OP.CONT] CONTINUIDAD DEL SERVICIO	[OP.CONT.2] PLAN DE CONTINUIDAD	[OP.CONT.2] - 0	SÍ
Q.032	Seguridad del tratamiento de datos personales	¿Se encuentran identificados los requisitos de legislación y contractuales aplicables para cada sistema de información y para la organización?	Art. 32	A.18. Cumplimiento	A.18.2. Cumplimiento de requisitos legales y contractuales	A.18.2.1. "Identificación de los requisitos de legislación y contractuales aplicables". A.18.2.3. "Protección de registros". A.18.2.4. "Privacidad y protección de la información identificable personalmente".	[ORG] MARCO ORGANIZATIVO Anexo III	[ORG.3] PROCEDIMIENTOS DE SEGURIDAD		[ORG.3] - 1	SÍ

Tabla 11. Convergencia de controles.

El análisis GAP permite asignar el nivel de madurez de cada control sobre los procesos de tratamiento de la compañía. Calculando la madurez media de cada control relacionado con los dominios de la "ISO 27001" se puede obtener un gráfico representativo del nivel actual de madurez para así compararlo con el nivel objetivo. Este análisis por dominio permite conocer el estado en el que se encuentra la compañía en cuando a "seguridad de la información", mostrando las debilidades que deberían ser paliadas.

De las entrevistas elaboradas en la fase anterior se extrae la información necesaria para valorar la madurez de cada uno de los anteriores controles.

CONTROLES		
ID	Descripción	Madurez
Q.001	La compañía cuenta con un responsable de seguridad definido como tal, aunque se considera conveniente formalizar todas las funciones y responsabilidades de esta figura. Asimismo, es necesario que el responsable de seguridad cuente con un equipo de soporte en cada una de las responsabilidades que le sean asignadas.	2
Q.002	Aunque existen procedimientos que decretan los permisos de acceso y funcionalidades que ha de tener cada empleado sobre los SSII, no se dispone de una política de segregación de funciones que defina el rol y funcionalidades que ha de tener cada usuario según su puesto de trabajo. Asimismo, la asignación de permisos no es automática ni es posible controlar de manera sistemática que los perfiles asignados a cada trabajador han sido los correctos.	1
Q.003	No se ha observado la existencia de mecanismos que tengan en cuenta la privacidad desde el diseño en el desarrollo y contratación de nuevos productos/servicios.	2
Q.004	Al incorporarse un trabajador a la compañía, se le hace entrega de unos clausulados en materia de "seguridad de la información" que están alineados con los exigido por la LOPD de 1999. Como comprobante de ello, se les hace firmar un "recibí".	1
Q.005	Los empleados de la compañía, más allá de las recomendaciones puntuales que puedan transmitirles el departamento de IT en cuento a "seguridad de la información", no reciben ningún tipo de formación o concienciación en esta materia.	1
Q.006	- Pese a que no existe una política de gestión de activos, si no que el procedimiento del que disponen es el de gestión de activos incluido en el documento de seguridad exigido por la LOPD de 1999, poseen un inventario de activos informáticos HW que no incluye los periféricos. Sin embargo, no tienen un inventario de software. - Cada equipo informático está asociado a un empleado. - No existe un manual de usuario que detalle las pautas a seguir en el uso de la información y activos asociados a información de la compañía.	1
Q.007	- No existe una política de clasificación de la información. - La información no es etiquetada, ni existe un procedimiento que define como hacerlo. - No existe una política de clasificación de la información ni un manual de uso de activos acorde a la información contenida en los mismos.	1
Q.008	No existen procedimientos de gestión de medios removibles. Asimismo, la compañía incorpora el cifrado de equipos mediante el uso de BitLocker, pero no utilizan cifrado para medios extraíbles.	2
Q.009	- La gestión de permisos es por Active Directory, se controla a los usuarios por áreas y departamentos. - Solo existe el procedimiento de "Gestión de usuarios" definido como parte de lo exigido por la LOPD de 1999, y aunque el procedimiento actual es sostenido por la utilización de la herramienta REDMINE no está documentado como tal. - Existe una normativa de "seguridad de la información" pero no se garantiza su cumplimiento. - No se garantiza que la política de contraseñas de acceso a las aplicaciones cumpla con las buenas prácticas. - Aunque ha de estudiarse para cada caso, los permisos de acceso privilegiado son asignados según unos criterios concretos conocidos por el personal de IT pero que no están escritos ni documentados.	2
Q.010	- CPD principal (oficinas centrales): el único control de accesos indebidos es el control de accesos al edificio, ya que la puerta de acceso al CPD no está ni siquiera cerrada con llave. CPD en Sant Isidre: está protegido por llave tradicional. - No existen controles de entrada apropiados para proteger las áreas seguras.	3
Q.011	- Las medidas de protección a los equipos reside en el control de acceso al edificio.	2
Q.012	- El único procedimiento de gestión de cambios con el que cuenta la compañía es el que se generó para el cumplimiento de la LOPD de 1999. - Para las aplicaciones desarrolladas internamente, no existen entornos diferenciados de desarrollo y producción, sino que para los desarrollos se hacen copias parciales sobre las que ejecutar los cambios y comprobar su funcionamiento. Mientras que para las aplicaciones mantenidas por un desarrollador externo, se presupone que sí existen entornos diferenciados, pero se desconoce cómo trabajan. Además, se sabe que los usuarios desarrolladores también tienen acceso al entorno de producción. Asimismo, no para todos los casos existe un entorno de test como tal. Sino que los cambios son testeados en el entorno de desarrollo.	2
Q.013	La salida a internet es a través de FW y para la protección de los equipos ante infecciones malware cuentan con herramientas de antivirus. Estas medidas están documentadas en uno de los procedimientos anexos al Documento de Seguridad definido para el cumplimiento con la LOPD de 1999. Aunque se detecta que existe un amplio margen de mejora en este ámbito (las recomendaciones aparecen detalladas en el informe de trabajo resultante del análisis de intrusión que se ha llevado a cabo sobre los SSII de la compañía)	3
Q.014	Se realizan copias de seguridad completas de los SSII de la compañía en disco duros de conexión USB y con periodicidad diaria. A partir de la que se almacena una copia diaria de la última semana, una copia semanal del último mes y las copias mensuales del último año. La ejecución de copias sobre las unidades de red se ha instalado una nueva cabina de discos. Aunque el proceso de copias de seguridad es conocido por los integrantes del departamento de IT, no existe un procedimiento formalmente definido como tal.	1
Q.015	No se protege la información que contienen los mensajes electrónicos.	1
Q.016	- El acceso de los proveedores a los activos de información de la compañía es gestionado de manera informal, no existiendo para cada caso un documento que recoja los niveles y requisitos acordados. Ni tampoco existe el análisis realizado para la asignación de permisos. - Puesto que no se acuerdan los requisitos de seguridad con los proveedores, no es posible revisar los niveles de seguridad acordados.	1
Q.017	- El único procedimiento que tiene la compañía para la gestión de incidentes es el formulado como parte de lo exigido por la LOPD de 1999. El cual se detecta que no corresponde exactamente con la configuración actual. El proceso actual no está documentado, y el procedimiento e gestión de incidentes es gestionado por el responsable de sistemas, y no existe backup de esta persona para estos fines. - Sin embargo, el único mecanismo conocido de monitorización que ha implementado la compañía es la emisión de una alarma al ocurrir un fallo en el registro a un acceso VPN.	1
Q.018	No existe un "Plan de Continuidad de Negocio" definido para la compañía. Si no que en caso de contingencia se actuaría de manera reactiva.	1
Q.019	La relación de requisitos legislativos para la compañía no está registrada.	1
Q.020	- No existe una política de clasificación de la información. - La información no es etiquetada, ni existe un procedimiento que define como hacerlo. - No existe una política de clasificación de la información ni un manual de uso de activos acorde a la información contenida en los mismos.	1

Q.021	No existen procedimientos de gestión de medios removibles. Asimismo, la compañía incorpora el cifrado de equipos mediante el uso de BitLocker, pero no utilizan cifrado para medios extraíbles.	1
Q.022	- La gestión de permisos es por Active Directory, se controla a los usuarios por áreas y departamentos. - Solo existe el procedimiento de "Gestión de usuarios" definido como parte de lo exigido por la LOPD de 1999, y aunque el procedimiento actual es sostenido por la utilización de la herramienta REDMINE no está documentado como tal. - Existe una normativa de "seguridad de la información" pero no se garantiza su cumplimiento. - No se garantiza que la política de contraseñas de acceso a las aplicaciones cumpla con las buenas prácticas. - Aunque ha de estudiarse para cada caso, los permisos de acceso privilegiado son asignados según unos criterios concretos conocidos por el personal de IT pero que no están escritos ni documentados.	1
Q.023	- CPD principal (oficinas centrales): el único control de accesos indebidos es el control de accesos al edificio, ya que la puerta de acceso al CPD no está ni siquiera cerrada con llave. CPD en Sant Isidre: está protegido por llave tradicional. - No existen controles de entrada apropiados para proteger las áreas seguras.	1
Q.024	- Las medidas de protección a los equipos reside en el control de acceso al edificio.	1
Q.025	- El único procedimiento de gestión de cambios con el que cuenta la compañía es el que se generó para el cumplimiento de la LOPD de 1999. - Para las aplicaciones desarrolladas internamente, no existen entornos diferenciados de desarrollo y producción, sino que para los desarrollos se hacen copias parciales sobre las que ejecutar los cambios y comprobar su funcionamiento. Mientras que para las aplicaciones mantenidas por un desarrollador externo, se presupone que sí existen entornos diferenciados, pero se desconoce cómo trabajan. Además, se sabe que los usuarios desarrolladores también tienen acceso al entorno de producción. Asimismo, no para todos los casos existe un entorno de test como tal. Sino que los cambios son testeados en el entorno de desarrollo.	1
Q.026	La salida a internet es a través de FW y para la protección de los equipos ante infecciones malware cuentan con herramientas de antivirus. Estas medidas están documentadas en uno de los procedimientos anexos al Documento de Seguridad definido para el cumplimiento con la LOPD de 1999. Aunque se detecta que existe un amplio margen de mejora en este ámbito (las recomendaciones aparecen detalladas en el informe de trabajo resultante del análisis de intrusión que se ha llevado a cabo sobre los SSII de la compañía)	1
Q.027	Se realizan copias de seguridad completas de los SSII de la compañía en disco duros de conexión USB y con periodicidad diaria. A partir de la que se almacena una copia diaria de la última semana, una copia semanal del último mes y las copias mensuales del último año. La ejecución de copias sobre las unidades de red, se ha instalado una nueva cabina de discos. Aunque el proceso de copias de seguridad es conocido por los integrantes del departamento de IT, no existe un procedimiento formalmente definido como tal.	2
Q.028	No se protege la información que contienen los mensajes electrónicos.	1
Q.029	- El acceso de los proveedores a los activos de información de la compañía es gestionado de manera informal, no existiendo para cada caso un documento que recoja los niveles y requisitos acordados. Ni tampoco existe el análisis realizado para la asignación de permisos. - Puesto que no se acuerdan los requisitos de seguridad con los proveedores, no es posible revisar los niveles de seguridad acordados.	1
Q.030	- El único procedimiento que tiene la compañía para la gestión de incidentes es el formulado como parte de lo exigido por la LOPD de 1999. El cual se detecta que no corresponde exactamente con la configuración actual. El proceso actual no está documentado, y el procedimiento e gestión de incidentes es gestionado por el responsable de sistemas, y no existe backup de esta persona para estos fines. - Sin embargo, el único mecanismo conocido de monitorización que ha implementado la compañía es la emisión de una alarma al ocurrir un fallo en el registro a un acceso VPN.	2
Q.031	No existe un "Plan de Continuidad de Negocio" definido para la compañía. Si no que en caso de contingencia se actuaría de manera reactiva.	1
Q.032	La relación de requisitos legislativos para la compañía no está registrada.	1

Tabla 12. Evaluación niveles de madurez.

Madurez actual promedio	24,1%	Madurez Objetivo	60,0%

Evaluación por Dominio			
Dominio		Nivel de Madurez	Nivel Objetivo
A.05	"POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN"	1,00	3,00
A.06	"ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"	1,14	3,00
A.07	"SEGURIDAD DE LOS RECURSOS HUMANOS"	1,00	3,00
A.08	"GESTIÓN DE ACTIVOS"	1,00	3,00
A.09	"CONTROL DE ACCESO"	1,46	3,00
A.10	"CRIPTOGRAFÍA"	2,00	3,00
A.11	"SEGURIDAD FÍSICA Y AMBIENTAL"	1,27	3,00
A.12	"SEGURIDAD DE LAS OPERACIONES"	1,42	3,00
A.13	"SEGURIDAD DE LAS COMUNICACIONES"	1,29	3,00
A.14	"ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS"	1,00	3,00
A.15	"RELACIONES CON LOS PROVEEDORES"	1,00	3,00
A.16	"GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN"	1,14	3,00
A.17	"CONTINUIDAD DE NEGOCIO"	1,00	3,00
A.18	"CUMPLIMIENTO"	1,13	3,00

Tabla 13. Evaluación por dominios ISO.

Figura 8. Gráfico por dominios ISO.

En paralelo, se ha dibujado el estado de adaptación al RGPD de la compañía con el nivel de madurez medio por cada dominio del reglamento. En este caso, el dominio bajo alcance del trabajo es el 7, Seguridad del tratamiento de datos personales.

El gráfico es obtenido de la misma forma que el de la evaluación de la seguridad; generando un análisis sobre los controles que se han agrupado según la convergencia establecida, en el que se valoran todos los dominios de las normativas aplicables a la compañía, teniendo en cuenta todos los procesos de negocio que manejan. Esta visión permite conocer los puntos principales de mejora de la compañía en relación al RGPD, información que servirá para dar enfoque al plan de acción encaminado a mejorar los niveles de madurez.

Madurez actual promedio	32,9% (1,6)	Madurez Objetivo	60,0% (3,0)

Evaluación por Dominio			
Dominio		Nivel de Madurez	Nivel Objetivo
1	"Principios básicos del tratamiento"	**1,50**	3,00
2	"Licitud del tratamiento"	**2,00**	3,00
3	"Consentimiento"	**1,00**	3,00
4	"Derechos de los interesados"	**1,00**	3,00
5	"Responsabilidad del responsable del tratamiento"	**2,00**	3,00
6	"Registro de las actividades del tratamiento"	**3,00**	3,00
7	"Seguridad del tratamiento de datos personales"	**1,11**	3,00
8	"Notificación de una violación de la seguridad de los datos personales a la autoridad de control y a los interesados"	**1,00**	3,00
9	"Evaluación de Impacto relativa a la Protección de Datos"	**2,00**	3,00
10	"Consulta previa"	**2,00**	3,00
11	"Delegado de Protección de Datos (DPO)"	**1,50**	3,00
13	"Transferencias internacionales a datos a terceros países u organizaciones internacionales"	**n.a.**	3,00

Tabla 14. Evaluación por dominios RGPD.

Figura 9. Gráfico por dominios RGPD.

Los niveles de madurez se han seleccionado con respecto a la normativa del "Esquema Nacional de Seguridad", siendo esta la escala de los niveles [15]:

Descripción del Nivel de Madurez	
n.a.	**No existe**
	▸ No se tiene en cuenta este control. No consta como objetivo de la organización.
1	**Inicial**
	▸ Básico, ad hoc, indocumentado; la capacidad de cambio puede darse con tecnología y algunas herramientas; procesos locales limitados; apoyo organizativo limitado.
2	**Repetible**
	▸ Se disponen de procedimientos sistemáticos de los cuales no se hace una formalización por escrito, sino que pasan a depender de la buena suerte o el buen hacer de los empleados.
3	**Definido**
	▸ Existe una normativa y una formalización de los procedimientos a seguir en relación a cada incidente, el personal dispone de cierta formación y las métricas mejoran. Sigue existiendo un factor de azar.
4	**Gestionado**
	▸ Se dispone de un conjunto de procedimientos detallados que aportan un nivel de confianza estable para la organización.
5	**Optimizado**
	▸ La organización tiene todos los procesos controlados y sus métricas están definidas claramente. En este nivel el objetivo es la mejora continua de la seguridad y la implementación de nuevas soluciones que permitan mejorar las existentes al nivel de detalle.

Tabla 15. Descripción niveles de madurez.

3.4 Análisis de riesgos y evaluaciones de impacto

3.4.1 Metodología Magerit

Para realizar el análisis de riesgos, la metodología escogida es la Magerit. Este método permite conocer los activos que forman el negocio, el valor que poseen y las amenazas a las que están expuestos. A través del análisis interno de la compañía se confecciona un tratamiento para los riesgos a los que ésta se encuentra expuesta, se proponen medidas de seguridad y se evalúa su nivel de cumplimiento actual y se compara con el nivel deseado.

En primer lugar, se identifican los activos de la compañía. Existen amenazas que pueden afectar de forma directa o indirecta a dichos activos y ser perjudiciales para el valor de la compañía, pudiendo causar un impacto negativo.

Estimando la probabilidad de que la amenaza pueda llegar a afectar al activo, se consideran los Riesgos a los que la compañía está expuesta. Para hacer frente a los riesgos, se seleccionan una serie de medidas o salvaguardas que hagan a los sistemas menos vulnerables. Estas salvaguardas tratan de minimizar el impacto que las amenazas tendrían sobre la compañía, hasta el punto de asumir únicamente unos valores de riesgo aceptables [16].

3.4.2 Análisis de Riesgos con PILAR

Una de las herramientas al alcance de las Administraciones Publicas para el análisis de riesgos es PILAR, capaz de realizar un análisis siguiendo la "metodología Magerit".

PILAR analiza los activos que se introducen en el software, que son el núcleo del funcionamiento de la organización. Conocidos los activos, PILAR asigna las amenazas a las que estos están expuestos según su naturaleza y su relación entre ellos para, de esta forma, averiguar cuáles son los riesgos reales a los que se expone la compañía. [17]

Figura 10. Pasos que seguir en PILAR.

3.4.3 Activos

3.4.3.1 Identificación

En este apartado se muestran los elementos que se han volcado sobre la herramienta, necesarios para el análisis de riesgos.

En primer lugar, se identifican las actividades de tratamiento sobre las que tiene aplicación el ENS, cuyo marco de controles va a ser el seleccionado para establecer las salvaguardas.

Servicios e Información afectados por el ENS	Dimensiones				
	D	C	I	T	A
Gestión de cobro a clientes (pagos online)	M	M	B	B	B
Gestión de títulos	B	B	B	B	B
Página web	B	B	B	B	B
Atención al cliente	M	B	B	B	B
Gestión servicio autobuses	A	B	B	B	B
Servicios especiales (línea 96)	M	A	B	B	B
Sorteos y promociones	B	B	B	B	B
Conexión Wifi	B	B	B	B	B

Tabla 16. Valoración Servicios ENS.

En la siguiente tabla se muestran los "Sistemas de la Información" vulnerables a amenazas y su criticidad.

Activos y servicios de información	Categorización sistemas
LOTUS NOTES	Medio
Gestor Documental	Bajo
Portal del empleado	Medio
AP. Operaciones	Bajo
AP. Nóminas	Bajo
Redes sociales	Bajo
EPESI (BDD clientes)	Medio

Tabla 17. Categorización Sistemas de Información.

Para comenzar con el análisis de riesgos, el primer paso consiste en identificar y calificar activos.

Los activos pertenecen a dominios de seguridad, que pueden englobar más activos, pero un activo solo puede pertenecer a un dominio.

El dominio de seguridad es un bloque de activos al que se le aplican unas mismas protecciones. Los dominios diferencian las zonas del sistema de información.

Se han identificado los siguientes dominios de seguridad:

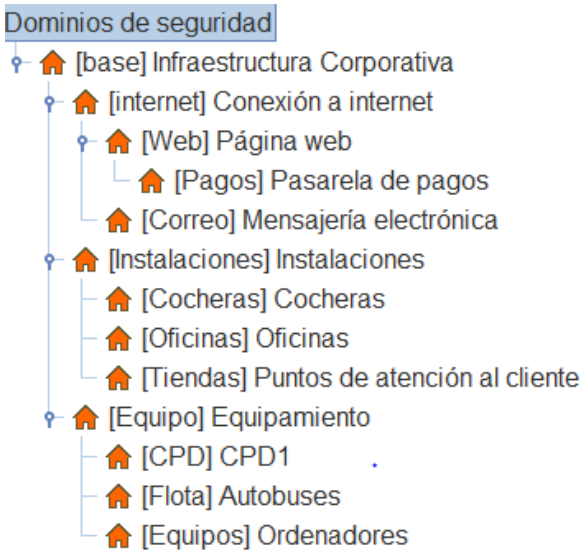


Figura 11. Dominios de seguridad.

A continuación, se crean los activos en base a la información obtenida de las sesiones de entendimiento con la compañía y se ubican en su dominio correspondiente.

En primer lugar, tenemos los **activos esenciales**, consistentes en la información y los servicios que maneja el sistema. Este tipo de activo puede ser de clase 'información' o 'servicio', incluso de ambos.

Cada activo es caracterizado por sus requisitos, los activos de información suelen estar definidos por confidencialidad e integridad. Los de tipo servicio se caracterizan por la disponibilidad.

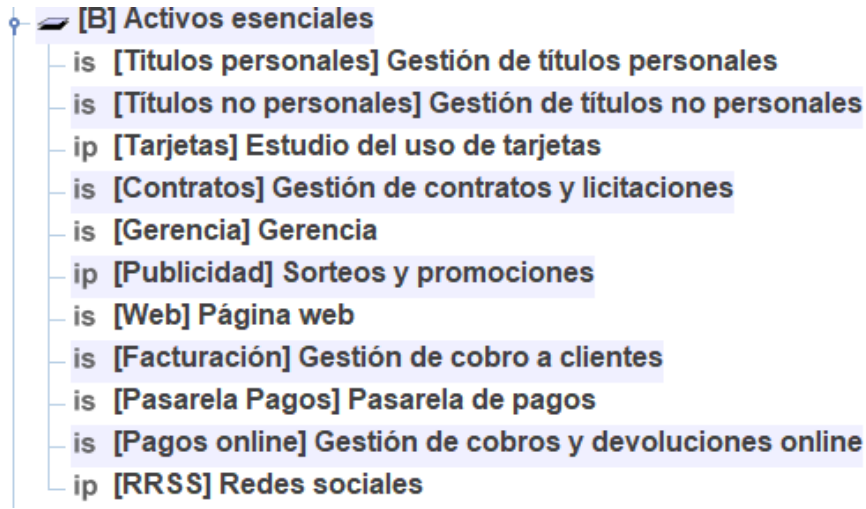


Figura 12. Activos esenciales.

El siguiente tipo de activo son los **servicios internos,** procesos relativos al funcionamiento de la propia compañía y sus empleados.

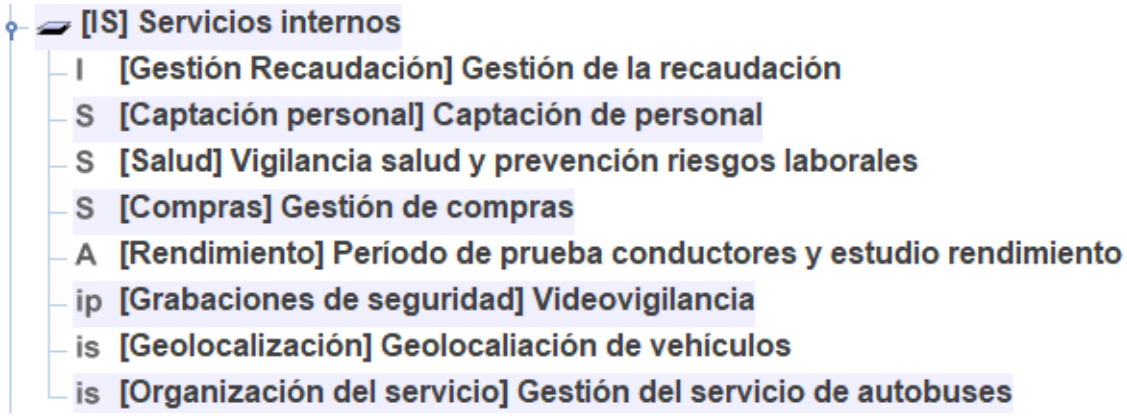


Figura 13. Servicios Internos.

El equipamiento es el siguiente tipo de activo a identificar. Activos de tipo equipamiento son las aplicaciones, las redes de comunicaciones, los elementos auxiliares y todo el hardware.

Los servicios subcontratados por la compañía también han sido añadidos.

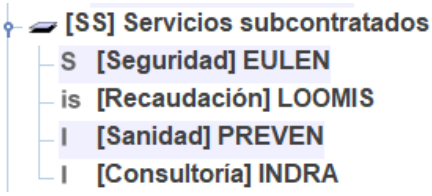


Figura 14. Servicios subcontratados.

Así como los servicios que la compañía presta a la ciudadanía.

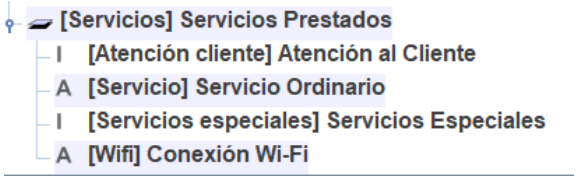


Figura 16. Servicios prestados.

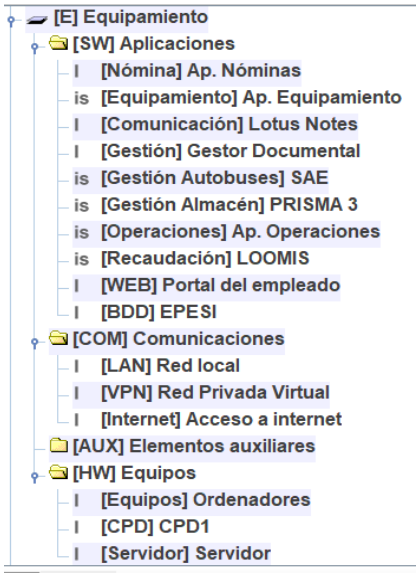


Figura 15. Equipamiento.

3.4.3.2 Clases de activos

Una vez identificados todos los activos, el siguiente paso consiste en clasificarlos. PILAR nos permite asignar a cada activo una o varias clases, que dependen del tipo de información o proceso que éste relacionado al activo.

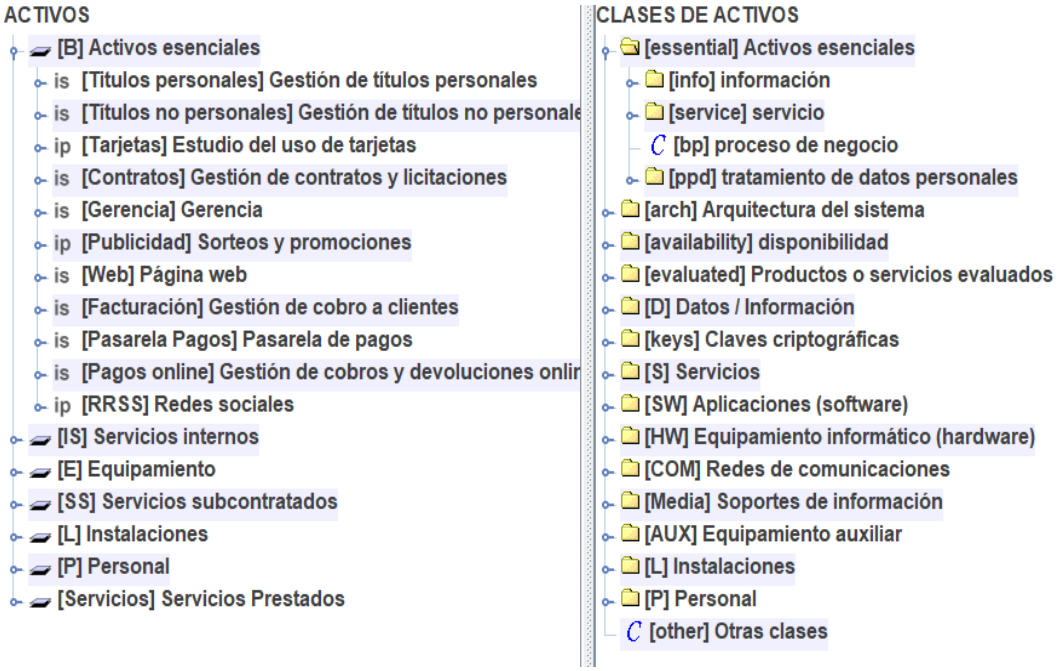


Figura 17. Clases de activos.

3.4.3.3 Valoración de activos

Los criterios de evaluación / clasificación se han asignado según el nivel requerido de seguridad por dominio (disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y daños personales). PILAR determina el valor de riesgo de los procesos según el nivel de seguridad de cada componente.

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[B] Activos esenciales							
is [Titulos personales] Gestión de títulos personales	[2]	[2]	[3]	[2]	[2]		[3]
is [Títulos no personales] Gestión de títulos no personales	[2]	[2]	[2]	[2]	[2]		[1]
ip [Tarjetas] Estudio del uso de tarjetas			[1]				[1]
is [Contratos] Gestión de contratos y licitaciones	[1]	[1]	[1]	[1]			[1]
is [Gerencia] Gerencia	[1]	[1]	[1]	[1]			[1]
ip [Publicidad] Sorteos y promociones	[1]	[1]	[1]	[1]			[1]
is [Web] Página web	[4]	[4]	[4]	[4]	[4]		[4]
is [Facturación] Gestión de cobro a clientes	[2]	[4]	[4]	[2]	[2]		[4]
is [Pasarela Pagos] Pasarela de pagos	[4]	[4]	[4]	[4]	[4]		[4]
is [Pagos online] Gestión de cobros y devoluciones online	[4]	[3]	[2]	[3]	[3]		[2]
ip [RRSS] Redes sociales	[1]	[1]	[2]	[1]			[1]

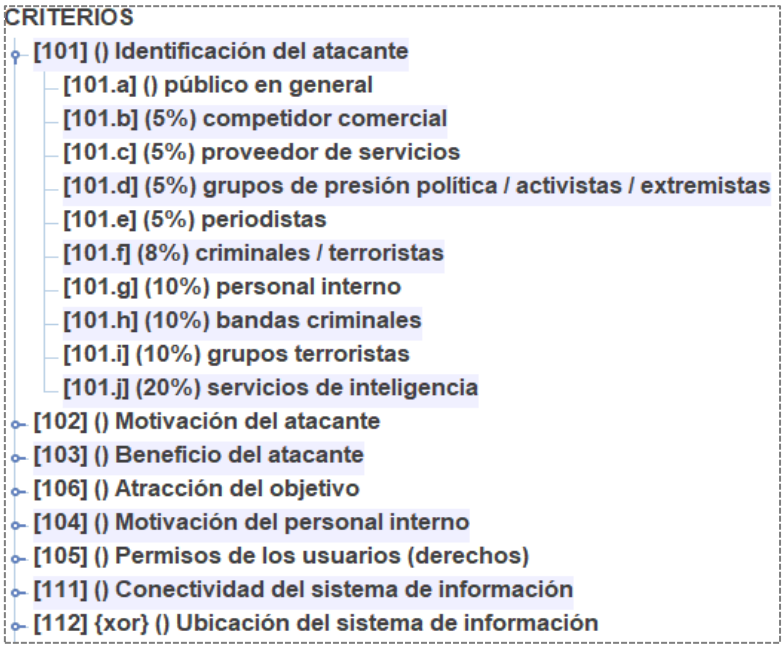
Figura 18. Valoración de activos.

Escala criterios evaluación.											
Nivel 10	Nivel 9	Alto (+)	Alto	Alto (-)	Medio (+)	Medio	Medio (-)	Bajo (+)	Bajo	Despreciable	No aplica
10	9	8	7	6	5	3	3	2	1	0	n.a

Tabla 19. Escala criterios de evaluación.

3.4.4 Amenazas

3.4.4.1 Factores agravantes/atenuantes



De forma manual, se añaden factores agravantes o atenuantes que pueden afectar a cada activo. Estos criterios se añaden en forma de sumatorio, suponiendo un atenuante o un agravante, en función del caso seleccionado.

Figura 20. Criterios agravantes/atenuantes.

Según la naturaleza del propio proceso de negocio, son de aplicación unas amenazas u otras:

- "Desastres naturales" [N].
- "De origen industrial "[I].
- "Errores y fallos no intencionados" [E].
- "Ataques deliberados" [A].
- "Riesgos sobre la privacidad" [PR].

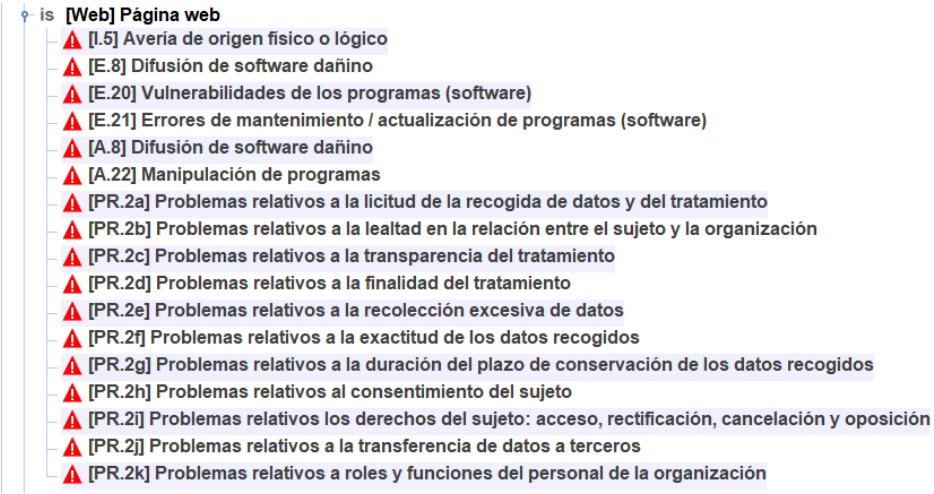


Figura 21. Ejemplo amenazas.

3.4.5 Medidas técnicas y organizativas

3.4.5.1 Identificación y valoración de salvaguardas

Para mitigar los riesgos obtenidos mediante el análisis de los activos de la compañía, en el siguiente paso, se analiza el grado de cumplimiento de normativas de seguridad, formadas por controles que pueden ser mejorados con salvaguardas, para el caso del trabajo, las normativas ISO 27002 y RGPD.

- Observando la ***Figura 20. Valoración controles,*** se tiene que, en cada una de las medidas de seguridad, hay una columna, **Recomendación,** que otorga importancia a cada una de ellas.
- El semáforo, siguiente columna, indica con un color el grado de madurez de cada medida.

recomendación		control	...	...	...	...	current	target	PILAR
		[27002:2013] Código de prácticas para los controles de seguridad de la información					(_-L2)	(L3)	L2-L5
2		[5] Políticas de seguridad de la información					(L2)	(L3)	L2
7		[6] Organización de la seguridad de la información					(_-L2)	(L3)	L2-L4
6		[7] Seguridad relativa a los recursos humanos					(L2)	(L3)	L3-L4 (L2-L4)
7		[8] Gestión de activos					(L1-L2)	(L3)	L2-L4
7		[9] Control de acceso					(L1-L2)	(L3)	L2-L4
4		[10] Criptografía					(_-L1)	(L3)	L3 (L2-L3)
5		[11] Seguridad física y del entorno					(L1-L2)	(L3)	L3 (L2-L3)
8		[12] Seguridad de las operaciones					(L1-L2)	(L3)	L2-L5
8		[13] Seguridad de las comunicaciones					(_-L2)	(L3)	L3-L5 (L2-L5)
6		[14] Adquisición, desarrollo y mantenimiento de los sistemas de información					(L1)	(L3)	L2-L4
5		[15] Relación con proveedores					(L1)	(L3)	L3 (L2-L3)
4		[16] Gestión de incidentes de seguridad de la información					(L2)	(L3)	L3 (L2-L3)
6		[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio					(L1-L2)	(L3)	L3-L4 (L2-L4)
4		[18] Cumplimiento					(L1-L2)	(L3)	L2-L3

Figura 22. Valoración controles ISO 27002.

rec...		control	du...	fu...	apl...	co...	current	target	PILAR
		[R_2016-679] Reglamento relativo al tratamiento de datos personales					L1-L2	L3	L3
5		[C2] Capítulo II - Principios			M		L2	L3	L3
5		[C3] Capítulo III - Derechos del interesado					L1	L3	L3
5		[C4] Capítulo IV - Responsable del tratamiento y encargado del tratamiento					L2	L3	L3
5		[C5] Capítulo V - Transferencias de datos personales a terceros paises u organizaciones internacionales					n.a.	n.a.	L3

Figura 23. Valoración controles RGPD.

Una vez valorados los controles, PILAR nos muestra las salvaguardas recomendadas para los anteriores controles. También es asignado un grado de recomendación. Además, se ha puesto el nivel de cumplimiento con respecto a cada salvaguarda (L0-L5), teniendo en cuenta la situación actual, la objetivo y el nivel recomendable impuesto por PILAR.

La columna "tdp" indica el tipo de protección que ofrece cada salvaguarda, pudiendo ser:

- PR: prevención.
- DR: disuasión.
- EL: eliminación.
- IM: minimización del impacto.
- CR: corrección.
- RC: recuperación.
- AD: administrativa.
- AW: de concienciación.

- DC: detección.
- MN: monitorización.
- std: norma.
- proc: procedimiento.
- cert: certificación o acreditación.

Habiendo cuatro aspectos; general (G), técnico (T), físico (F) y personal (P).

as...	tdp	salvaguarda	...	...	...	recome...		current	target	PILAR
		SALVAGUARDAS								
G	EL	[IA] Identificación y autenticación				8		L2	L3	L2-L5
T	EL	[AC] Control de acceso lógico				7		L2	L3	L2-L4
G	PR	[D] Protección de la Información				7		L1	L3	L2-L4
G	EL	[K] Protección de claves criptográficas							L3	n.a.
G	PR	[S] Protección de los Servicios				6		L1	L3	L2-L4
G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)				7		L1	L3	L2-L4
G	PR	[HW] Protección de los Equipos Informáticos (HW)				7		L1	L3	L2-L4
G	PR	[COM] Protección de las Comunicaciones				8		L1	L3	L2-L5
G	PR	[IP] Sistema de protección de frontera lógica						L1	L3	n.a.
G	PR	[MP] Protección de los Soportes de Información				7		L1	L3	L2-L4
G	PR	[AUX] Elementos Auxiliares				6		L2	L3	L2-L4
F	EL	[HW_0049] Protección física del equipamiento				6		L1	L3	L3-L4
F	PR	[L] Protección de las Instalaciones				7		L1	L3	L2-L4
F	EL	[PPS] Protección del perímetro físico						L1	L3	n.a.
P	PR	[PS] Gestión del Personal				6		L2	L3	L2-L4
G	PR	[PDS] Servicios potencialmente peligrosos						_-L1	L3	n.a.
G	CR	[IR] Gestión de incidentes				6		L2	L3	L2-L4
T	PR	[tools] Herramientas de seguridad				8		L1	L3	L2-L5
G	CR	[V] Gestión de vulnerabilidades				6		L1	L3	L2-L4
T	MN	[A] Registro y auditoría				5		L2	L3	L2-L3
G	RC	[BC] Continuidad del negocio				5		L1	L3	L2-L3
G	AD	[G] Organización				4		L2	L3	L2-L3
G	AD	[E] Relaciones Externas				5		L1	L3	L2-L3
G	AD	[NEW] Adquisición / desarrollo				5		L1	L3	L2-L3

Figura 24. Salvaguardas propuestas.

3.4.6 Resultados

3.4.6.1 Análisis de resultados: impacto

El impacto indica que sucedería en caso de que las amenazas llegaran a ocurrir.

En las ***Figuras 25 y 26***, se muestran los valores de impacto que pilar ha asignado a los activos seleccionaos.

potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[6]	[5]	[6]	[6]	[5]		[7]
[B] Activos esenciales	[4]	[4]	[4]	[5]	[5]		[7]
[IS] Servicios internos							[7]
[E] Equipamiento	[6]	[5]	[6]	[6]			[7]
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							
[Servicios] Servicios Prestados	[4]	[4]	[4]	[5]	[5]		[7]

Figura 25. Valores de impacto actuales

potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	[3]	[3]	[3]	[3]	[2]		[7]
[B] Activos esenciales	[2]	[2]	[2]	[3]	[2]		[7]
[IS] Servicios internos							[7]
[E] Equipamiento	[3]	[3]	[3]	[3]			[7]
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							
[Servicios] Servicios Prestados	[2]	[2]	[2]	[3]	[2]		[7]

Figura 26. Valores de impacto objetivo.

La siguiente gráfica aporta una visión más clarificadora de los niveles de impacto que tendrían las amenazas sobre cada dominio de seguridad, si llegan a ocurrir.

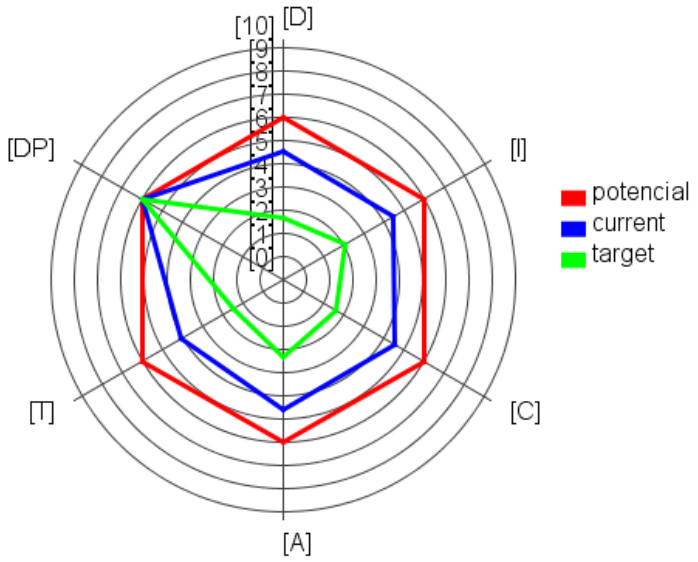


Figura 27. Impacto según dimensiones.

3.4.6.2 Análisis de resultados: riesgos

PILAR estima los niveles de riesgo actual en función de las amenazas y el impacto estimado anteriormente. En la siguiente figura se muestran los niveles de riesgo actual junto con los niveles de riesgo potencialmente más altos de los activos de la compañía.

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS	{4,5}	{4,3}	{5,0}	{4,8}	{4,2}		{5,4}
[B] Activos esenciales	{3,6}	{3,6}	{2,8}	{3,4}	{3,8}		{5,4}
is [Titulos personales] Gestión de títulos persona							{5,4}
is [Titulos no personales] Gestión de títulos no p							{5,4}
is [Contratos] Gestión de contratos y licitaciones							{5,4}
is [Gerencia] Gerencia							{5,4}
ip [Publicidad] Sorteos y promociones							{5,4}
is [Web] Página web	{0,82}	{1,9}	{1,9}				{3,6}
is [Facturación] Gestión de cobro a clientes							{5,4}
is [Pasarela Pagos] Pasarela de pagos							{3,6}
is [Pagos online] Gestión de cobros y devolucior							{5,4}
ip [RRSS] Redes sociales	{3,6}	{3,6}	{2,8}	{3,4}	{3,8}		{5,4}
[IS] Servicios internos							{5,4}
[E] Equipamiento	{4,4}	{4,3}	{5,0}	{4,8}			{5,4}
[SW] Aplicaciones	{3,8}	{3,7}	{4,8}	{4,6}			{5,4}
I [Nómina] Ap. Nóminas	{1,0}	{0,89}	{1,1}				{2,5}
I [Comunicación] Lotus Notes	{1,0}	{0,89}	{1,1}				
I [Gestión] Gestor Documental	{1,0}	{0,89}	{1,1}				{2,5}
is [Operaciones] Ap. Operaciones	{1,0}	{0,89}	{1,1}				
I [WEB] Portal del empleado	{0,82}	{1,9}	{1,9}				
I [BDD] EPESI	{3,8}	{3,7}	{4,8}	{4,6}			{5,4}
[COM] Comunicaciones	{4,4}	{2,2}	{3,3}	{3,8}			
I [LAN] Red local	{4,2}	{2,2}	{3,3}	{3,8}			
I [VPN] Red Privada Virtual	{4,4}						
I [Internet] Acceso a internet	{4,2}	{2,2}	{3,3}	{3,8}			
[HW] Equipos	{4,1}	{4,3}	{5,0}	{4,8}			
I [Servidor] Servidor	{4,1}	{4,3}	{5,0}	{4,8}			
[SS] Servicios subcontratados							
[L] Instalaciones							
[P] Personal							
[Servicios] Servicios Prestados	{4,5}	{3,8}	{3,4}	{3,6}	{4,2}		{5,4}
I [Atención cliente] Atención al Cliente	{3,6}	{3,6}	{2,8}	{3,4}	{3,8}		{5,4}
I [Servicios especiales] Servicios Especiales	{3,6}	{3,6}	{2,8}	{3,4}	{3,8}		{5,4}
A [Wifi] Conexión Wi-Fi	{0,89}	{0,80}	{0,66}	{0,76}	{0,94}		
is [Aparcamiento] Servicio de aparcamiento	{4,5}	{3,8}	{3,4}	{3,6}	{4,2}		{5,4}

Figura 28. Valores de riesgo.

La leyenda de la herramienta nos indica el significado de cada valor.

Figura 29. Leyenda riesgos.

En la siguiente gráfica, se comparan los resultados del nivel de riesgo actual, objetivo y propuesto por PILAR como objetivo para los procesos de negocio de la compañía.

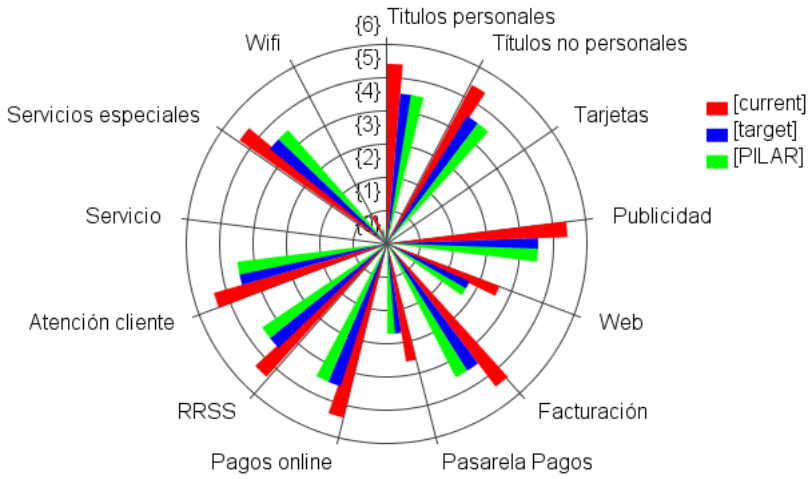


Figura 30. Niveles de riesgo Procesos de negocio.

Por último, se evalúa el nivel de riesgo de los activos correspondientes a los "sistemas de información" de la compañía.

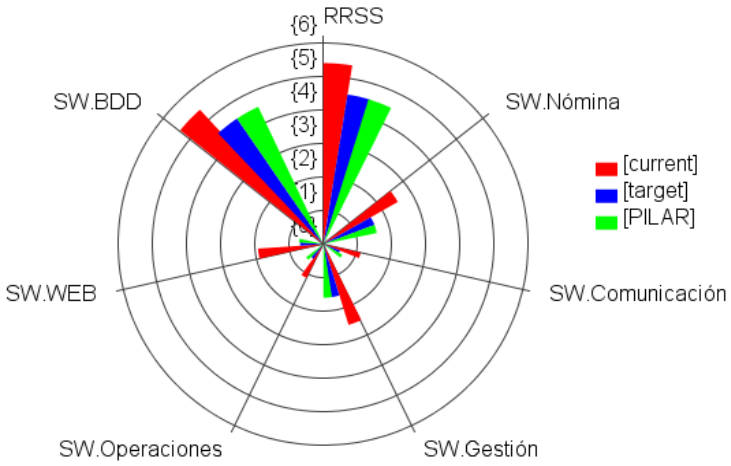


Figura 31. Niveles de riesgo Sistemas de Información

3.4.6.3 Análisis de resultados: salvaguardas

PILAR contiene un grupo de informes predefinidos, elaborados a partir de la información volcada en la herramienta y los riesgos e impacto que se estiman.

Para el caso de este trabajo, se han seleccionado los resultados que definen el estado de los activos de la compañía bajo el alcance del ENS.

Las gráficas relacionan las salvaguardas con su estado de implantación en la compañía.

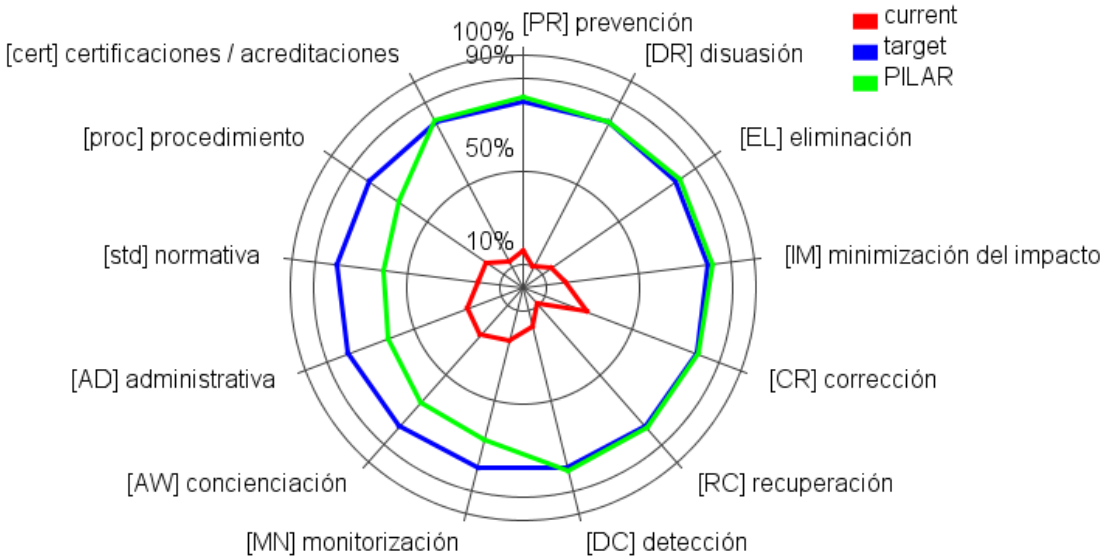


Figura 32. Gráfico salvaguardas

Lo que nos indica el gráfico es que la organización actualmente se encuentra en un nivel básico de seguridad, encontrándose por debajo del nivel objetivo en todos y cada uno de los tipos de protección que proporciona cada salvaguarda.

Los informes que PILAR ha construido permiten ver el nivel de madurez de la compañía en cuanto a los marcos de seguridad que hemos escogido para el proyecto. Los informes dejan entrever los puntos débiles de la organización, así como sus procesos más críticos, sufriendo un mayor nivel de riesgo. Las salvaguardas propuestas y el nivel estimado de adaptación de las mismas servirán de gran ayuda para tejer el plan de acción que permita a la compañía alcanzar los niveles de seguridad que han sido fijados como objetivo.

Las administraciones bajo el alcance del ENS tienen como obligación reportar su estado de "seguridad de la información" mediante los informes de PILAR al Centro Criptológico Nacional, por lo tanto, con los informes textuales que pone la herramienta a nuestra disposición, este paso quedaría cumplimentado.

3.4.7 "Evaluaciones de Impacto para la Privacidad de los Datos (EIPD)"

Tal y como se especifica en el Artículo 35 del "Reglamento General de Protección de Datos", "*ante la probabilidad de que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas será necesario llevar a cabo una EIPD antes de la puesta en marcha del tratamiento*". [18]

Una EIPD debe incluir [19]:

- Las actividades de tratamiento a realizar y su descripción detallada.
- Una relación en cuanto a la necesidad de su ejecución con "*la proporcionalidad del tratamiento respecto a su finalidad*".
- Una evaluación de los posibles riesgos derivados del tratamiento.
- Un plan de medidas destinado a mitigar los riesgos derivados, que permitan preservar la seguridad de los datos personales.

"La Agencia Española de Protección de Datos", señala que son tratamientos que requieren un EIPD, aquellos que se vean afectados por dos o más de los siguientes criterios [20]:

- "***Elaboración de perfiles***", esto es, la evaluación de situaciones relacionadas con hábitos, situaciones de salud, preferencias, desplazamientos del interesado, etc.
- "***Toma de decisiones automatizada***" con efecto significativo legal o similar.
- ***"Observación sistemática"*** para tratar de controlar o supervisar a los interesados.
- Datos sensibles (categorías especiales), esto incluiría datos relacionaos con estado de salud, localización o datos financieros.
- ***"Datos procesados a gran escala"***, entendiéndose como el volumen de datos que se manejas o el número de afectados en cifras relativas a la proporción de la población correspondiente.
- Grupos de datos que han sido cruzados.
- ***"Datos de colectivos vulnerables"***, en los que se puede incluir a niños, parte de la sociedad que necesita protección y puede ser más vulnerable y cualquier caso que pueda suponer un desequilibrio significativo entre un responsable de tratamiento y un interesado
- ***"Introducción de nuevas soluciones de naturaleza tecnológica"***, como controles de acceso por reconocimiento facial o dactilar.
- ***"Denegación de Derechos"***, cuando el interesado no pueda ejercer sus derechos por impedimento directo del responsable.

Para el caso del proyecto, se han identificado los siguientes tratamientos para los que se requiere una EIPD:

Gestión de títulos de transporte: en el que **s**e consideran de aplicación los criterios de privacidad:

→ **"Datos procesados a gran escala"**, porque se gestionan entorno 200.000 pases anuales en la ciudad de Valencia.
→ **"Colectivos vulnerables"**, puesto que existen tarjetas de transporte que están a nombre de menores.

Captación de personal: en el que se consideran de aplicación los criterios de privacidad:

→ **"Evaluación o perfilado de los candidatos"**, necesario como parte del proceso de selección de personal.
→ **"Datos de categorías especiales"**, porque se tratan datos de salud relativos a minusvalías.

Videovigilancia: en la que se consideran de aplicación los criterios de privacidad:

→ **"Observación sistemática"**, porque capta ininterrumpidamente lo ocurrido en la ubicación en la que se encuentran.
→ **"Gran escala"**, porque además de las cámaras instaladas en las ubicaciones de la compañía, también están activas las cámaras de 7 de los autobuses de los que disponen.

De esta forma, para cada una de estas actividades se ha definido una EIPD. La forma de realizar la evaluación ha seguido los siguientes pasos:

1. Identificar las amenazas que afectan a cada control de la ISO 27002 aplicable para cada tratamiento. En este paso ha sido de gran ayuda PILAR, ya que previamente ha generado un informe de amenazas que afectan a cada proceso, lo que ha facilitado mucho esta tarea. Se han tenido en cuenta un total de 36 amenazas que afectan a la "seguridad de la información".
2. El siguiente paso consiste en realizar un sumatorio de las amenazas que afectan a cada control, para así ver el promedio de amenazas por las que se ven afectados.
3. La próxima tarea consiste en evaluar las probabilidades de que un riesgo llegue a acontecer. Esto se consigue mediante la distribución de amenazas sobre cada riesgo contemplado y viendo las probabilidades de que estas lleguen a afectar. De esta forma se consigue la probabilidad de que un escenario llegue a ocurrir y el nivel de riesgo que éste tendría.
4. Por último, se elabora un mapa de calor con los riesgos contemplados, donde el eje vertical indica el impacto del riesgo y el horizontal la probabilidad de que llegue a ocurrir.

3.4.7.1 Mapa de riesgos

El resultado del EIPD nos muestra la relación impacto/probabilidad de cada uno de los procesos analizados para los siguientes riesgos:

ID	Riesgo
R.01	Exposición o fuga de información confidencial a causa de configuraciones inadecuadas de los sistemas propios de la compañía.
R.02	Pérdida de integridad de datos personales.
R.03	Indisponibilidad o saturación del sistema debido a ataques o errores de mantenimiento.
R.04	Incumplimiento de las regulaciones de privacidad porque los sistemas de información no están asegurados adecuadamente.
R.05	Incumplimiento de las regulaciones de privacidad debido a la falta de la aplicación de las prácticas de carácter legal exigidas por el RGPD.

Tabla 19. Riesgos asociados EIPD.

- **Gestión de títulos de transporte**

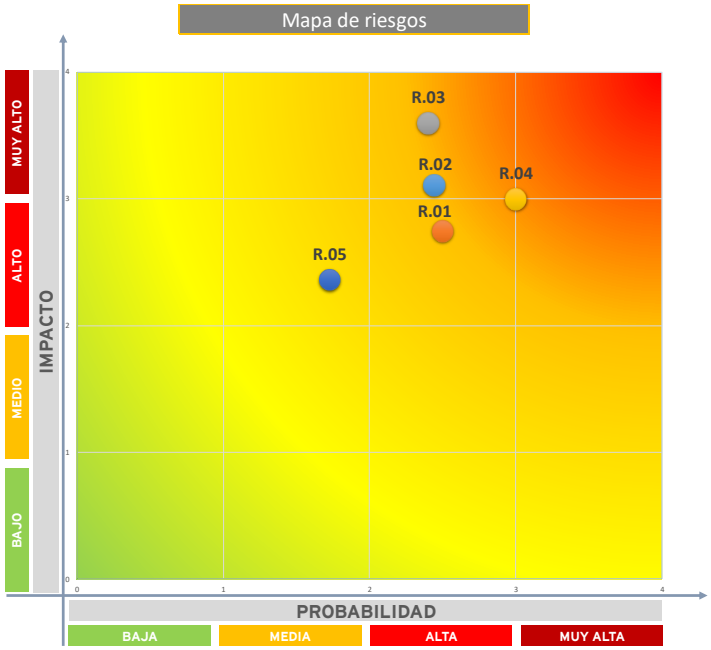


Figura 33. Mapa de riesgos gestión de títulos.

- **Captación de personal**

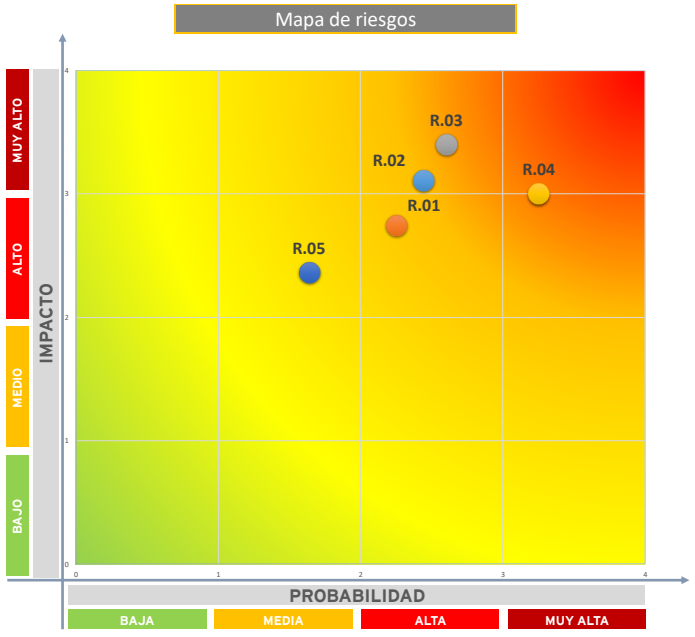


Figura 34. Mapa de riesgos Captación de personal.

- **Videovigilancia**

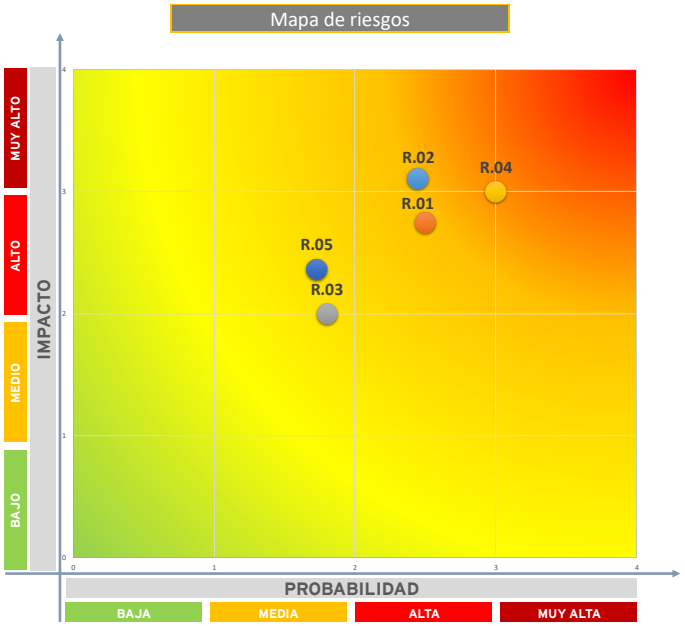


Figura 35. Mapa de riesgos Videovigilancia.

3.5 Asesoramiento en la implantación de medidas

3.5.1 Principales hallazgos

Como resultado de todo el proceso de análisis de la organización, se extraen las siguientes conclusiones sobre la situación actual:

1. Se ha identificado que **los procesos y la organización de la "seguridad de la información" en la compañía es todavía incipiente** debido a la ausencia de un equipo responsable para gestionar la "seguridad de la información".
2. Se ha identificado que **no existen medidas, políticas y normativas formales que aseguren la aplicación de medidas y criterios de seguridad únicos** para toda la compañía que permita realizar una gestión de riesgos acorde a las necesidades de negocio.
3. **Acceso no autorizado** a la información de la compañía por la falta de gestión en las autorizaciones de usuarios tales como: bajas o modificación de usuarios (revisiones de accesos, notificaciones de bajas o modificaciones de roles).
4. No existe un proceso **integración transversal de la función de "seguridad de la información"** en proyectos de todas las áreas de la compañía.
5. Ausencia de métodos **criptográficos y securización** en las comunicaciones internas.
6. Es necesario establecer una **clasificación de la información** como pilar fundamental de la "seguridad de la información" en la compañía. La ausencia de dicha clasificación no permite la aplicación de medidas proporcionales a la criticidad de la información.
7. Es **necesario establecer las medidas de seguridad que deben aplicar los proveedores**. Asimismo, se recomienda que los proveedores cuenten con certificaciones de seguridad (i.e. ISO/IEC 27001).
8. **No existe un "Plan de Continuidad de Negocio"** para garantizar que todos los procesos críticos, junto con sus sistemas, están cubiertos en su operativa para disminuir su impacto

en caso de que se produzca algún incidente que les afectara. Asimismo, se requiere la definición y test de recuperación de sistemas críticos.

El nivel de madurez recomendado por la ISO es igual a 3, mientras que, después del estudio de los controles que implementa la compañía, la organización cuenta con el siguiente nivel de madurez:

3.5.1.1 *Análisis técnico de seguridad*

Se han detectado vulnerabilidades críticas que permiten tomar el control de sistemas **con privilegios de administrador, llegando a controlar todo el dominio y comprometiendo todas sus máquinas**. Así mismo, se han detectado múltiples vulnerabilidades de riesgo alto explotables las cuales permiten obtener el control del servicio, y un gran número de vulnerabilidades de nivel medio. Por todo ello, el nivel de seguridad que presenta la red interna es de un 3.0 sobre 10.

Con ayuda del departamento de hacking ético, se han realizado diferentes pruebas técnicas con el objetivo de evaluar el nivel de seguridad de la infraestructura tecnológica externa de la compañía, así como de determinar la viabilidad de realizar ataques exitosos por parte de usuarios externos e internos.

Como resultado de las pruebas se extraen las siguientes conclusiones:

- Gran cantidad de sistemas obsoletos, que pueden poner en riesgo el resto de la infraestructura. Como Lotus Domino que, por su anticuada versión ha permitido, junto con otras vulnerabilidades, tomar el control de la máquina.
- Contraseñas débiles, que debilitan el inicio de sesión seguro debido a una mala implementación y la ausencia de mecanismos anti-automatización.

- Abuso de las funcionalidades de la aplicación a través de la ausencia de mecanismos anti-automatización, han permitido obtener credenciales válidas para servicios como Lotus Domino que más tarde han servido para vulnerar otras cuentas y sistemas.
- Escasa validación de los datos de entrada, pudiendo así realizar ataques del tipo Cross Site Scripting que puedan modificar el normal funcionamiento de los servicios web.
- Revelación de la tecnología utilizada a través de la gestión incorrecta de errores HTTP y debido a fugas de información en otros ficheros y servicios, puede permitir realizar ataques a servicios de red con vulnerabilidades o realizar ataques más complejos.
- Deficiencias en la negociación SSL, que pueden llegar a causar una denegación del servicio, así como la realización de ataques para sustraer información sobre las conexiones supuestamente seguras.
- Ejecución de código a través de la explotación de vulnerabilidades conocidas debido a la ausencia de actualización de software.
- Información sensible almacenada en claro, se han detectado múltiples documentos en carpetas de red con información sensible almacenada en claro (credenciales, DNIs, presupuestos…). Obteniendo así acceso a datos de configuración, contraseñas, maquetas de instalación y muchos otros datos sensibles.

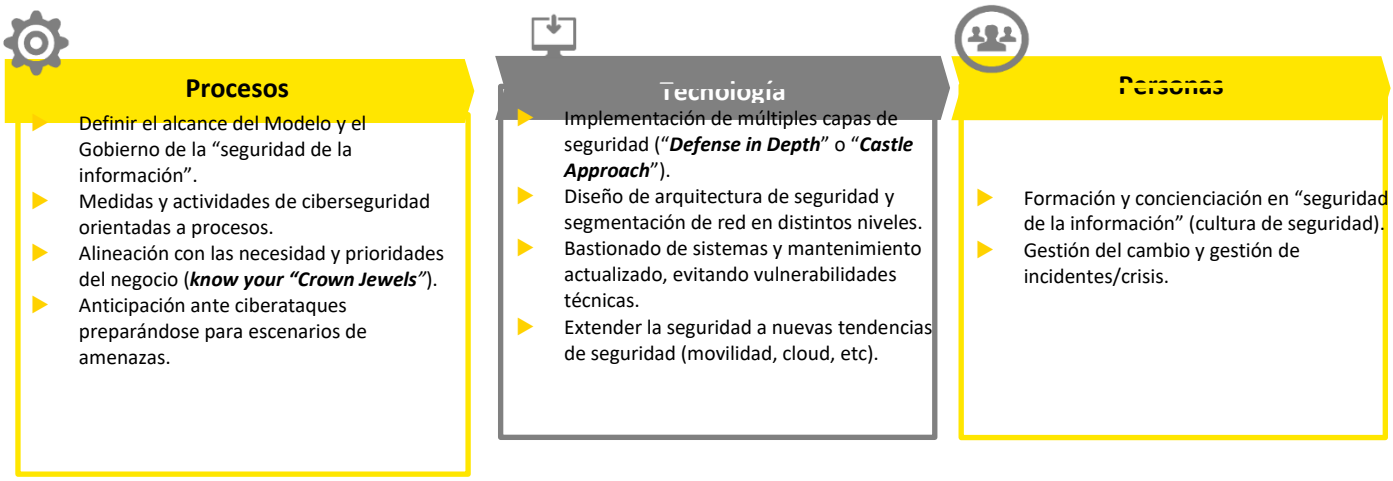
Tras el análisis de las debilidades observadas y descritas en el apartado anterior, se proponen las principales líneas de actuación que la compañía debe llevar a cabo para minimizar los riesgos identificados durante el desarrollo del trabajo:

- ✓ **Actualizar los sistemas operativos a versiones soportadas**
- ✓ **Actualizar las versiones del software** utilizado a la última versión para evitar la exposición de vulnerabilidades públicamente conocidas.
- ✓ **Aplicar los parches disponibles** para las vulnerabilidades más críticas.
- ✓ Desplegar un **sistema de correlación de eventos y/o un sistema de detección de intrusiones** que permita monitorizar la actividad generada dentro de la infraestructura.
- ✓ **Implantar una política de contraseñas robustas** en toda la organización, prohibiendo claves que sean adivinables por un atacante.
- ✓ **Eliminar todas las credenciales por defecto** de los dispositivos.
- ✓ **Revisar certificados SSL** para garantizar la confidencialidad de los datos transmitidos.
- ✓ **Utilizar software que protejan de accesos a información confidencial**, y cifrar la información sensible, en las carpetas compartidas
- ✓ **Concienciación de contraseñas seguras**, especialmente para el personal que trata información confidencial o critica.

3.5.2 Estrategia futura

Una vez conocida la estructura de la empresa y su nivel de seguridad, el siguiente paso consiste en crear un plan de acción que permita subsanar las deficiencias detectadas.

El modelo futuro se diseña para conseguir la **transformación de la "seguridad de la información"** en la compañía tomando como **base** los **tres pilares** siguientes**:**



Con esta finalidad, se ha elaborado una lista de proyectos divididos en cuatro bloques diferenciados por el coste de ejecución, tanto en tiempo como en esfuerzo económico. Además, se ha elaborado una hoja de mapeo que relaciona cada proyecto con los controles de la ISO 27002 a los que afecta.

3.5.3 Quickwins

En primer lugar, se plantean una serie de proyectos clasificados como "Quickwins", es decir, iniciativas que proporcionan un incremento rápido de los niveles de seguridad invirtiendo poco tiempo y dinero. Estos proyectos tienen una duración máxima de un año y, como norma general, la compañía podría ejecutarlos sin invertir dinero en terceros.

Se elijen una serie de medidas que cubran las necesidades más inmediatas de la compañía, no tanto a nivel de seguridad de las comunicaciones, sino más bien a nivel normativo, con el objetivo de evitar posibles sanciones por el no cumplimiento de los reglamentos a los que están obligados a adaptarse.

La lista de "Quickwins" la componen los siguientes proyectos:

ID	Proyecto	Prioridad
QW.01	Definición de la política y cuerpo normativo de la Seguridad IT.	Alta
QW.02	Definición y aplicación de una política de contraseñas robusta sobre todos los SSII de EMT Valencia.	Alta
QW.03	Formalización de la Función de Seguridad de la Información: misión y objetivos, ámbito y organización.	Alta
QW.04	Definición e implantación de un proceso de gestión de alertas e incidentes de Seguridad de la Información.	Alta
QW.05	Definición e implantación de un proceso de gestión de parches y actualizaciones de seguridad IT.	Alta
QW.06	Tests de ingeniería social (Phishing, USB, etc).	Media
QW.07	Encuesta de satisfacción y entendimiento del nivel de concienciación en Seguridad de la Información.	Baja
QW.08	Definición de un plan anual de formación y concienciación en materia de Seguridad IT.	Alta
QW.09	Definición e implantación de un procedimiento de análisis y gestión de riesgos.	Alta
QW.10	Definición e implantación de un procedimiento de revisión de usuarios en los sistemas de información críticos.	Alta
QW.11	Definición e implantación de un procedimiento de gestión del teletrabajo.	Alta

Tabla 21. Quickwins.

Con la implantación de estas medidas, el nivel de seguridad de los controles de la ISO 27002 de la empresa quedaría como muestra la siguiente figura:

Figura 36. Madurez QW.

3.5.4 Medidas a corto plazo

El siguiente bloque de mediadas comprende aquellas acciones que podrían prolongarse hasta algo más de un año vista. Sin llegar a ser medidas muy técnicas, comienzan a ser de utilidad para mejorar la "seguridad de la información". La lista de proyectos a corto plazo es la siguiente:

ID	Proyecto	Prioridad
CP.01	Plan anual de auditorías y revisiones técnicas de Seguridad de la Información.	Media
CP.02	Definición e implantación de la política de clasificación de la información.	Alta
CP.03	Diseño de solución para la de gestión de activos de información.	Alta
CP.04	Definición e implantación de un Plan de Continuidad de Negocio.	Alta
CP.05	Creación de un equipo de respuesta ante incidentes de Seguridad IT.	Media
CP.06	Definición de un proceso para incluir el área de Seguridad de la Información en la operación diaria de los procesos y proyectos IT.	Alta
CP.07	Definición de la politica de contratación, instalación e implementación de servidores y aplicaciones y la gestión de proyectos involucrando al area TIC.	Alta
CP.08	Implantación de una herramienta de gestión de dispositivos móviles (MDM) o securizar la conexión a los SSII de EMT a través de dispositivos móviles.	Alta
CP.09	Evaluación de amenzas en materia de Seguridad Física y diseño de solución para mitigar las amenazas.	Alta
CP.10	Definición e implantación de un Sistema de Gestión de Seguridad de la Información (SGSI).	Alta
CP.11	Cifrado de dispositivos y soportes extraíbles.	Alta

Tabla 22. Proyectos a corto plazo.

Figura 37. Madurez proyectos corto plazo.

3.5.5 Medidas medio plazo

Las medidas propuestas para un plazo de tiempo medio se podrían extender entre uno y tres años. La naturaleza de estas medidas es de un carácter más técnico que las anteriores, lo que supone un volumen de recursos mayor. El listado lo componen los siguientes proyectos:

ID	Proyecto	Prioridad
MP.01	Definición e implantación del nuevo modelo de arquitectura de red segura.	Alta
MP.02	Bastionado de sistemas y dispositivos informáticos.	Alta
MP.03	Definición e implantación de un modelo de reporting y cuadro de mandos integral para la función de Seguridad.	Media
MP.04	Definición e implantación de un proceso de desarrollo seguro (S-SDLC).	Media
MP.05	Definición e implantación de un programa de gestión de identidades y accesos (IAM).	Alta
MP.06	Análisis de escenarios de riesgo y definición de un Programa de Prevención de Fugas de Información.	Alta
MP.07	Definición de marco de gestión y control de proveedores y modelo de monitorización de medidas de seguridad en servicios TI.	Media
MP.08	Implantación de herramienta de protección de información sensible en BBDD.	Alta
MP.09	Cifrado de comunicaciones.	Media
MP.10	Implantación de una solución para evitar el uso de credenciales definidas en claro en el codigo en aplicaciones o scripts.	Alta

Tabla 23. Proyectos a medio plazo.

Figura 38. Madurez proyectos medio plazo.

3.5.6 Medidas largo plazo

Este tipo de medidas se prolongan desde los dos años hasta los cuatro o cinco años de duración. Son proyectos destinados a mejorar y revisar un sistema de seguridad con un nivel de madurez ya adecuado.

ID	Proyecto	Prioridad
LP.01	Firma digital y cifrado de correo electrónico (interno y externo).	Media
LP.02	Implantación de herramienta para prevención de fuga de información a través del correo electrónico	Media
LP.03	Implantación de una solución o servicio de Cyberthreat Intelligence.	Baja
LP.04	Implantación de una solución o servicio de análisis forense y cibercrimen.	Media
LP.05	Revisión y actualización del plan anual de auditorías de Seguridad de la Información.	Alta
LP.06	Revisión y actualización de materiales de soporte del Plan Anual de formación y concienciación	Alta
LP.07	Revisión y actualización de las campañas de concientización de Seguridad de la Información.	Alta
LP.08	Revisión y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).	Alta
LP.09	Revisión y mantenimiento del Plan de Continuidad de Negocio (BCP).	Alta
LP.10	Implantación de una herramienta de gestión de vulnerabilidades (SIEM), mecanismos e inteligencia para la detección de incidentes de Seguridad IT.	Alta

Tabla 24. Proyectos a largo plazo.

Figura 39. Madurez proyectos largo plazo.

Capítulo 4. Pliego de condiciones

4.1 Descripción de proyectos.

Llegado el momento de la implantación de medidas, se destacan aquellas que han de ponerse en funcionamiento de forma más urgente debido a su utilidad.

De los proyectos propuestos a la compañía destacan los siguientes como relevantes a la hora de mejorar en seguridad:

<table>
<tr><th>QW.01</th><th colspan="5">Definición de la política y cuerpo normativo de la Seguridad IT.</th></tr>
<tr><th colspan="2">Descripción y objetivos</th><th colspan="2">ISO 27002</th><th colspan="2">ENS</th></tr>
<tr><td colspan="2" rowspan="5">Para poder regular el comportamiento respecto a la “seguridad de la información” es necesario la definición y aprobación de un Cuerpo Normativo de Seguridad que proporcione el marco regulatorio de dicho aspecto, así como que dictamine el comportamiento acorde a la Política de Seguridad

El presente proyecto tiene por objetivo desarrollar la Política de Seguridad de La compañía y sus directrices de seguridad</td><td colspan="2">5 6 7
9 10 11
12 13 14
15 16 17
18</td><td rowspan="5">Marco orgnizativo
Marco operacional
Medidas de protección</td></tr>
<tr><th colspan="2">Estrategia de implantación</th><th colspan="2">Costes</th></tr>
<tr><td colspan="2" rowspan="2">Las principales acciones que realizar para ejecutar adecuadamente el proyecto son:
▪ Actualizar la Política de “seguridad de la información” por parte de la Dirección de la Compañía.
▪ Desarrollar y aprobar un Cuerpo Normativo que soporte la Política de Seguridad, definiendo las normativas de niveles inferiores, que como mínimo debería incluir los siguientes aspectos:
▪ Acceso remoto, Escritorios vacíos, Uso de equipos y dispositivos móviles, Protección del correo electrónico, Uso de Internet, Instalación de software, Seguridad del personal, Seguridad física y medioambiental, etc.
▪ Definir los procesos formales para soportar la revisión y evaluación periódica del cuerpo normativo, así como la asignación de responsabilidades específicas.
▪ Definir los mecanismos necesarios para divulgar y publicar el cuerpo normativo de seguridad a todo el Grupo.</td><td>28,5K €</td><td>2 meses</td></tr>
<tr><td>Security
470 h</td><td>Others
30h</td></tr>
</table>

<table>
<tr><th>CP.04</th><th colspan="5">Definición e implantación de un “Plan de Continuidad de Negocio”.</th></tr>
<tr><th>Descripción y objetivos</th><th colspan="3">ISO 27002</th><th colspan="2">ENS</th></tr>
<tr><td rowspan="6">El objetivo de este proyecto es identificar las necesidades de negocio para definir e implementar un plan de continuidad.

Identificar escenarios de desastre y definir las posibles estrategias de continuidad y recuperación, basadas en los requisitos de negocio (RTO y RPO: Recovery Point Objective y Recovery Time Objective).</td><td>5</td><td>6</td><td>7</td><td rowspan="6">Marco orgnizativo
Marco operacional
Medidas de protección</td></tr>
<tr><td>9</td><td>10</td><td>11</td></tr>
<tr><td>12</td><td>13</td><td>14</td></tr>
<tr><td>15</td><td>16</td><td>17</td></tr>
<tr><td>18</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><th>Estrategia de implantación</th><th colspan="5">Costes</th></tr>
<tr><td rowspan="2">Con el fin de lograr el objetivo de este proyecto, a continuación, se presentan las tareas que se recomienda desarrollar:

▪ Realizar un análisis de impacto de negocio:
▪ Identificar claramente el Proceso de Negocio de manera crítica que soporte las operaciones de La compañía incluyendo la definición de RTOs y RPOs.
▪ Obtener un entendimiento de los procesos de negocio responsable definido sobre el RTO y RPO.
▪ Identificar escenarios de desastre y sus correspondientes estrategias de recuperación para cumplir con los requisitos establecidos por la compañía.
▪ Realizar un estudio de viabilidad y analizar el coste de la estrategia.
▪ En base a la criticidad de los datos y sistemas que soportan los procesos de negocio de la organización, crear un “Plan de Continuidad de Negocio” considerando:
▪ Definir y asignar roles y responsabilidades para asegurar la correcta ejecución del plan.
▪ Definición y desarrollo de procedimientos operativos sobre contingencia y estados de recuperación.
▪ Planificación y ejecución de pruebas periódicas que garanticen, en la medida de lo posible, las funcionalidades propias de las estrategias definidas en el “Plan de Continuidad de Negocio”.
▪ Implementación de procesos, canales de comunicación y coordinación para asegurar una adecuada toma de conciencia de la estrategia de continuidad para el personal clave.

▪ Gestionar la relación con proveedores de servicios externalizados IT para garantizar que proporcionen los servicios en caso de contingencia.</td><td colspan="3"> 
53K €</td><td colspan="2"> 
3 meses</td></tr>
<tr><td colspan="3"> 
880 h</td><td colspan="2">
100 h</td></tr>
</table>

<table>
<tr><th>MP.01</th><th colspan="5">Definición e implantación del nuevo modelo de arquitectura de red segura.</th></tr>
<tr><th>Descripción y objetivos</th><th colspan="3">ISO 27002</th><th colspan="2">ENS</th></tr>
<tr><td rowspan="6">Para poder regular el comportamiento respecto a la “seguridad de la información” es necesario la definición y aprobación de un Cuerpo Normativo de Seguridad que proporcione el marco regulatorio de dicho aspecto, así como que dictamine el comportamiento acorde a la Política de Seguridad

El presente proyecto tiene por objetivo desarrollar la Política de Seguridad de La compañía y sus directrices de seguridad</td><td>5</td><td>6</td><td>7</td><td rowspan="6">Marco orgnizativo
Marco operacional
Medidas de protección</td></tr>
<tr><td>9</td><td>10</td><td>11</td></tr>
<tr><td>12</td><td>13</td><td>14</td></tr>
<tr><td>15</td><td>16</td><td>17</td></tr>
<tr><td>18</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><th>Estrategia de implantación</th><th colspan="5">Costes</th></tr>
<tr><td rowspan="2">Las principales acciones a realizar para ejecutar adecuadamente el proyecto son:

Identificar el estado actual de la arquitectura de red de EMT Valencia.

Revisar el esquema actual de la red y proponer mejoras con el objetivo de aumentar la seguridad de la red.

Realizar una segmentación de red, siguiendo las siguientes directrices:

•Definir la prioridad de cada servicio o el tiempo de respuesta que necesita el servicio, de acuerdo con el volumen de información actual.

•Instalar nuevos Firewalls intermedios.

•Crear subredes para la gestión de la administración en todas las capas de la red y reglas para permitir el acceso remoto a esta gestión.

•Habilitar / crear todas las subredes definidas en todos los Firewalls (tanto nuevos como existentes).

•Establecer un modelo de arquitectura de red en el que el que implementar controles de seguridad en cada capa

•Las reglas de firewall para la mayoría de los servicios prioritarios, o aquellos que necesitan más tiempo de respuesta, deben ser las primeras reglas (Top-Down rules).

•Potenciar un enfoque de lista blanca o híbrida, es decir, permitir el acceso a lo que sabemos que es seguro.</td><td colspan="3">25K €</td><td colspan="2">2 meses</td></tr>
<tr><td colspan="3">430 h</td><td colspan="2">60h</td></tr>
</table>

<table>
<tr><th>LP.01</th><th colspan="5">Firma digital y cifrado de correo electrónico (interno y externo).</th></tr>
<tr><th colspan="2">Descripción y objetivos</th><th colspan="3">ISO 27002</th><th>ENS</th></tr>
<tr><td colspan="2" rowspan="4">El objetivo de este proyecto es definir un modelo de gestión de los certificados digitales, adaptado a las necesidades actuales de la compañía y garantizar la seguridad de los mismos.

Además, se podría crear e implementar una Autoridad de Certificación que garantice la seguridad de las comunicaciones y mejore los procesos de autenticación de la compañía.</td><td>5</td><td>6</td><td>7</td><td rowspan="4">Marco orgnizativo
Marco operacional
Medidas de</td></tr>
<tr><td>9</td><td>10</td><td>11</td></tr>
<tr><td>12</td><td>13</td><td>14</td></tr>
<tr><td>15</td><td>16</td><td>17</td></tr>
<tr><td colspan="2"></td><td>18</td><td colspan="3"></td></tr>
<tr><th colspan="2">Estrategia de implantación</th><th colspan="4">Costes</th></tr>
<tr><td colspan="2" rowspan="2">Para alcanzar el objetivo de este proyecto, se deben realizar las siguientes tareas para crear un modelo de gestión de certificados:

Identificación y análisis del alcance de los certificados digitales y la solicitud de firma electrónica (es decir, firma electrónica corporativa, autenticación de usuario, facturación electrónica, firma de software, cifrado de correo electrónico, etc.)

Establecer un modelo de gestión de certificados digitales, que incluya:

Determinación de los tipos de certificados homologados por la compañía, así como de dispositivos / software de creación de firmas.

Desarrollo de la política de uso de controles criptográficos, los cuales deben determinar los diferentes procesos asociados, tales como: proceso de aplicación, creación / adquisición, instalación, renovación y revocación de los mismos.

Determinación del proceso de gestión del inventario de certificación. Analizar la necesidad de adquirir un módulo de seguridad de hardware (HSM) como un dispositivo físico de computación que protege y gestiona las claves digitales para la autenticación fuerte y proporciona el cripto-procesamiento.

Determinación de un repositorio centralizado de certificados, así como controles de seguridad asociados.

Análisis de factibilidad para el diseño, implementación y operación de una Autoridad de Certificación (CA) propiedad de la compañía, incluyendo diseño y análisis de costos para implementar una arquitectura PKI (infraestructura de clave pública), para la posterior implementación de una Autoridad de Certificación siguiendo las normas establecidas por la industria.</td><td colspan="3"> 
62K €</td><td> 
4 meses</td></tr>
<tr><td colspan="3"> 
1100 h</td><td>
100 h</td></tr>
</table>

Capítulo 5. Conclusiones y propuesta de trabajo futuro.

El exhaustivo estudio de la compañía en cada uno de sus procesos de negocio y sistemas de gestión de la información ha permitido tener una vista detallada de sus niveles de seguridad.

Partiendo de esa base, se han identificado las fortalezas y las debilidades de la compañía para tratar de corregir los puntos débiles que podrían desembocar en catástrofes (fuga de información, sanciones, interrupción del servicio, pérdidas económicas, ect.).

Con el objetivo de fortalecer los aspectos en los que la compañía no aplica las correctas medidas de protección se ha hecho uso de los tres reglamentos principales que se encuentran bajo el alcance de aplicación de la compañía. La convergencia de los reglamentos en un único marco de controles ha permitido realizar el análisis de seguridad de manera mucho más eficiente, pudiendo evaluar los niveles de implantación de cada uno de ellos mediante controles únicos.

El resultado del análisis sirve para detectar las deficiencias de la compañía en materia de "seguridad de la información", y junto con el análisis de riesgos realizado en PILAR obtenemos un mayor grado de conocimiento de los riesgos a los que está expuesta la compañía.

De dichos análisis se derivan medidas/propuestas diseñadas concretamente para cada uno de los dominios de seguridad a mejorar en la compañía. Cada propuesta está relacionada con los dominios de la ISO y el ENS que mejorarían al implantarse. Así pues, se ha elaborado una serie de propuestas de proyecto de inmediata implantación para subsanar los puntos que se han considerado críticos en la compañía, donde se detallan las horas a invertir en personal de seguridad y el coste económico. Todos estos proyectos dan soporte a la implantación del "Reglamento General de Protección de Datos", cuya implantación está asesorada por el equipo de abogados.

Para realizar el trabajo de asesoría se ha hecho entrega al cliente de una bolsa de horas en la que están incluidos todos los proyectos con sus respectivos costes, de este modo la compañía asesorada podrá seleccionar que medidas desea implantar atendiendo a las necesidades obtenidas del resultado del análisis.

Bibliografía

[1] Agencia Estatal, Boletín Oficial del Estado, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. «BOE» núm. 298, de 14/12/1999.
<https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>

[2] Agencia Estatal, Boletín Oficial del Estado, "Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos", «BOE» núm. 150, de 23/06/2007.
<https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352>

[3] Wikipedia, ISO/IEC 27002:2013, "Directrices del estándar".
<https://es.wikipedia.org/wiki/ISO/IEC_27002>

[4] Wikipedia, ISO/IEC 27002:2013, "Certificación".
<https://es.wikipedia.org/wiki/ISO/IEC_27002>

[5] [6] [7] [8] [9] Agencia Estatal, Boletín Oficial del Estado Reglamento (UE) 2016/679 del Parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("Reglamento General de Protección de Datos"), páginas 14-27.
<https://boe.es/doue/2016/119/L00001-00088.pdf>

[10] Privacy Regulation EU, UE "Reglamento General de Protección de Datos", Diario Oficial de la Unión Europea | L 119/1 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ("Reglamento General de Protección de Datos").
< http://www.privacy-regulation.eu/es/>

[11] Privacy Regulation EU, UE "Reglamento General de Protección de Datos", Diario Oficial de la Unión Europea | L 119/1 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 Artículo 32 UE RGDP "Seguridad del tratamiento"
< http://www.privacy-regulation.eu/es/32.htm>

[12] Centro Criptológico Nacional, "Esquema Nacional de Seguridad", "Adecuación y cumplimiento".
<https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens/adecuacion-y-cumplimiento>

[13] Centro Criptológico Nacional, "Esquema Nacional de Seguridad", "Valoración de los sistemas", página 4.
<https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf>

[14] ISO Tools, Controles de la ISO/IEC 27002.

< https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ >

[15] Centro Criptológico Nacional, "Esquema Nacional de Seguridad", "Guía de Implantación", páginas 6-7.

<https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_implantacion_del_ens.pdf>

[16] Portal de Administración electrónica, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

<https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XUv1JugzaUk>

[17] Centro Criptológico Nacional, Guía de Seguridad de las TIC, PILAR – Manual de Usuario v7.1

<https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2841-ccn-stic-470i1-pilar-manual-de-usuario-v7-1/file.html>

[18] Privacy Regulation EU, UE "Reglamento General de Protección de Datos", Artículo 35, "Evaluación de impacto relativa a la protección de datos"

<http://www.privacy-regulation.eu/es/35.htm>

[19] Agencia Española de Protección de Datos, Grupo "protección de datos" del artículo 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, Adoptadas el 4 de abril de 2017. Página 9.

< https://www.aepd.es/media/criterios/wp248rev01-es.pdf>

[20] Agencia Española de Protección de Datos, Grupo "protección de datos" del artículo 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, Adoptadas el 4 de abril de 2017. Página 10.

< https://www.aepd.es/media/criterios/wp248rev01-es.pdf>