Máster de Seguridad de las Tecnologías de la Información y de las Comunicaciones – MISTIC (interuniversitario: UOC, UAB, URV)

Universitat Oberta de Catalunya

UAB Universitat Autònoma de Barcelona

UNIVERSITAT ROVIRA i VIRGILI

Memoria Trabajo Fin de Máster

Inclusión de los sistemas de información de una organización dentro del Esquema Nacional de seguridad (ENS) en virtud del Real Decreto 3/2010

Director: Antonio José Segovia Henares
Autor: Esteban Sánchez Sánchez
06/06/2017

RESUMEN DEL TRABAJO

Español:

La presente memoria muestra el trabajo realizado para la adaptación al Esquema Nacional de Seguridad (ENS) de los sistemas de información que constituyen el núcleo del negocio en un organismo público.

Para llevarlo a cabo se han puesto en práctica todos los conocimientos en materia de análisis y gestión de la seguridad adquiridos durante la realización del Máster de Seguridad de las Tecnologías de la Información y de las Comunicaciones.

Inglés:

The present report shows the work done for the adaptation to the National Security Scheme (ENS) of the information systems that constitute the core of the business in a state organization.

In order to carry it out, all the knowledge learnt in the field of security analysis and management acquired during the Master's Degree in Information Technology and Communications Security has been put into practice.

Índice de Contenido:

Índice de Tablas:

Índice de Imágenes:

1 Introducción

El Esquema Nacional de Seguridad (en adelante ENS) se encuentra recogido en el Real Decreto 3/2010 del 8 de Enero de 2010. Dicho esquema tiene como objetivo crear las condiciones necesarias de confianza en el uso de los medios electrónicos para el ejercicio de derechos de los ciudadanos y el cumplimiento de deberes a través de estos medios.

En base a lo anterior se ha decidido en una organización incluir los servicios que forman el núcleo del negocio de dicho organismo

Para incluir dichos servicios en la gestión de la seguridad de la información de acuerdo con el ENS se ha realizado el siguiente TFM planificado en las siguientes fases:

- **Identificación de los sistemas de información**. Se identifica cada sistema y se proporciona proporciona una descripción del servicio proporcionado por el mismo.

- **Valoración de las dimensiones de seguridad de la información sistemas y servicios y categorización de los sistemas de acuerdo al ANEXO I del ENS**. Se indica para cada dimensión de la información y los servicios el motivo de la asignación de un determinado nivel de seguridad

- **Análisis de riesgos de los sistemas de información**. La metodología a usar para el análisis de riesgos ha sido Magerit y se ha llevado acabo usando la herramienta PILAR recomendada por el Ministerio. Dicho análisis ha incluido:

    - Modelado en PILAR de los activos que componen los sistemas de información. Se han identificado las categorías de los diferentes activos así como la relaciones entre ellos mediante un modelo que se adecuado para el análisis de riesgos al que se va a someter.

    - Identificación y valoración de las diferentes amenazas sobre los activos en función de su categoría

    - Selección de las diferentes salvaguardas a aplicar en base a la categoría del sistema tal y como se recoge en el ANEXO 2 así como la valoración del cumplimiento de las mismas en base a su nivel de madurez.

    - Cálculo del residual resultante de la aplicación de los controles de seguridad

- Establecimiento de un plan para la mejora de la seguridad. Dicho plan tendrá se ha divido en diferentes acciones indicando su alcance, responsable, recursos los objetivos a cumplir en cada una de ellas. Además se san usado las herramientas de análisis y modelado gráfico proporcionadas por PILAR para reflejar tanto la situación actual como la situación objetivo esperada a la finalización de dicho plan.

Así pues la presente memoria se organiza en diferentes apartados que llevan a cabo lo indicado en las diferentes fases. Dichos apartados son:

- **El Esquema Nacional de Seguridad (ENS) :** Incluye una introducción sobre los conceptos del ENS y su relación con otras normativas de seguridad

- **Entorno del proyecto:** Incluye una descripción del entorno funcional y técnico del organismo así como la identificación de los sistemas de información (SI) a analizar.

- **Valoración y categorización de los sistemas. Controles de seguridad:** En este apartado se lleva a cabo la valoración de los sistemas de información y su categorización de acuerdo con el procedimiento marcado por el ENS. A continuación se seleccionan los controles de seguridad del ENS que son de aplicación a dichos sistemas

- **Análisis de Riesgos:** En este apartado se crea en primer lugar el proyecto en PILAR que contiene el modelo de activos que componen los sistemas de información. A continuación se valoran dichos activos y se identifican y valoran las amenazas. Seguidamente se realiza una auditoría interna para identificar y valorar las salvaguardas y de esta forma estimar el riesgo residual.

- **Plan de mejora de la Seguridad:** Se describe el programa para la mejora de la seguridad incluyendo su alcance y objetivos así como las actuaciones recomendadas para reducir los niveles de riesgo al tiempo que se mejora el cumplimiento de los niveles del ENS por parte del organismo.

2 El Esquena Nacional de seguridad (ENS)

2.1 Introducción

El Esquema Nacional de Seguridad (en adelante ENS) surgió inicialmente para dar respuesta el artículo 42.2 de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Dicho esquema se articula a través del Real Decreto 3/2010 del 8 de Enero y tiene como objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Actualmente la ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común reafirma el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos a través de un entorno cuya seguridad venga determinada por el ENS.

Dentro del ENS se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. Así pues la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

2.2 Estructura y Contenido

En este apartado se resume el contenido del Real Decreto describiendo brevemente los capítulos que lo contienen así como sus Anexos los cuales sirven de guía para llevar a cabo el proceso de adecuación al ENS. Así pues El Real Decreto se estructura en diez capítulos:

Capítulo	Nombre	Descripción
I	**Disposiciones Generales**	Contiene el objeto y ámbito de aplicación del ENS indicando que están excluidos de su ámbito de aplicación los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.
II	**Principios básicos**	Incluye los 6 principios básicos que deberá tener en cuenta cualquier organización administrativa a la hora de tomar decisiones en materia de seguridad. Dichos principios son: o Seguridad Integral o Gestión de Riesgos o Prevención reacción y recuperación

		o Líneas de defensa o Reevaluación Periódica o Función diferenciada
III	**Requisitos mínimos**	El ENS establece que todas las Administraciones Públicas deberán contar con una Política de Seguridad basada en los principios anteriores y que además dicha política deberá desarrollarse aplicando los siguientes requisitos mínimos: o Organización e implantación del proceso de seguridad. o Análisis y gestión de los riesgos. o Gestión de personal. o Profesionalidad. o Autorización y control de los accesos. o Protección de las instalaciones. o Adquisición de productos. o Seguridad por defecto. o Integridad y actualización del sistema. o Protección de la información almacenada y en tránsito. o Prevención ante otros sistemas de información interconectados. o Registro de actividad. o Incidentes de seguridad. o Continuidad de la actividad. o Mejora continua del proceso de seguridad. El ENS también indica en este capítulo que estos requisitos mínimos se exigirán siempre de forma proporcional a los riesgos identificados en cada sistema lo cual se traduce en el hecho de que algunos de ellos no serán de obligado cumplimiento en

		determinados sistema siempre que quede debidamente justificado en base a los riesgos a los que está expuesto dicho sistema.
IV	**Comunicaciones electrónicas**	En este capítulo del ENS se propone como la guía que debe seguirse para implementar las condiciones técnicas de seguridad no sólo en las comunicaciones electrónicas sino en los mecanismos de firma electrónica.
V	**Auditoría de la seguridad**	La implantación del ENS en una organismo público conlleva la implantación de un sistema de Gestión de la Seguridad de la Información (en adelante SGSI) sujeto a un proceso cíclico de mejora continua en el que las actividades de auditoría juegan un papel crucial para llevar a cabo dichas mejoras. Así pues en este capítulo se establecen los diferentes tipos y niveles de auditoría a realizar dentro del ENS en base a la categoría del sistema. Las auditorías se llevarán a cabo mediante criterios, métodos de trabajo y de conducta generalmente reconocidos a nivel nacional e internacional.
VI	**Estado de seguridad de los sistemas**	El Comité Sectorial de Administración Electrónica es el encargado de articular los procedimientos necesarios para recoger información sobre el estado de implantación del ENS en los diferentes organismos públicos. Actualmente dicha recogida de información es llevada a cabo mediante la cumplimentación por los diferentes organismos de un cuestionario con preguntas sobre la seguridad en su institución. Los resultados de dicho informe se usan para crear el Informe Nacional sobre el Estado de la Seguridad (INES) que da una idea del estado de seguridad en las Administraciones Públicas.
VII	**Respuesta a incidentes de seguridad**	El proceso de respuesta a incidentes de seguridad es otro de los aspectos claves para hacer frente a los incidentes de seguridad que lleguen a materializarse dentro de una entidad. Cada organismo público debe tratar dichos incidentes a través de un proceso de respuesta que incluirá informar de los más graves al Equipo de Respuesta ante Incidentes de Seguridad del Centro Criptológico Nacional (en adelante CCN-CERT). El CCN-CEERT articula de esta forma la respuesta ante incidentes de seguridad entre diferentes Administraciones Públicas. Además de esta responsabilidad, en este capítulo se le atribuyen otras como la de Informar sobre vulnerabilidades o la de formación en materia de seguridad al personal de las Administraciones.
VIII	**Normas de conformidad**	Se indica que la seguridad en base al ENS estará presente tanto en las sedes como los registros electrónicos, así como en el ciclo de vida de los diferentes servicios y sistemas los cuales deberán incluir los mecanismos de control adecuados. El cumplimiento de todo lo anterior se hará visible mediante la expedición de

		certificaciones de seguridad.
IX	**Actualización**	Se pone de manifiesto lo que se ha comentado anteriormente de la necesidad de un ciclo continuo de mejora de la seguridad de forma que la seguridad no sea vista como algo puntual sino como algo vivo y sujeto al cambio. Por ello que es necesario la actualización permanente de las medidas y capacidades de seguridad de forma que s epoda hacer frente a las nuevas amenazas que puedan surgir.
X	**Categorización de los sistema de información**	Se indica que se establecerá una clasificación de los sistemas de información por categorías en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad.

Tabla 2-1. Capítulos del RD 3/2010

En los 3 anexos siguientes a estos capítulos, el ENS introduce los procedimientos para la selección de los elementos comunes que han de guiar la actuación de las Administraciones Públicas en materia de seguridad de las Tecnologías de la Información. Para ello se usan tres “herramientas” o conceptos:

- **Las dimensiones de la seguridad y sus niveles. (Anexo I)**

  Definen los distintos aspectos que abarca la seguridad de un sistema de información. Para un análisis de cualquier sistema o servicio, se deben evaluar estas cinco dimensiones.

  - **Disponibilidad:** la información y los servicios deben estar accesibles según las necesidades de la organización.
  - **Autenticidad:** una entidad es quien dice ser.
  - **Integridad:** El activo no se ha alterado de forma no autorizada.
  - **Confidencialidad:** la información o servicio sólo debe estar disponible para los autorizados.
  - **Trazabilidad:** se controlan las actuaciones de una entidad y se le pueden imputar (también se le denomina “no repudio”).

  Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles: Bajo, Medio o Alto. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel:

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

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

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

- **La categorización de los sistemas (Anexo I)**

  En base a los valores asignados a las dimensiones de seguridad de los sistemas se categorizará el sistema de información en una de las siguientes categorías:

  - **Categoría Alta:** Un sistema de información será de categoría Alta si alguna de sus dimensiones de seguridad alcanza el nivel Alto.

  - **Categoría Media:** Un sistema de información será de categoría Media si alguna de sus dimensiones de seguridad alcanza el nivel Medio, y ninguna alcanza un nivel superior.

  - **Categoría Básica**: Un sistema de información será de categoría básica si alguna de sus dimensiones de seguridad alcanza el nivel básico, y ninguna alcanza un nivel superior.

- **La selección de las medidas de seguridad. (Anexo II)**

  Son necesarias para lograr el cumplimiento de los principios básicos de seguridad y los requisitos establecidos. Se dividen en tres grupos:

  - **Organizativas** (4 medidas en total): se refieren a la organización global de la seguridad.

  - **Operacionales** (31 medidas): son para la protección de la operación del sistema (control de acceso, explotación, continuidad, etc.)

  - **De protección** (40 medidas): se centran en proteger activos concretos (instalaciones, personal, equipos, comunicaciones, etc.)

  No todas se aplican globalmente, sino que en muchos casos son de aplicación en función de la categorización que se haya hecho del sistema. Por eso, es necesario reflejar en un documento cuáles de estas medidas son de aplicación en nuestro sistema.

- **La auditoría de seguridad (Anexo III)**

  Establece 2 tipos de auditorías en función de la categoría del sistema:

  - **Auditoría a sistemas de categoría Básica**

    No necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.

  - **Auditoría a sistemas de categoría Media o Alta**
    Si será necesario un informe de auditoría el cual dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas

2.3 Modificaciones del ENS

El Real Decreto 951/2015, de 23 de octubre introdujo una serie de modificaciones del Real Decreto 3/2010 entre las cuales podemos destacar las siguientes:

- Se definen las siguientes Instrucciones Técnicas de Seguridad las cuales son de obligado cumplimiento por las Administraciones pública:
  - Informe del estado de la seguridad.
  - Notificación de incidentes de seguridad.
  - Auditoría de la seguridad.
  - Conformidad con el Esquema Nacional de Seguridad.
  - Adquisición de productos de seguridad.
  - Criptología de empleo en el Esquema Nacional de Seguridad.
  - Interconexión en el Esquema Nacional de Seguridad.
  - Requisitos de seguridad en entornos externalizados.
- Se incluye la necesidad de adecuar los sistemas de identificación electrónica existentes actualmente a los previstos en el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

- Se obliga en los sistemas de nivel Medio al uso de al de al menos 2 factores de autenticación (Antes no se recomendaban claves concertadas pero no se decía explícitamente que no se pudiesen usar como único factor de autenticación)

- En as medidas de seguridad de firma electrónica se introduce el término de certificado cualificado en línea con el Reglamento nº 910/2014

- Se concreta el papel del CCN-CERT como coordinador y referencia en los temas de seguridad para las AAPP (elaboración de ITS, coordinador de incidentes, recolección de información de incidentes, recopilación sobre el estado de implantación en las AAPP, etc.), eliminando alguna referencia que había al INTECO en la versión 1.

2.4 Relación del ENS con las normas ISO 27001 e ISO 27002

Para la mejora continua de la seguridad se puede aplicar un modelo de ciclo de mejora continua del tipo Plan-Do-Check-Act (PCDA) para lo cual la normalización voluntaria ofrece herramientas como la norma UNE ISO/IEC 27001:2013 “Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2013)”. Dicha norma contiene los requisitos para la construcción (y ulterior certificación, en su caso) de un Sistema de Gestión de Seguridad de la Información y es una norma internacional certificable y de carácter voluntario para cualquier sistema de gestión de seguridad de la información.

En el Anexo A de esta norma se enumeran los controles que desarrolla la norma ISO 27002:2013 y que incluyen un conjunto de controles de seguridad para sistemas de información genéricos. Su cumplimiento se evidencia mediante una certificación, expedida por una entidad certificadora y previa auditoría con resultado satisfactorio

Por otro lado el ENS es una disposición de carácter legal, de obligado cumplimiento para los sistemas de información del ámbito de aplicación de las Administraciones Públicas. Como ya se ha comentado el ENS incluye en su Anexo II las medidas de seguridad aplicables. Muchas de estas medidas coinciden con los controles de la ISO 27002. No obstante el ENS es más preciso y establece un sistema de protección proporcionado a la información y servicios a proteger para racionalizar la implantación de medidas de seguridad y reducir la discrecionalidad. La ISO 27002 carece de esta proporcionalidad, quedando a la mejor opinión del auditor que certifica la conformidad con la ISO 27001. Además el ENS contempla diversos aspectos de especial interés en relación con la protección de la información y los servicios de administración electrónica (por ejemplo, aquellos relativos a la firma electrónica) no recogidos en la ISO 27002.

En cuanto al cumplimiento, en el caso del ENS se evidencia mediante una declaración de conformidad legal, previa auditoría con resultado satisfactorio. En la siguiente tabla se resumen las diferencias entre ambas normativas en diferentes ámbitos

	ISO 27001/27002	ENS
Ontología	Norma internacional de seguridad, sin rango legal.	Regulación legal de carácter estatal, perteneciente al ordenamiento jurídico español derivado de la Ley 11/2007.
Carácter	certificación voluntaria	cumplimiento obligatorio
Ámbito de aplicación	Para cualquier sistema de gestión de seguridad de la información.	Para los sistemas de información de las Administraciones públicas comprendidos en el ámbito de aplicación de la Ley 11/2007.
Modulación de las medidas	Según criterio del auditor	Regulado en función de los tipos de activos y los niveles de seguridad requeridos
Evidencia de cumplimiento o conformidad	Mediante certificación, expedida por un auditor autorizado, previa auditoría con resultado satisfactorio	Mediante declaración de conformidad legal, previa auditoría con resultado satisfactorio.

Tabla 2-2. Diferencias entre ISO27001 y ENS

Por tanto, el Esquema Nacional de Seguridad y las citadas normas ISO difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen. El ENS que trata la 'protección' de la información y los servicios, contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión el cual podría implantarse en base a la ISO27001.

No obstante cabe señalar que aquellas organizaciones que se encuentren certificadas contra ISO 27001 tienen una buena parte del camino recorrido para lograr su conformidad con el ENS, toda vez que las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional. Con esta idea es con la que el CCN-CERT ha publicado la guía de seguridad CCN-STIC 825 titulada "Esquema Nacional de Seguridad Certificaciones 27001". Dicha guía tiene como objetivos:

- Por un lado explicar la utilización de una certificación 27001 como soporte de cumplimiento del ENS

- Por otro determinar qué controles de la norma 27002 son necesarios para el cumplimiento de cada medida del Anexo II y, en su caso, qué elementos adicionales son requeridos. Es decir, si el organismo tiene una certificación 27001 y se han cubierto los controles referenciados de la 27002, con incorporar lo adicional se puede considerar cumplido el Anexo II del ENS

3 Entorno del proyecto

3.1 Introducción

La administración pública a la que se le va a aplicar el ENS será una Universidad pública ficticia que se conocerá como Universidad pública de Rocagorda (en adelante UPRG). Dicha Universidad cuenta con unos 5000 alumnos y proporciona enseñanzas en el campo de las humanidades y nuevas tecnologías. Recientemente equipo rector de dicha Universidad ha sido requerido para la implantación del ENS en cumplimiento del Real Decreto. Mi objetivo será llevar a cabo la implantación del esquema del esquema siguiendo los principios y requisitos fijados por el ENS.

En la siguiente imagen se muestra el organigrama de la Universidad:

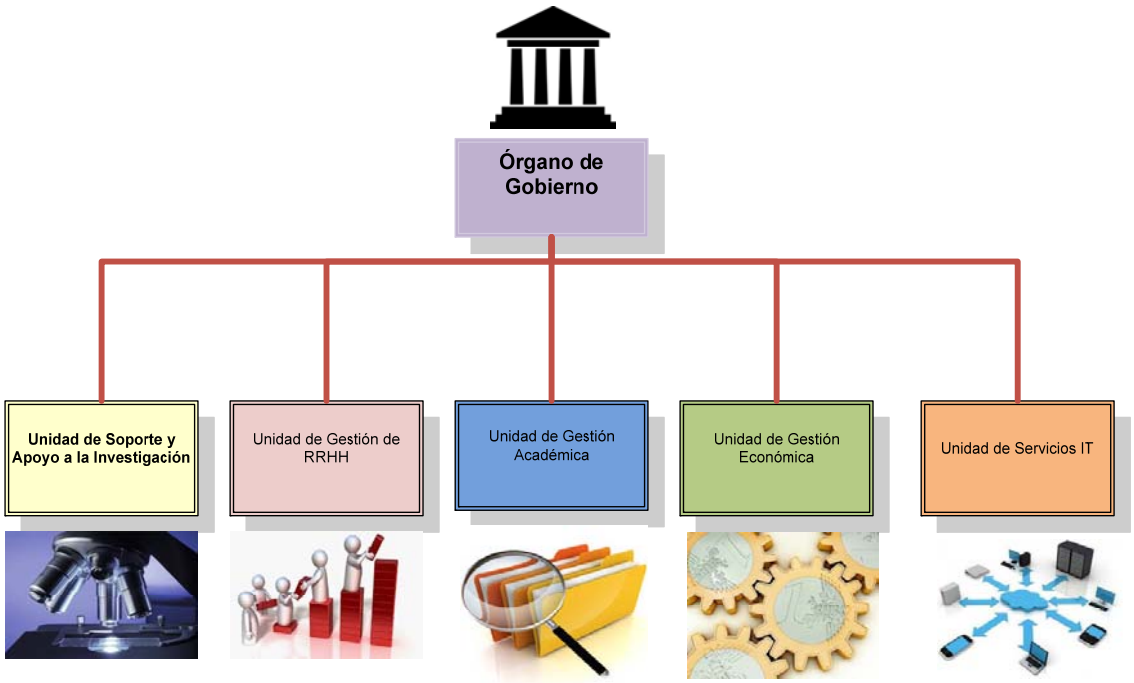

Ilustración 3-1. Organigrama de la UPRG

Como se puede observar existe un Órgano de Gobierno Central del que dependen diferentes Unidades Administrativas y de gestión. Estas Unidades permiten el cumplimiento del objetivo final de la Universidad que consiste de la prestación de los servicios públicos de la educación superior. Todos estos servicios se componen de una ser de procedimientos que son soportados por diferentes tecnologías de la información las cuales son proporcionadas y gestionadas por la Unidad de servicios IT. Estos servicios IT son transversales al resto de unidades Administrativas permitiendo alcanzar los objetivos de forma más eficaz y eficiente. Además el reconocimiento del derecho de los ciudadanos a relacionarse con la Administraciones Públicas por medios electrónicos ha llevado a que muchos de los servicios proporcionados por dichas unidades sean proporcionados dentro del marco de la Administración Electrónica con la consiguiente obligación del cumplimento del ENS antes mencionada.

Las aplicaciones informáticas que dan soporte a las Unidades Administrativas siguen todas la misma arquitectura que es la que se muestra en la imagen

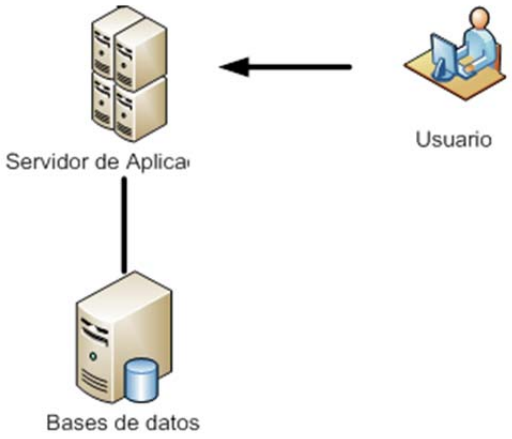

Ilustración 3-2.Arquitectura TI General

Se trata de una arquitectura donde existen servidores de aplicaciones que proporcionan el frontal web y la lógica de negocio de las aplicaciones. La información manejada por las aplicaciones web se almacena en servidores de bases de datos. Cuando se aborde el modelado de los activos en PILAR se profundizará en los activos que componen la arquitectura

3.2 Servicios e Información

El primer paso a realizar en todo este proceso de adecuación al ENS consistirá en identificar los sistemas de información en base a los activos más valiosos en toda entidad que son los servicios ofrecidos (a través de las aplicaciones e infraestructura de TI) y la información tratada por los mismos. Se han identificados los siguientes Servicios e información tratada en los mismos:

- **SERVICIO: Gestión Académica**

  Tiene como finalidad gestión del expediente académico de los alumnos de la UPRG. Sus funciones, entre otras son las de gestión de matrícula, gestión de actas, gestión de la emisión de títulos oficiales,…

  Este servicio es accedido por personal de Administración y Servicios (en adelante PAS), concretamente por el personal dedicado a la gestión académica, así como por el Personal Docente e Investigador (en adelante PDI), y por la información contenida en él es accedida por el propio alumno, principalmente para consulta.

  Información almacenada:

  - Datos identificativos de los alumnos
  - Datos del expediente académico en curso
  - Becas y datos de la unidad familiar de los alumnos
  - Títulos obtenidos

- Datos económicos de matrícula.

- **SERVICIO: Gestión Económica**

  El servicio de Gestión Económica tiene como finalidad gestión de la actividad presupuestaria y el gasto de la UPRG. Sus funciones, entre otras son las de gestión de proveedores, gestión económica y presupuestaria, gestión de las unidades de gasto,…

  Este servicio es accedido por PAS, concretamente por el personal dedicado a la gestión económica, así como por PDI con privilegios concretos.

  Información almacenada:

  - Datos de proveedores
  - Datos de personal (dietas, …)
  - Gestión económica y presupuestaria
  - Unidades de gasto (control presupuestario de la ejecución), …

- **SERVICIO: Gestión RRHH**

  El servicio tiene como finalidad gestión de los recursos humanos de la UPRG. Sus funciones, entre otras son las de gestión del personal, gestión de la jornada laboral, gestión de nóminas internas y externas, gestión de bajas,…

  Este servicio es accedido por PAS, concretamente por el personal dedicado a la gestión de recursos humanos, así como por PDI con privilegios concretos. La información contenida en él es accedida en algunos casos a través del servicio ERP – Portal, principalmente para consulta.

  Información almacenada:

  - Datos de proveedores
  - Datos de personal (dietas, …)
  - Gestión económica y presupuestaria
  - Unidades de gasto (control presupuestario de la ejecución), …

- **SERVICIO: Investigación**

Tiene como finalidad gestión investigación, el desarrollo y la innovación en la UPRG. Sus funciones, entre otras son las de gestión del personal investigador, gestión del expediente investigador, gestión de proyectos de investigación, gestión de patentes, gestión de empresas colaboradoras…

Este servicio es accedido por PAS, concretamente por el personal dedicado a la gestión económica, así como por PDI.

Información almacenada:

- Datos identificativos de los investigadores
- Grupos de investigación
- Méritos investigadores (publicaciones, congresos, referencias …)
- Proyectos de investigación (metadatos, datos de gestión)
- Convocatorias de proyectos
- Patentes
- Datos de empresas colaboradoras, …

- **SERVICIO: Sede Electrónica**

  El servicio Sede Electrónica tiene como finalidad ser interfaz de acceso unificado a los servicios de Administración Electrónica prestados por la UPRG: tablón, registro telemático

  Información almacenada:

  El servicio de AE - Sede Electrónica no almacena información significativa más allá de los enlaces e informaciones generales de los diferentes servicios a los que enlaza**.**

- **SERVICIO: Tablón Oficial**

  Es el servicio de publicación electrónico de información oficial de la Universidad

  Información almacenada:

  La información almacenada en el servicio es información pública y abierta: becas, ayudas, convocatorias de empleo, procesos de admisión…

- **SERVICIO: Registro electrónico y tramitación**

Tiene como finalidad la digitalización del proceso administrativo dentro del servicio de administración electrónica, permitiendo al ciudadano y a los miembros de la comunidad universitaria la ejecución de trámites electrónicos que requieran de procesos de verificación y autenticidad de su identidad.

Información almacenada

Debido a la naturaleza misma de un Registro General la información contenida en el mismo tiene alta heterogeneidad, pudiendo estar relacionada con cualquiera de los ámbitos en los que la Organización participa, así como en cualesquiera otros en los que esporádicamente pudiera participar.

3.3 Sistemas de Información

El criterio aplicado ha partido de la interrelación existente entre servicios, creando agrupaciones lógicas según su nivel de integración y la relación funcional entre los mismos. Han sido identificados un total de 2 sistemas. Son los siguientes:

- **Sistema ERP Institucional:** Este sistema agrupa, como indica su nombre, todos los servicios relacionados con la gestión de recursos institucionales. Estos servicios, anteriores a la aparición de las sedes electrónicas, conforman el grueso de la administración electrónica tradicional existente en las universidades españolas: gestión académica, económica, RRHH e investigación

- **Sistema de Administración Electrónica:** Este sistema agrupa todos los servicios que se prestan a partir de la sede electrónica y que están relacionados con la ley 39/2015.

A continuación se recoge la matriz que asocia los servicios con los sistemas identificados:

Sistema	Servicio
Sistema ERP Institucional	ERP – Académico
Sistema ERP Institucional	ERP – Económico
Sistema ERP Institucional	ERP – RRHH
Sistema ERP Institucional	ERP – Investigación
Sistema AE	AE – Sede
Sistema AE	AE - Tablón Oficial
Sistema AE	AE – Registro telemático y tramitación

Tabla 3-1. Agrupación de servicios por Sistema

4 Valoración y categorización de los sistemas. Controles de seguridad

Con frecuencia, el valor del sistema en materia de seguridad se concentra en unos pocos activos que son la esencia y razón de ser del sistema, y en unas pocas dimensiones. Es conveniente centrarse en aquellos activos y en aquellas dimensiones en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante. Conviene comenzar por los activos de tipo información, valorando en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel.

Conviene seguir con los activos de tipo servicio, valorando en este orden: disponibilidad, autenticidad y trazabilidad. Los requisitos en materia de confidencialidad e integridad suelen venir impuestos por la información que maneja el servicio, heredándose los establecidos en el párrafo anterior. El sistema queda valorado por los valores máximos de la información que maneja y los servicios que presta Estos principios están recogidos en la metodología de valoración descrita en el Anexo I del ENS y que trata sobre las dimensiones de la seguridad y sus niveles así como la categorización de los sistemas de información. Como ya se ha explicado anteriormente la categoría del sistema se calcula, a su vez, en función del nivel de seguridad en cada dimensión. Tanto las dimensiones de seguridad como los niveles y categorías y su interrelación se han comentado en el apartado 2.2 del presente TFM por lo que se recomienda su lectura previa para tener claros estos conceptos antes de continuar leyendo.

No obstante el Anexo I del ENS aunque establece el proceso de determinación de niveles y categorías no entra en detalle sobre los criterios para determinar el nivel de seguridad requerido en cada dimensión. Es por ello que el CCN-CERT decidió publicar la guía CCN-STIC 803 titulada “Esquema Nacional de Seguridad Valoración de los sistemas”. En dicha guía se analizan los elementos esenciales: información y servicios, estableciendo en base a ellos los criterios que el responsable de cada información y cada servicio podrá utilizar. Se ha usado por tanto dicha guía para la valoración de la información y los servicios que se desarrolla en los apartados siguientes. El número de criterios se encuentra dividido en base a las dimensiones de seguridad y debido a su amplitud se ha decido no incluirlo en el presente documento. Únicamente se resumen en las siguientes tablas los criterios generales seguidos para la valoración de la información y los servicios (el lector puede no obstante a acudir a dicha guía para consultar todos los criterios seguidos)

Dimensión	Criterios Generales para valorar la información	Criterios Generales para valorar los Servicios
Confidencialidad	El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.	

Integridad	El nivel de seguridad requerido en el aspecto de integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información	Los requisitos de integridad sobre un servicio derivan de la información que maneja. Esto incluye la posibilidad de que la información quede en un estado impropio porque el servicio no se complete adecuadamente.
Autenticidad	El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.	El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que el servicio fuera usado por personas indebidamente autenticadas; o sea, por personas que no son quienes se cree que son
Trazabilidad	El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.	El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido al servicio.
Disponibilidad	El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.	El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera usar al servicio cuando lo necesita.

Tabla 4-1. Criterios Generales de Valoración de la Información y los Servicios

4.1 Valoración de las dimensiones de seguridad

4.1.1 Sistema ERP Institucional - Servicio de Gestión Académica

4.1.1.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	Bajo	Información de uso interno para un grupo de Personal de Administración y Servicios (PAS). Sin autorización explícita. Contiene datos personales de nivel bajo.
Integridad	**Medio**	**Daños importantes, aunque subsanables. El principal riesgo es la emisión de títulos auténticos con información falsa.**
Autenticidad	Bajo	La falsedad en el origen o el destinatario causaría algún tipo de perjuicio.
Trazabilidad	Bajo	La ausencia de trazabilidad dificultaría la subsanación de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días. Excepcionalmente, en

		periodos de matrícula y actas deberá ser de menos de 1 día.

Tabla 4-2. Servicio de Gestión Académica. Valoración de la Información

La información de gestión académica no tiene riesgos especiales en cuanto a disponibilidad y confidencialidad. Por la naturaleza de la información: datos académicos, no presenta un riesgo especialmente sensible en cuanto a su difusión. Así mismo el servicio no es un servicio crítico de la organización, salvo en periodos muy concretos. El principal riesgo es la modificación de la información para la obtención de un título auténtico en base a datos modificados fraudulentamente.

4.1.1.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Bajo	Servicio de intranet, autenticado.
Integridad	**Medio**	**Equiparado a la información.**
Autenticidad	**Medio**	**Afecta a procesos de gestión y a la gestión de datos identificativos.**
Trazabilidad	Bajo	La ausencia de trazabilidad dificultaría la subsanación de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días. Excepcionalmente, en periodos de matrícula y actas deberá ser de menos de 1 día.

Tabla 4-3. Servicio de Gestión Académica. Valoración del Servicio

El servicio de gestión académica está estrechamente relacionado con la información que contiene, presentando unos niveles equivalentes. Adicionalmente debido a la integración entre servicios y al uso de tecnologías SSO, la autenticidad del servicio y de sus usuarios es fundamental para el mantenimiento de la seguridad en la organización.

4.1.2 Sistema ERP Institucional - Servicio de Gestión Económica

4.1.2.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	Bajo	Información de uso interno, menos sensible que la información académica o de RRHH. La información presupuestaria es de naturaleza pública.
Integridad	**Medio**	**Daño económico apreciable para la entidad en caso de modificación de la misma.**
Autenticidad	**Medio**	**La falsedad de la información causaría perjuicios apreciables. Equiparable a la integridad.**
Trazabilidad	Bajo	Dificultaría el seguimiento de delitos y la corrección de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días. Excepcionalmente: <1d

Tabla 4-4. Servicio de Gestión Económica. Valoración de la Información

La información de gestión económica no tiene riesgos especiales en cuanto a disponibilidad y confidencialidad. Por la naturaleza de la información: datos económicos de una AAPP, no presenta un riesgo especialmente sensible en cuanto a su difusión. Así mismo el servicio no es un servicio de disponibilidad crítica, salvo en periodos muy concretos. El principal riesgo es la modificación de información que permita el desvío económico de fondos.

4.1.2.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Bajo	Servicio de intranet. Autenticado para un colectivo concreto.
Integridad	**Medio**	**Equiparable a la información.**
Autenticidad	**Medio**	**Afecta a procesos de gestión y permite el acceso a datos identificativos.**
Trazabilidad	Bajo	Dificultaría el seguimiento de delitos y la corrección de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días. Excepcionalmente: <1d

Tabla 4-5. Servicio de Gestión Económica. Valoración del Servicio

El servicio de gestión económica está estrechamente relacionado con la información que contiene, presentando unos niveles equivalentes. Adicionalmente debido a la integración entre servicios y al uso de tecnologías SSO, la autenticidad del servicio y de sus usuarios es fundamental para el mantenimiento de la seguridad en la organización.

4.1.3 Sistema ERP Institucional - Servicio de Gestión de RRHH

4.1.3.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	**Medio**	**Existencia de información relacionada con gestión de bajas del personal, así como de su información económica. Datos de personales de minusvalía y afiliación sindical para pago de nóminas.**
Integridad	Bajo	Daño económico a individuos concretos y múltiples protestas individuales.
Autenticidad	Bajo	La falsedad de la información causaría perjuicios.
Trazabilidad	Bajo	Dificultaría el seguimiento de delitos y la corrección de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días.

Tabla 4-6. Servicio de Gestión de RRHH. Valoración de la Información

El principal aspecto de riesgo de la información contenida en el sistema de recursos humanos es su confidencialidad, debido a datos médicos, para la gestión de bajas y datos de perfil económico. El resto de dimensiones tienen una importancia baja, debido a que los errores serían subsanables de forma sencilla y las protestas no superarían el ámbito individual.

4.1.3.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Bajo	Servicio de Intranet a un determinado colectivo.
Integridad	Bajo	Equiparación con información.
Autenticidad	**Media**	**Afecta a procesos de gestión y acceso a datos identificativos.**
Trazabilidad	Bajo	Dificultaría el seguimiento de delitos y la corrección de errores.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días.

Tabla 4-7. Servicio de Gestión de RRHH. Valoración del Servicio

El principal aspecto de riesgo del servicio de recursos humanos es la autenticidad del servicio, en relación a su integración con el resto de componentes de la organización, así como a la posibilidad de que una suplantación en su autenticidad derive en una obtención de credenciales.

4.1.4 Sistema ERP Institucional - Servicio de Investigación

4.1.4.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	Bajo	Información interna. Podría causar un perjuicio su publicación.
Integridad	Bajo	Daño económico leve. Perjuicio a determinadas personas.
Autenticidad	Bajo	Protestas individuales. Perjuicio leve.
Trazabilidad	Sin valorar	Fácilmente subsanable.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días.

Tabla 4-8. Servicio de Gestión de RRHH. Valoración de la Información

Ni la información, ni por su uso puede ser considerado un servicio crítico para la organización, estando sus dimensiones en un nivel bajo.

4.1.4.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Bajo	Servicio de Intranet. Prestado a PDI y PAS determinado.
Integridad	Bajo	Equiparable a información.
Autenticidad	**Medio**	**Integración SSO.**
Trazabilidad	Sin valorar	Fácilmente subsanable.
Disponibilidad	Bajo	La disponibilidad común es de 1 a 5 días.

Tabla 4-9. Servicio de Gestión de RRHH. Valoración del Servicio

Al igual que para el caso de la información no puede ser considerado un servicio crítico para la organización, estando sus dimensiones en un nivel bajo, trasladando esa valoración al servicio. El aspecto más crítico del servicio es la integración con el ERP y por tanto el uso de credenciales únicas compartidas en otras áreas de la organización.

4.1.5 Sistema AE- Sede Electrónica

4.1.5.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	Sin valorar	Web pública donde se relacionan los servicios de AE.
Integridad	**Medio**	**Daño importante / Incumplimiento Ley 40/2015 art.38.2**
Autenticidad	**Medio**	**Daño importante aunque subsanable**
Trazabilidad	Sin	Errores fácilmente reparables.

	valorar	
Disponibilidad	**Medio**	**El valor del Objetivo de Tiempo de recuperación (RTO) tenderá un valor menor a 1 día**

Tabla 4-10. Servicio de Sede Electrónica. Valoración de la Información

Tanto por los daños a la imagen, como los riesgos derivados de la modificación de la información existente en ella, pudiendo sufrir ataques de suplantación de identidad o de robo de credenciales, la integridad y la autenticidad de la sede electrónica son aspectos fundamentales. Paralelamente su tiempo de recuperación debe ser inferior a un día.

4.1.5.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Sin valorar	Web pública donde se relacionan los servicios de AE.
Integridad	**Medio**	**Daño reputacional significativo**
Autenticidad	**Medio**	**Daño reputacional significativo**
Trazabilidad	Bajo	Dificultad de perseguir delitos.
Disponibilidad	**Medio**	**Aceptable 4h-1d. El resto de la plataforma es independiente.**

Tabla 4-11. Servicio de Sede Electrónica. Valoración del Servicio

Tanto por los daños a la imagen, como los riesgos derivados de la modificación de la información existente en ella, pudiendo sufrir ataques de suplantación de identidad o de robo de credenciales, la integridad y la autenticidad de la sede electrónica son aspectos fundamentales. Paralelamente su tiempo de recuperación debe ser inferior a un día.

4.1.6 Sistema AE – Tablón Oficial

4.1.6.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	Sin valorar	Información pública
Integridad	**Medio**	**Daño importante / Incumplimiento Ley 40/2015 art.38.2**
Autenticidad	**Medio**	**Daños importantes aunque subsanable.**
Trazabilidad	Bajo	Dificultaría la subsanación de errores
Disponibilidad	**Medio**	**Inferior a 1 día.**

Tabla 4-12. Servicio de Tablón oficial. Valoración de la Información

Las dimensiones críticas para la información contenida en el servicio Tablón oficial son la integridad, la autenticidad y la disponibilidad, al tratarse de gestión de documentación y publicaciones oficiales que pueden estar usualmente asociadas a derechos del ciudadano, con los perjuicios que para el mismo puede suponer su alteración, falsedad o indisponibilidad.

4.1.6.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Sin valorar	Servicio público

Integridad	**Medio**	**Equiparación a Información**
Autenticidad	**Medio**	**Equiparación a Información**
Trazabilidad	Bajo	Dificultaría la subsanación de errores y seguimiento de delitos.
Disponibilidad	**Medio**	**Equiparación a la información**

Tabla 4-13. Servicio de Tablón oficial. Valoración del Servicio

La valoración del servicio ha sido equiparada a la valoración de la información.

4.1.7 Sistema AE – Registro Telemático y Tramitación

4.1.7.1 Valoración de la Información

Información	Nivel	Motivo
Confidencialidad	**Medio**	**Autorización explícita para acceso por parte del emisor y del receptor. Daño reputacional severo.**
Integridad	**Medio**	**Daño importante / Incumplimiento Ley 40/2015 art.38.2**
Autenticidad	**Medio**	**Daño importante / Incumplimiento autenticidad documento electrónico**
Trazabilidad	**Medio**	**Sellado de tiempo en documentos electrónicos**
Disponibilidad	Sin valorar	Se valora en el servicio.

Tabla 4-14. Registro Telemático y Tramitación. Valoración de la Información

El proceso de registro telemático presenta unos requerimientos medios en las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad, debido a su naturaleza y a la importancia del mismo dentro del proceso de Administración Electrónica.

4.1.7.2 Valoración del Servicio

Servicio	Nivel	Motivo
Confidencialidad	Sin valorar	Servicio público
Integridad	**Medio**	**Daño importante / Incumplimiento ley de notificación electrónica**
Autenticidad	**Medio**	**Incumplimiento autenticidad documento electrónico**
Trazabilidad	**Medio**	**Sellado de tiempo en documentos electrónicos**
Disponibilidad	Bajo	Normativa de registro electrónico de la UPRG

Tabla 4-15. Registro Telemático y Tramitación. Valoración del Servicio

El servicio está estrechamente relacionado con la información que contiene en las dimensiones de integridad, autenticidad y trazabilidad.

4.2 Categorización de los Sistema de Información

El resultado final de valoración de los servicios e información llevada a cabo en el apartado anterior se muestra en la siguiente tabla:

Servicio	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
ERP - Académico	Bajo	Medio	Medio	Bajo	Bajo	Medio
ERP - Económico	Bajo	Medio	Medio	Bajo	Bajo	Medio
ERP - RRHH	Medio	Bajo	Medio	Bajo	Bajo	Medio
ERP - Investigación	Bajo	Bajo	Medio	Sin valorar	Bajo	Medio
ERP - Portal	Bajo	Bajo	Medio	Bajo	Bajo	Medio
AE - Sede	Sin valorar	Medio	Medio	Bajo	Medio	Medio
AE - Tablón Oficial	Sin valorar	Medio	Medio	Bajo	Medio	Medio
AE - Registro Telemático + Tramitación	Medio	Medio	Medio	Medio	Bajo	Medio

Tabla 4-16. Valoración de Servicios e Información

El siguiente paso es la categorización de los sistemas identificados, siguiendo las indicaciones de catalogación señaladas en el ANEXO I del ENS, así como las recomendaciones de la guía CCN-STIC 803; esto queda recogido en la siguiente tabla:

Sistema	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
Sistema ERP Institucional	Medio	Medio	Medio	Bajo	Bajo	Medio
Sistema AE	Medio	Medio	Medio	Medio	Medio	Medio

Tabla 4-17. Categoría de los Sistemas

4.3 Selección de controles de seguridad

De acuerdo con el ENS una vez categorizados lo sistemas de información hay que llevar a cabo la declaración de aplicabilidad de las medidas de seguridad para cada uno de los sistemas. El resultado de aplicabilidad de las medidas, siguiendo la codificación y nomenclatura del ENS (ver Anexo II del RD 3/2010) ha sido el siguiente:

Código	Descripción	Sistema ERP	Sistema AE
org.1	Política de seguridad	aplica	aplica
org.2	Normativa de seguridad	aplica	aplica
org.3	Procedimiento de seguridad	aplica	aplica
org.4	Proceso de autorización	aplica	aplica
op.pl.1	Análisis de riesgos	+	+
op.pl.2	Arquitectura de seguridad	aplica	aplica

Código	Descripción	Sistema ERP	Sistema AE
op.pl.3	Adquisición de nuevos componentes	aplica	aplica
op.pl.4	Dimensionamiento / Gestión de capacidades	n.a	aplica
op.pl.5	Componentes certificados	n.a	n.a
op.acc.1	Identificación	aplica	aplica
op.acc.2	Requisitos de acceso	aplica	aplica
op.acc.3	Segregación de funciones y tareas	aplica	aplica
op.acc.4	Proceso de gestión de derechos de acceso	aplica	aplica
op.acc.5	Mecanismo de autenticación	+	+
op.acc.6	Acceso local (local logon)	+	+
op.acc.7	Acceso remoto (remote login)	+	+
op.exp.1	Inventario de activos	aplica	aplica
op.exp.2	Configuración de seguridad	aplica	aplica
op.exp.3	Gestión de la configuración	aplica	aplica
op.exp.4	Mantenimiento	aplica	aplica
op.exp.5	Gestión de cambios	aplica	aplica
op.exp.6	Protección frente a código dañino	aplica	aplica
op.exp.7	Gestión de incidencias	aplica	aplica
op.exp.8	Registro de la actividad de los usuarios	n.a	n.a
op.exp.9	Registro de la gestión de incidencias	aplica	aplica
op.exp.10	Protección de los registros de actividad	n.a	n.a
op.exp.11	Protección de claves criptográficas	aplica	aplica
op.ext.1	Contratación y SLAs	aplica	aplica
op.ext.2	Gestión diaria	aplica	aplica
op.ext.9	Medios alternativos	n.a	n.a
op.cont.1	Análisis de impacto	n.a	n.a
op.cont.2	Plan de continuidad	n.a	n.a
op.cont.3	Pruebas periódicas	n.a	n.a
op.mon.1	Detección de intrusión	n.a	n.a
op.mon.2	Sistema de métricas	n.a	n.a
mp.if.1	Áreas separadas y con control de acceso	aplica	aplica
mp.if.2	Identificación de las personas	aplica	aplica
mp.if.3	Acondicionamiento de los locales	aplica	aplica
mp.if.4	Energía eléctrica	aplica	+
mp.if.5	Protección frente a incendios	aplica	aplica
mp.if.6	Protección frente a inundaciones	n.a	aplica
mp.if.7	Registro de entrada y salida de equipamiento	aplica	aplica
mp.if.9	Instalaciones alternativas	n.a	n.a
mp.per.1	Caracterización del puesto de trabajo	aplica	aplica
mp.per.2	Deberes y obligaciones	aplica	aplica
mp.per.3	Concienciación	aplica	aplica

Código	Descripción	Sistema ERP	Sistema AE
mp.per.4	Formación	aplica	aplica
mp.per.9	Personal alternativo	n.a	n.a
mp.eq.1	Puesto de trabajo despejado	+	+
mp.eq.2	Bloqueo de puesto de trabajo	aplica	aplica
mp.eq.3	Protección de equipos portátiles	aplica	aplica
mp.eq.9	Medios alternativos	n.a	aplica
mp.com.1	Perímetro seguro	aplica	aplica
mp.com.2	Protección de la confidencialidad	aplica	aplica
mp.com.3	Protección de la autenticidad y de la integridad	+	+
mp.com.4	Segregación de redes	n.a	n.a
mp.com.9	Medios alternativos	n.a	n.a
mp.si.1	Etiquetado	aplica	aplica
mp.si.2	Criptografía	aplica	aplica
mp.si.3	Custodia	aplica	aplica
mp.si.4	Transporte	aplica	aplica
mp.si.5	Borrado y destrucción	aplica	aplica
mp.sw.1	Desarrollo	aplica	aplica
mp.sw.2	Aceptación y puesta en servicio	+	+
mp.info.1	Datos de carácter personal	aplica	aplica
mp.info.2	Calificación de la información	+	+
mp.info.3	Cifrado	n.a	n.a
mp.info.4	Firma electrónica	+	+
mp.info.5	Sellos de tiempo	n.a	n.a
mp.info.6	Limpieza de documentos	aplica	aplica
mp.info.9	Copias de seguridad (backup)	aplica	aplica
mp.s.1	Protección del correo electrónico	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	+	+
mp.s.8	Protección frente a la denegación de servicio	n.a	aplica
mp.s.9	Medios alternativos	n.a	n.a

Tabla 4-18. Medidas de seguridad aplicables

Se usa la siguiente nomenclatura basada en el ENS:

Nomenclatura	Significado
org	Organizativas
op.pl	Operativas de Planificación
op.acc	Operativas de control de acceso
op.exp	Operativas de explotación
op.ext	Operativas de externalización
op.cont	Operativas de continuidad
op.mon	Operativas de monitorización

mp.if	Protección de las instalaciones e Infraestructuras
mp.per	Protección del Personal
mp.eq	Protección de los equipos
mp.com	Protección de las comunicaciones
mp.si	Protección de los soportes de información
mp.sw	Protección del software
mp.info	Protección de la Información
mp.s	Protección de los servicios
n.a.	Medida de seguridad no aplicable
aplica	Medida de seguridad aplicable debido a las dimensiones de seguridad o categoría del sistema actual
+	Indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad

Tabla 4-19. Nomenclatura para indicar la aplicación de medidas

5 Análisis de Riesgos

Para el análisis de riesgos de los sistemas emplearemos la metodología Magerit v3 usando PILAR como herramienta de apoyo para llevar a cabo dicho análisis. La herramienta PILAR soporta el análisis y el tratamiento de riesgos de un sistema de información siguiendo la metodología Magerit v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Se actualizan periódicamente y existen diversas variantes:

- **PILAR:** versión íntegra de la herramienta
- **PILAR Basic:** versión sencilla para Pymes y Administración Local
- **μPILAR:** versión de PILAR reducida, destinada a la realización de análisis de riesgos muy rápidos

Todas las versiones de PILAR disponen de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- **ISO/IEC 27002 (2005, 2013)-** Código de buenas prácticas para la Gestión de la Seguridad de la Información
- **ENS - Esquema Nacional de Seguridad.**

Para el presente análisis de riesgos se usará la versión íntegra de la herramienta (en concreto la versión 5.4.8) la cual permite analizar los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (accountability) y tratar el riesgo. Para tratar el riesgo se proponen salvaguardas (o contramedidas), normas de seguridad y procedimientos de seguridad analizándose el riesgo residual a lo largo de diversas etapas de tratamiento.

Por su parte MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (la versión actual de Magerit es la versión Magerit v3). MAGERIT permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

El análisis de riesgos en Magerit v3 se basa en los siguientes conceptos:

- **Activo:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos

- **Valor propio de un activo:** El del elemento en sí mismo.

- **Valor acumulado de un activo:** el proporcional a los elementos que tiene encima

- **Valor nuclear de un activo:** El que tiene el elemento de más alto nivel (generalmente la información)

- **Amenazas:** Eventos que pueden desencadenar un incidente en la organización produciendo daños materiales o pérdidas inmateriales. Las amenazas varían de un activo a otro. Existen una amenaza por cada activo y dimensión de seguridad y no todas las dimensiones están afectadas por todas las amenazas

- **Impacto:** Medida del daño sobre un activo derivado de la materialización de una amenaza. Se calcula por cada amenaza, activo y dimensión

- **Impacto acumulado:** Se calcula sobre un activo teniendo en cuenta su valor acumulado (el propio más el acumulado por los activos que dependen de él) y la degradación producida por las amenazas a las que está expuesto

- **Impacto repercutido:** Se calcula sobre un activo teniendo en cuenta su valor propio y la degradación provocada por las amenazas a las que están expuesto los activos de los que depende

- **Riesgo:** Medida del daño probable de un sistema. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Se calcula por cada activo amenaza y dimensión.

- **Riesgo potencial:** Riesgo sin tener en cuenta la aplicación de ningún tipo de salvaguarda

- **Riesgo acumulado:** Se calcula sobre un activo teniendo en cuenta el impacto acumulado sobre un activo y la frecuencia de la amenaza

- **Riesgo repercutido:** Se calcula sobre un activo teniendo en cuenta el impacto repercutido sobre un activo y la frecuencia de la amenaza

- **Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo.

- **Impacto residual:** Impacto remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información.

- **Riesgo residual:** Riesgo remanente en el sistema tras la implantación de las salvaguardas

En el siguiente diagrama se muestra la relación entre algunos de estos conceptos y que son la base para obtener el impacto y riesgo potencial:

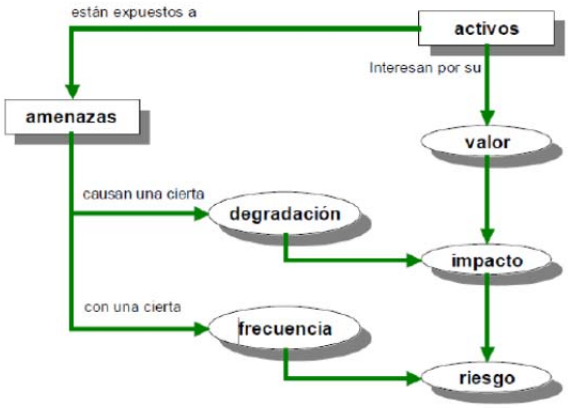

Ilustración 5-1. Relaciones entre conceptos del análisis de riesgos

En los resultados del análisis de riesgos que se obtiene en base a los conceptos del diagrama se calcula el riesgo potencial sin tener en cuenta la aplicación de ningún tipo de salvaguardas. Una vez que se conoce el riesgo potencial es necesario llevar a cabo una identificación y valoración del impacto de las salvaguardas sobre dicho riesgo para obtener el riesgo resultante de la aplicación de las mismas, lo cual hemos definido como riesgo repercutido. En el siguiente diagrama se muestra el efecto de las salvaguardas sobre el impacto y el riesgo

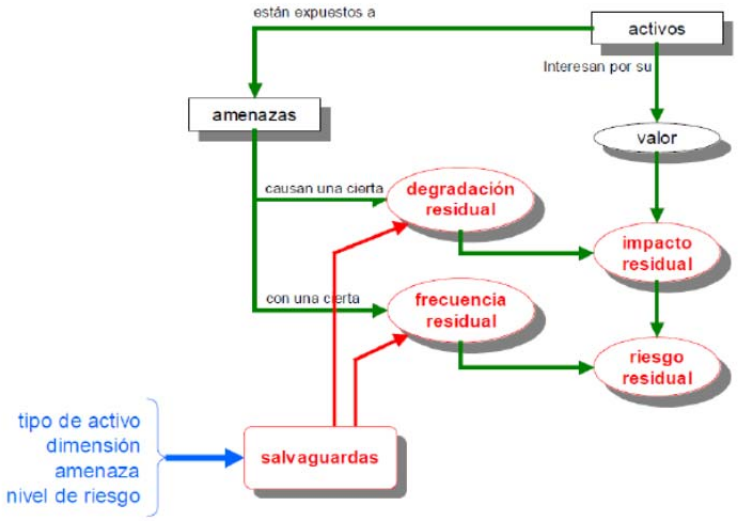

Ilustración 5-2. Consecuencias de la implantación de salvaguardas

Así pues vemos como las salvaguardas actúan reduciendo la degradación así como la frecuencia de las amenazas lo cual se traduce en la obtención de un impacto y riesgo residuales. Es necesario indicar que en el caso de PILAR dichas salvaguardas se aplican a nivel global para todo el sistema reduciendo y evitando el riesgo (gestionando el riesgo) de forma que:

- La salvaguarda debe/puede producir reducción en la degradación de la amenaza para cada dimensión

- La salvaguarda debe/puede producir una reducción en la frecuencia para cada dimensión

5.1 Escenario a analizar

En la siguiente imagen se muestra la arquitectura lógica de la red del escenario a modelar:

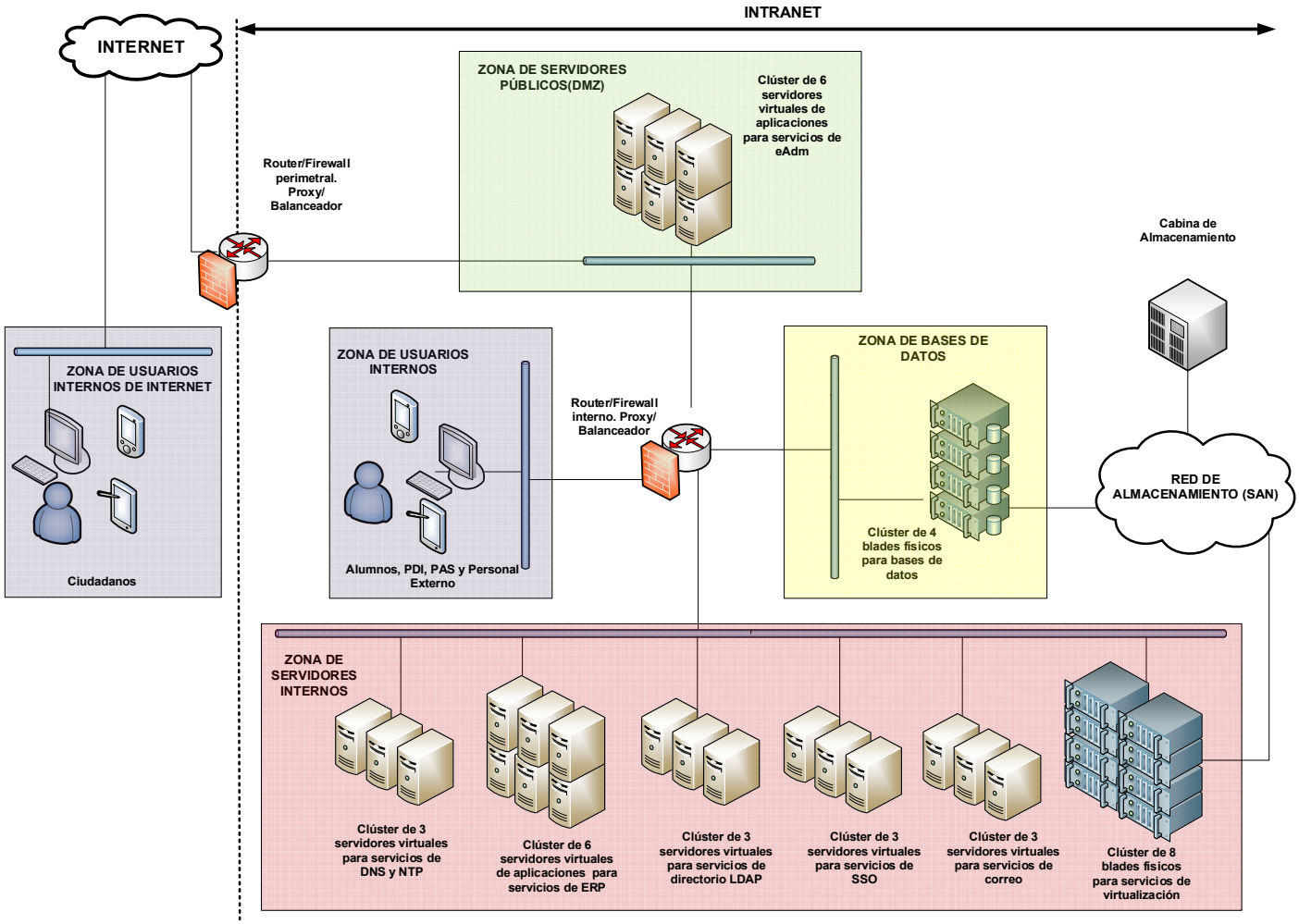

Ilustración 5-3. Arquitectura lógica de Red

En el diagrama de arquitectura lógico de red nos encontramos con 4 zonas bien diferencias:

- **Zona de servidores públicos**: Se trata de una zona desmilitarizada ubicada entre el firewall perimetral y el firewall interno. A las VLANs asignadas a esta zona se encuentran conectados 6 servidores de aplicaciones virtualizados con sistema operativo Linux donde se encuentran instaladas las aplicaciones que proporcionan los servicios accesibles desde Internet. Dichos servidores funcionan sobre un chasis de blades físicos usando la tecnología de vitualización Hyper-V de Microsoft. Los servicios accesibles desde Internet proporcionados a través de este entorno virtualizado se corresponden con los servicios de Administración electrónica que integran el sistema de AE y que se corresponden con 3 aplicaciones web desarrolladas en J2EE y corriendo sobre servidores Apache-Tomcat:

    - Registro electrónico y tramitación

- Tablón oficial
- Sede electrónica

Estas 3 aplicaciones corren de forma simultánea en cada uno de los 6 servidores formando un clúster activo-activo de manera que las peticiones contra dichas aplicaciones son balanceadas entre todos estos servidores repartiendo la carga entre los mismos al tiempo que se consigue una alta disponibilidad de los servicios proporcionados por dichas aplicaciones.

- **Zona de servidores internos**: Al igual que la zona de servidores públicos, esta zona cuenta con la misma infraestructura de 6 servidores virtualizados en un clúster activo-activo pero en este caso las aplicaciones instaladas en dichos servidores proporcionan los servicios agrupados en el sistema ERP los cuales son gestionados por los empleados de la universidad y son únicamente accesibles por el personal que tiene una relación con la Universidad. Estas aplicaciones que están desarrolladas en J2EE y corren sobre servidores Apache-Tomcat son:
  - Aplicación de gestión académica
  - Aplicación de gestión económica
  - Aplicación de RRHH
  - Aplicación de Investigación

  Así mismo se encuentran ubicado en dicha zona un clúster de 8 blades físicos sobre los que se encuentra instalada una tecnología de virtualización basada en el hypervisor Hyper-V como sistema anfitrión sobre el que se ejecutan los diferentes servidores virtuales (máquinas virtuales) sobre los que corren los aplicativos que proporcionan los servicios públicos e internos de la Universidad. Los 8 blades forman a nivel virtual un clúster activo-pasivo de forma que si alguno de dichos blades falla, los servidores virtuales que corren sobre el blade que ha fallado son automáticamente reubicados en el resto de blades que forman dicho clúster.

- **Zona de base de datos:** En la VLAN asignada a esta zona se localiza un clúster de 4 blades físicos con sistema operativo Linux sobre el que funciona un clúster activo-activo de base de datos MySQL que albergan la información correspondiente al modelo de datos de las diferentes aplicaciones tanto públicas como internas.

- **Zona de base de usuarios:** En esta zona se ubican los equipos usados por el personal con vinculación con la Universidad. Dicho acceso se lleva cabo tanto mediante terminales fijos ubicados dentro de la correspondiente Escuela o Facultad como a través de terminales móviles (teléfonos, PDAs,..) a través de los diferentes puntos de acceso wifi distribuidos a lo largo de todo el campus. En el caso del acceso por wifi existe un procedimiento de control de acceso consistente en un portal cautivo donde el usuario debe introducir sus credenciales

de usuario y contraseña antes de poder acceder a la red. Además una vez autenticado, se asigna al usuario una VLAN en función de su perfil de acceso el cual puede ser:

- Personal Docente e Investigador (PDI). Acceden a los siguientes servicios:
  - Servicio de gestión académica para dar cuenta del progreso académico de sus estudiantes.
  - Servicio de gestión de RRHH para conocer el estado de su nómina
  - Servicio de Investigación para dar cuenta del progreso de sus proyectos de investigación.
- Personal de Administración y Servicios (PAS). Acceden a los siguientes servicios:
  - Servicio de gestión académica para la gestión administrativa diaria relacionada con el desarrollo de las enseñanzas Universitarias
  - Servicio de gestión económica para la gestión de los bienes y recursos de la Universidad (presupuestos, cuentas, financiación,…)
  - Servicio de gestión de RRHH para llevar a cabo la gestión diaria del personal al servicio de la Universidad (altas, bajas, nóminas, etc…)
  - Servicio de Investigación para dar soporte a los investigadores en las tareas administrativas relacionadas con la gestión de sus investigaciones (solicitud de becas, sistemas de evaluación de la calidad de las investigaciones,….)
- Alumnos. Acceden a los siguientes servicios:
  - Servicio de gestión académica: Para la consulta de sus notas y expedientes
- Personal Externo: Se trata de personal que está vinculado a la Universidad en función de un contrato por obra y servicio tales como empresas o profesionales para proporcionar funciones de consultoría, soporte y mantenimiento de los diferentes sistemas existentes en la Universidad. Deberán tener acceso en cada momento a los sistemas que requieran para llevar a cabo sus funciones de soporte y mantenimiento.

Todos los perfiles anteriores acceden a su vez a los servicios de Administración electrónica para llevar a cabo aquellos trámites que se encuentran a disposición del público en general tales como:

- Consulta de anuncios oficiales en el tabón oficial (resoluciones y normativas de la Universidad, convocatorias de becas y empleo, resultados de pruebas selectivas,….)

- Realizar entradas en el registro electrónico de la Universidad (quejas y reclamaciones, solicitud de becas,…

El acceso a dichos servicios se puede hacer directamente en las URLs asociadas a los aplicativos que las proporcionan o mediante el acceso a la URL de la sede electrónica de la Universidad que actúa como punto centralizado de acceso a los mismos.

Además de estas 4 zonas podemos identificar el sistema de almacenamiento en red (Storage Area Network) que consiste en una switch Fabric que permite acceder vía Fiber Channel (FC) a la cabina de almacenamiento que contiene un conjunto de bandejas de discos de Fibra configurados en RAID 5 donde se almacena toda la información. Tanto el clúster de 8 blades físicos que implementan la infraestructura de virtualización como el clúster de 4 blades físicos que tienen instalado el sistema de base de datos se conectan a dicha red de datos mediante tarjeta FC para poder acceder a la cabina de almacenamientos y montar los volúmenes de datos con la información que necesitan.

A continuación se presenta un diagrama lógico donde se representa la interactuación entre los diferentes componentes para llevar a cabo las funciones de proxy y balanceo entre los diferentes aplicativos que proporcionan los servicios de acceso público.

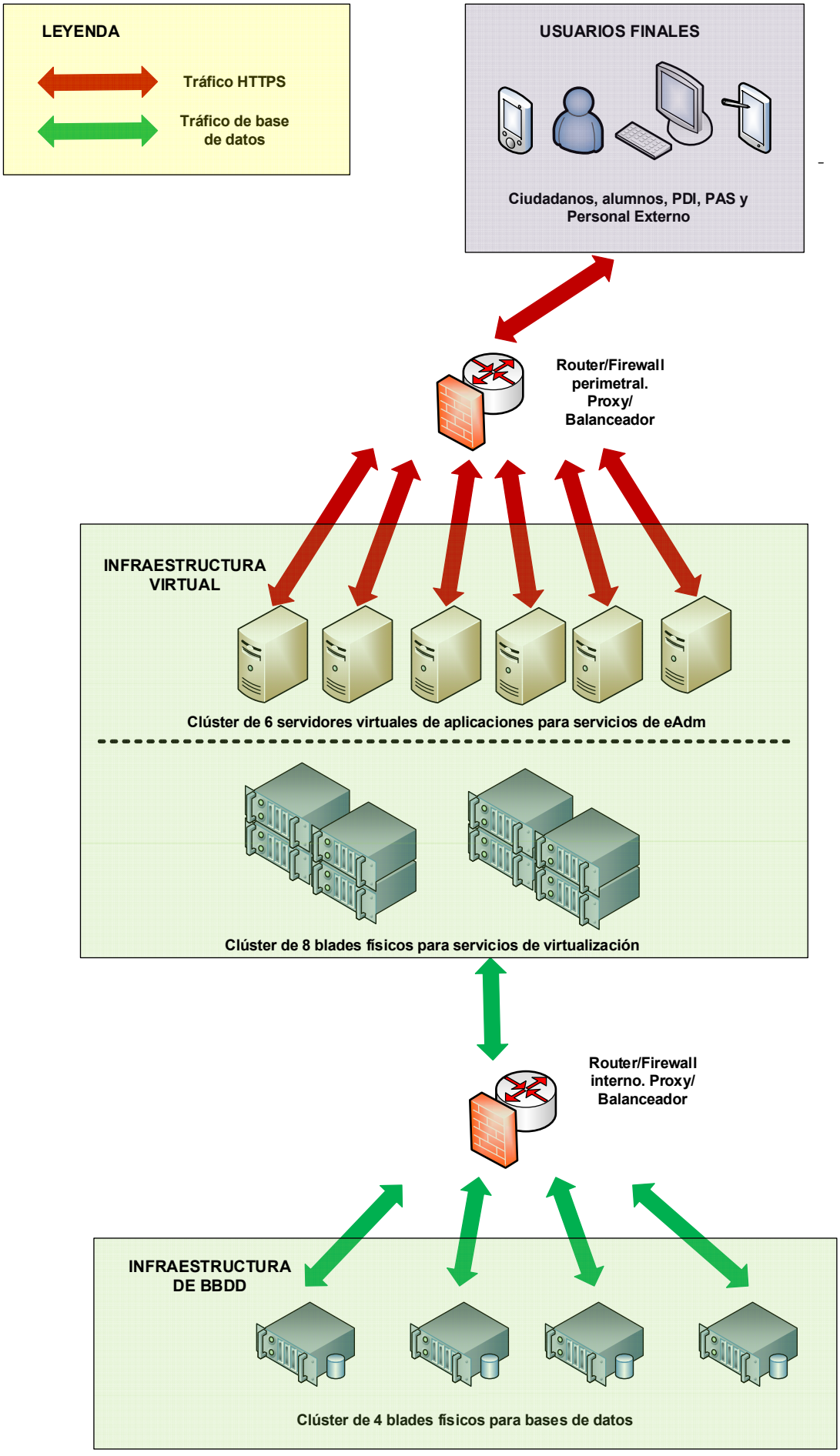

Ilustración 5-4. Diagrama lógico de flujos de tráfico para servicios de AE

Para el caso del acceso a los servicios de Administración electrónica tanto si se hace desde la intranet como si se accede vía Internet es el router con funciones de firewall perimetral el encargado de actuar como proxy y balanceador redirigiendo y repartiendo las peticiones entre el clúster de 6 servidores sobre los que se encuentran instaladas las aplicaciones. Cuando dichos servidores de aplicaciones requieren acceder a las bases de datos lo hacen a través del router interno que en este caso actúa por un lado como firewall filtrando las peticiones y por otro como proxy y balanceador repartiendo las peticiones de datos entre las diferentes instancia de MySql.

El diagrama lógico que se presenta a continuación para el caso de los servidores que proporciona los servicios internos de la Universidad es similar al anterior pero en este caso es el router interno con funciones de firewall el que realiza las funciones de proxy y balanceador no sólo para las peticiones contra los aplicativos sino para las peticiones contra los servidores de base de datos.

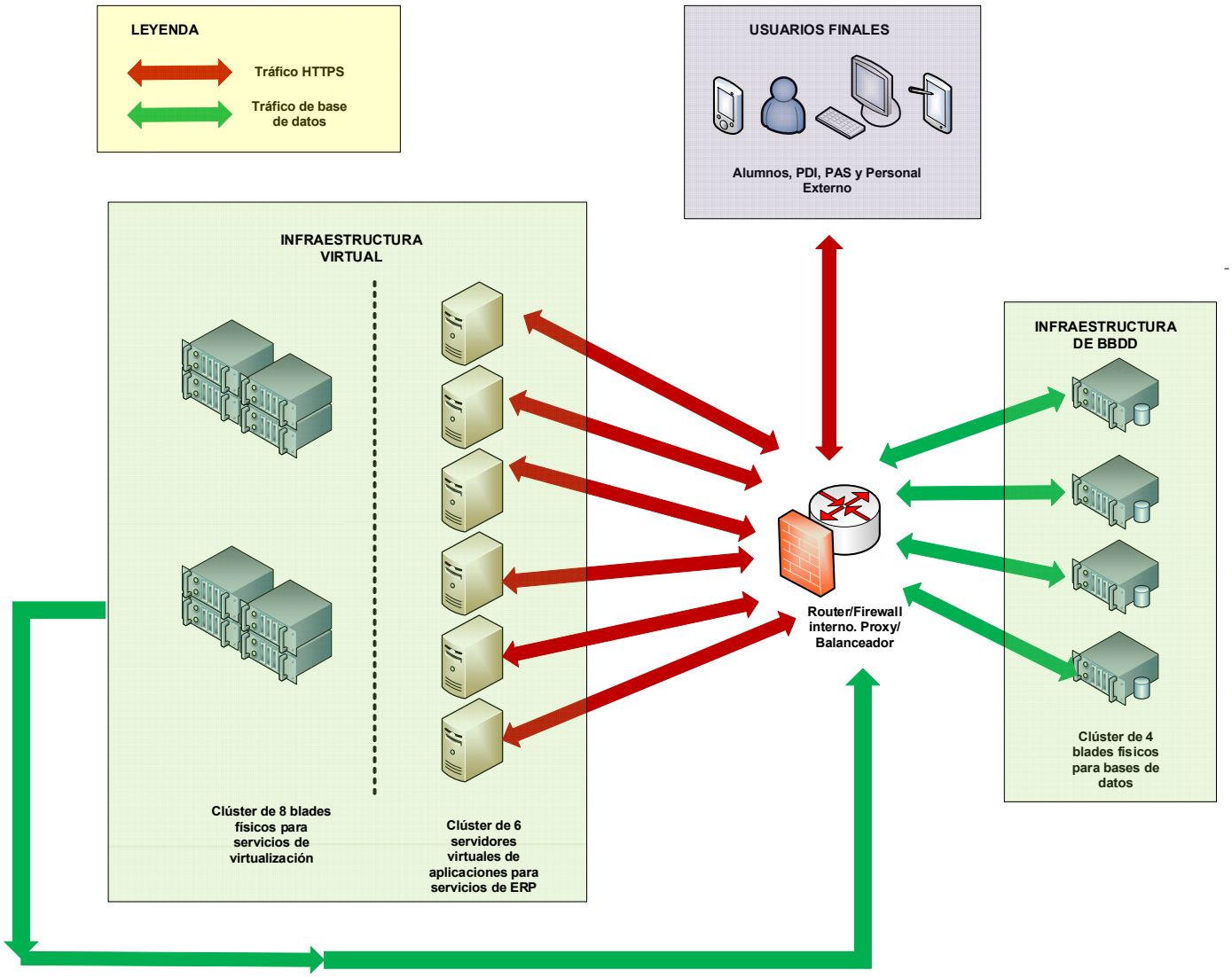

Ilustración 5-5. Diagrama lógico de flujos de tráfico para servicios de ERP

A nivel de ubicaciones físicas nos encontramos con un edificio localizado dentro del campus dedicado por completo a la unidad de IT que cuenta en su interior con una sala de servidores y otra sala de comunicaciones. En la sala de servidores se ubica todo el hardware físico incluyendo los blades físicos y la cabina de almacenamiento. En la sala de comunicaciones se encuentra el equipamiento de red que incluye los equipos con funciones de enrutamiento, firewall, proxy y balanceo. Sólo el personal de IT y los proveedores debidamente autorizados tienen acceso a estas 2 salas del edificio.

El resto del campus está compuesto por edificios de escuelas y facultades donde podemos localizar al resto del personal de la Universidad incluyendo alumnos, profesores y personal de administración.

5.2 Creación del proyecto

El primer reto que se plantea es como trasladar estos 2 sistemas a un proyecto en PILAR. Se han manejado 3 posibles opciones cada una con sus ventajas e inconvenientes:

- **Opción 1:** Un sólo proyecto para ambos sistemas y un mismo dominio de seguridad
    - Ventajas:
        - Todo en un único proyecto
        - No es necesario replicar activos
    - Desventajas:
        - Pérdida de visión de los sistemas por separado
- **Opción 2:** Un sólo proyecto para ambos sistemas y varios dominios de seguridad (uno por sistema)
    - Ventajas:
        - Todo en un único proyecto
        - Visión de los sistemas por separado (uno por dominio)
    - Desventajas:
        - Necesidad de replicar activos entre dominios
        - PILAR no termina de funcionar bien con varios dominios
- **Opción 3:** Un proyecto y un dominio de seguridad por cada sistema

- Ventajas:
  - Visión de los sistemas por separado (uno por dominio)
  - Seguridad de que PILAR funcionará correctamente
- Desventajas:
  - Necesidad de replicar activos entre dominios

Al final para evitar posibles problemas con el manejos de los dominios de seguridad con PILAR se ha optado por la opción 3, esto es, crear un proyecto para cada uno de los sistemas lo cual nos permitirá tener una visión por separado de cada uno de ellos a la hora de realizar el análisis y tratamiento de los riesgos.

5.3 Identificación y valoración de activos

El modelado de activos por capas empleado en PILAR es un proceso que para cada capa necesita un razonamiento de modelado para los activos que la componen y a su vez ese razonamiento o modelo dará lugar al razonamiento de las relaciones. Para crear la clasificación de niveles iniciales se siguió el principio de que cada capa superior "depende" de una capa inferior. A partir de dicho razonamiento es necesario establecer las relaciones entre los activos que hay en cada capa y con las capas que los rodean. Estas relaciones dependerán mucho de cómo se haya decidido modelar los activos dentro de capa siendo el modelo de una capa diferente del de las otras y por lo tanto dando lugar a diferentes relaciones. Hay que tener en cuenta que no debe de tratarse de un modelo exhaustivo porque entonces se volvería demasiado complejo de entender y gestionar. Por este motivo se optó por crear un modelo de relaciones práctico y orientado al objetivo final que queríamos obtener que es en este caso sería el cálculo del valor acumulado en base a esas relaciones lo cual determinará el resto de cálculos realizados por PILAR.

Además a la hora de establecer el modelo de relaciones el razonamiento a seguir puede variar de una capa a otra. Esto es, el razonamiento que se sigue para establecer las dependencias entre activos de tipo software y servidores es diferente a que se ha seguido para establecer las relaciones a nivel de los activos de Red. Además la forma en la que se plantean estas relaciones lleva a la necesidad de incluir nuevas incluir nuevos grupos y activos que permitiesen ayudar a modelarlas. Veremos ahora las capas iniciales y luego una por una el modelo que se siguió para el modelado de sus activos en cada capa y su relación con activos de otras capas y entre ellos. La clasificación tradicional recomendada por Pilar es la siguiente:

Capa
[B] Capa de Negocio
[IS] Servicios internos
[E] Equipamiento

[SS] Servicios subcontratados
[L] Instalaciones
[P] Personal

Tabla 5-1. Capas del modelo por defecto de activos en PILAR

La capa de Equipamiento se subdivide a su vez en las siguientes subcapas:

Capa	Subcapas
[E] Equipamiento	**[SW] Aplicaciones**
	[HW] Equipos
	[COM] Comunicaciones
	[AUX] Elementos auxiliares

Tabla 5-2. Subcapas del modelo por defecto de activos en PILAR

Esta clasificación no nos resulta adecuada ya que no incluye una capa para activos tan importantes como es el caso de la Información. Por ello decidimos conservar algunas de estas capas así como crear nuevas capas y subcapas para nuestro modelo. En la siguiente tabla se muestran las capas que componen dicho modelo:

Capa	Descripción
[I] Capa de Información [Negocio]	Incluye los activos de tipo información. Estos activos junto con los de tipo servicio son los más importantes del sistema
[S] Capa de Servicios [Negocio]	Incluye los activos de tipo servicio. Estos activos junto con los de tipo Información son los más importantes del sistema
[A] Aplicaciones	Aplicaciones que actúan de forma conjunta para proporcionar un servicio

[IT] Servicios IT	El objetivo de esta nueva capa es incluir los servicios que aunque no entran dentro del alcance del presente análisis son activos a tener en cuenta de cara a realizar el análisis de riesgo. Esto es así porque se trata de servicios horizontales que son usados por las aplicaciones que sí entran en el análisis y por lo tanto el buen funcionamiento de las aplicaciones depende de estos activos/servicios.
[H] Hosts	Capa que estaría ubicada en el modelo tradicional entre Aplicaciones y Equipo informático. Incluye los servidores virtualizados considerado desde el punto de vista de un sistema operativo que permite la ejecución software de base (Servidores web, servidores de Aplicaciones, etc....) para las aplicaciones que se ejecutan en ellos. Siempre que sea posible se agruparan los servidores que formen un clúster en un solo activo.
[HW] Hardware	En esta capa se incluye todo lo que sea equipamiento físico tanto a nivel de máquina como a nivel de almacenamiento.
[NET] Redes y Comunicaciones	Incluye todo lo relacionado con las redes y los equipamientos de red
[UBI] Ubicaciones	En esta capa se incluyen los espacios físicos
[P] Personas	Incluye los proveedores, personal del servicio de informática, Alumnos y PAS/PDI

Tabla 5-3. Descripción de capas del modelo

En la tabla que viene a continuación se describen las subcapas que se han introducido en la capa de Hardware y en la de Redes y Comunicaciones:

Capa	Subcapas	Contenido
[HW] Hardware	**[SERV] Servidores**	Servidores hardware físicos. Para los servidores que están en clúster creamos un grupo que representa la agrupación de servidores físicos relacionando cada uno de los servidores físicos con este grupo. Esto se hace así para simplificar el modelado de la conexión con los sistemas de almacenamiento así como con la capa superior de "Hosts". Así por ejemplo se creó el activo Cluster Virtualización. Este activo depende de una serie de blades que lo componen cada uno de los cuales está conectado a la cabina de almacenamiento. Para evitar tener que especificar que cada una de las conexiones de almacenamiento se especificó solamente para Clúster Virtualización.

	[ALM] Sistema de Almacenamiento	Equipos y redes de almacenamiento físico. Permite incluir lo elementos propios red de almacenamiento SAN como es el caso de la cabina de almacenamiento
	[EQU] Equipos	Dispositivos físicos electrónicos usados por los usuarios ya sean equipos de escritorio o dispositivos móviles
	[SPINF] Soportes de Información	Soportes de información electrónicos
[NET] Redes y Comunicaciones	**[NETTOP] Topología**	Representa la zona a la que están conectados los activos. Una zona puede estar compuesta por uno o más VLANs
	[NETHW] Equipos de Red	Se incluyen aquí todos los equipos que realizan funciones sobre el tráfico de datos que incluyen el routeado, filtrado de tráfico, proxy y balanceo

Tabla 5-4. Descripción de subcapas del modelo

Este modelo de capas incluye también las relaciones entre las mismas. En la siguiente tabla se muestran las relaciones de descendencia entre capas principales:

Capa	Relaciones con otras capas
[I] Capa de Información [Negocio]	[S] Capa de Servicios [Negocio]. La información se accede a través de los servicios que permiten el acceso a la misma
[S] Capa de Servicios [Negocio]	[S] Capa de Servicios [Negocio]. Para el caso de servicios que son horizontales a otros.
	[IT] Servicios IT. El funcionamiento de las servicios depende de determinados servicios IT
	[A] Aplicaciones. Las aplicaciones incluyen la funcionalidad para proporcionar los servicios
[A] Aplicaciones	[A] Aplicaciones. Ocurre para aplicaciones que son horizontales a otras. En el modelado de ambos sistemas no se han identificado este tipo de dependencias por lo que no aparece en el diagrama sacado de Pilar
	[H] Hosts . Relación con los hosts que contiene el software base sobre el que se ejecutan las aplicaciones.
[IT] Servicios IT	[IT] Servicios IT. Para el caso de servicios que son horizontales a otros.
	[A] Aplicaciones. Las aplicaciones incluyen la funcionalidad para proporcionar los servicios
	[H] Hosts . Relación con los hosts que contiene el software base sobre el que se ejecutan las aplicaciones.
[H] Hosts	[HW] Hardware. Máquinas hardware sobre las que corre el software base o sistema virtual.

	[NET] Redes y Comunicaciones. Esta relación permite modelar el hecho de que los servidores virtualizados pueden encontrarse en una zona de red diferente al del servidor físico que los contiene.
[HW] Hardware	[HW] Hardware. Para poder establecer relaciones entre el propio equipamiento hardware incluido los servidores y el equipamiento de las redes de almacenamiento SAN
	[NET] Redes y Comunicaciones. Para relacionar con la zona de Red IP en la que se encuentra la máquina hardware. En principio la capa Servidores tiene principalmente relaciones con la Red de almacenamiento SAN siendo las relaciones con la capa de Red IP más propias de la capa "hosts"
	[UBI] Ubicaciones. Al tratarse de activos físicos deben estar en una ubicación.
[NET] Redes y Comunicaciones	[NET] Redes y Comunicaciones. Para relacionar con la zona de Red IP en la que se encuentra un equipo de red
	[UBI] Ubicaciones. Al tratarse de activos físicos deben estar en una ubicación.
[UBI] Ubicaciones	[UBI] Ubicaciones. Es el caso de las salas de comunicaciones y de redes que están ubicada en la unidad de TI, el cual a su vez está ubicado en el campus
	[P] Personas . Las personas acceden a los espacios físicos
[P] Personas	

Tabla 5-5. Relación entre las capas del modelo

Una vez que sabemos el modelo de capas a emplear en PILAR entonces debemos establecer clases de activos para asociarlo a los activos a modelar e incluirlos en cada una de las capas anteriores. PILAR se basa en Magerit v3 para identificar diferentes clases y subclases de activos. Los activos principales identificados por Magerit v3 e incluidos en PILAR son:

Clases de Activos	Descripción
[essential] Activos Esenciales	En un sistema de información hay 2 cosas esenciales: — la información que se maneja y — los servicios que prestan. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos:
[arch] Arquitectura del sistema	Se trata de elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.
[D] Datos / Información	Los datos son el corazón que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
[keys] Claves criptográficas	Las criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos.
[S] Servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.
[SW] Aplicaciones (software)	Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

[HW] Equipamiento informático (hardware)	Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
[Media] Soportes de información	Se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
[AUX] Equipamiento auxiliar	Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
[L] Instalaciones	Se consideran los lugares donde se hospedan los sistemas de información y comunicaciones.
[P] Personal	Aparecen las personas relacionadas con los sistemas de información.

Tabla 5-6. Clases principales de activos en Magerit v3

Como se ha comentado cada uno de estas clases activos incluye a su vez subclases cada una con un identificador. Todas estas subclases y sus identificadores se pueden consultar en la guía de elementos de Magerit v3. Hay que señalar que la pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos.
A continuación sirviéndonos del modelo que hemos fijado de capas y de las clases y subclases de activos proporcionados por PILAR en base a Magerit v3, construimos el modelo de activos para cada uno de los sistemas en base a la información proporcionada en la descripción del escenario a analizar.

A la hora de identificar activos hemos tenido en cuenta los siguientes principios:

- A la hora de dar de alta activos es preferible agruparlos lo máximo posible y si luego vemos que queremos detallar los riesgos podemos entonces decidir disgregar los que nos interesen.

- Se recomienda que el número de activos no sea superior a 50 aunque en la práctica se manejan entre 100 y 150. Por encima de 150 es muy complejo de manejar con Pilar

En la siguiente tabla podemos ver para cada uno de los sistemas la agrupación de los activos identificados y dados de alta en PILAR y qué es cada uno (en el apartado común se incluyen los activos que son comunes a ambos sistemas):

Sistema	Capas	Activos
ERP	[I] Capa de Información [Negocio]	[I_ACADE] Información Académica
		[I_ECONO] Información Económica
		[I_RRHH] Información sobre Recursos Humanos
		[I_IDI] Información de Investigación, Desarrollo e Innovación
	[S] Capa de Servicios [Negocio]	[S_ACADE] Servicio ERP Académico
		[S_ECONO] Servicio ERP Económico
		[S_RRHH] Servicio ERP RRHH
		[S_IDI] Servicio ERP Investigación, Desarrollo e Innovación
	[A] Aplicaciones	[A_ACADE] Aplicación de Académico
		[A_CORREO] Aplicación de Correo
		[A_ECONO] Aplicación para Económico
		[A_RRHH] Aplicación de RRHH
		[A_IDI] Aplicación de IDI
	[H] Hosts	[H_SRVWEB] Cluster de 6 VMs para servicios de ERP
EADM	[I] Capa de Información [Negocio]	[I_PUBLICACION] Información de publicaciones electrónicas
		[I_TRAMITACION] Información de Tramitación electrónica
	[S] Capa de Servicios [Negocio]	[S_TABLON] Servicio Tablón Oficial
		[S_TRAMITACION] Servicio de Tramitación Electrónica
		[S_SEDE] Servicio de Sede Electrónica
	[A] Aplicaciones	[A_TABLON] Aplicación Tablón Electrónico
		[A_TRAMITACION] Aplicación Tablón Electrónico
		[A_SEDE] Aplicación de Sede
	[IT] Servicios IT	[IT_PROXY_BALANCEADOR_EXT] Servicio de Proxy y Balanceo para acceso externo
		[IT_DNS_EXT] Servicio DNS consultas publicas
	[H] Hosts	[H_SRVWEB] Cluster de 6 VMs para servicios de AE
COMUNES	[IT] Servicios IT	[IT_PROXY_BALANCEADOR_INT] Servicio de Proxy y Balanceo para acceso interno
		[IT_DNS_INT] Servicio DNS consultas internas
		[IT_NTP] Servicio NTP
		[IT_SGBD] Servicio de Bases de Datos
		[IT_DIRECTORIO] Servicio LDAP
		[IT_SSO] Servicio de Autenticación Centralizada y SSO
		[IT_CORREO] Servicio de Correo Electrónico
	[A] Aplicaciones	[A_CORREO] Aplicación de Correo
		[A_DNS] Aplicación de DNS
		[A_NTP] Aplicación de NTP
		[A_SGBD] Sistema de Gestión de Bases de Datos

		[A_DIRECTORIO] Aplicación de LDAP
		[A_SSO] Aplicación de SSO
	[H] Hosts	[H_DNS_NTP] Cluster de 3 VMs para DNS y NTP
		[H_SGBD] Cluster de 3 host físicos de BBDD
		[H_DIRECTORIO] Clúster de 3 VMs de directorio LDAP
		[H_SSO] Clusters de 3 VMs para servicios de SSO
		[H_CORREO] Clúster de 3 VMs de correo para PDI y PAS
	[HW] Hardware-[SERV] Servidores	[HW_VIRTUALIZACION] Cluster de blades físicos para Virtualización
		[HW_SGBD] Cluster de 3 hosts físicos para SGBD
	[HW] Hardware-[ALM] Sistema de Almacenamiento	[HW_CABINA] Cabina de Almacenamiento
		[HW_NETALM] Red de Almacenamiento
	[HW] Hardware-[EQU] Equipos	[EQU_FIJO] Equipo personal de escritorio de usuario
		[EQU_MOVIL] Equipo móvil de usuario
	[HW] Hardware-[SPINF] Soportes de información	[SPINF_EXTRAIBLES] Soportes extraíbles de información
	[NET] Redes y Comunicaciones-[NETTOP] Topología	[NETTOP_WAN] Red Externa e Internet
		[NETTOP_WIFI] Red WIFI
		[NETTOP_DMZ] LAN - Zona Servidores públicos
		[NETTOP_USUARIOS] LAN - Zona equipos de usuarios
		[NETTOP_SRVINT] LAN - Zona Servidores internos
		[NETTOP_BBDD] LAN - Zona Servidores de Bases de Datos
		[NETTOP_GEST] LAN - Zona Gestión de Equipamiento
	[NET] Redes y Comunicaciones-[NETHW] Equipos de Red	[NETHW_ROUTER_PERIMETRAL] Equipo conectado a la red externa con funciones de Router,Firewall,Proxy y Balanceador
		[NETHW_WAP] Puntos de acceso WIFI
		[NETHW_ROUTER_INTERNO] Equipo interno con funciones de Router,Firewall,Proxy y Balanceador
	[UBI] Ubicaciones	[UBI_IT] Unidad de IT
		[UBI_SERV] Sala de Servidores
		[UBI_COM] Sala de Comunicaciones
		[UBI_CAMPUS] Campus UPRG
	[P] Personas	[P_IT] Personal de IT
		[P_PASPDI] Personal PAS/PDI
		[P_ALU] Alumnos
		[P_PROV] Personal de Proveedores y Subcontratación

Tabla 5-7. Activos agrupados por capas

A continuación pasamos a la valoración de los activos la cual nos dará una visión de la importancia de nuestro activo en términos de seguridad en base a la valoración de las 5 dimensiones de la seguridad (IDCAT). Tal y como se comenta en Magerit v3 la información y los servicios es lo más importante en cuanto a valor nuclear desde el punto de vista del ENS y no debe haber nada más

valioso en el sistema. En base a esto el procedimiento que se ha seguido ha sido incorporar en PILAR la valoración de los activos de información y servicios que se rellenó en las tablas del apartado 4.1 y a continuación arrastrar al resto de elementos dicho valor haciendo que el valor de los activos diferentes a la información y los servicios sea igual al valor acumulado. El uso de los valores acumulados nos permite tener una mejor visión de la importancia de los activos desde un punto de vista global integral ya que un activo por sí mismo puede valer menos que la suma de los activos que tiene por encima.

La valoración de los activos se hizo en virtud de una métrica cualitativa de tipo numérico que se corresponde con los valores asignados a las dimensiones de seguridad en el ENS tal y como se muestra en la siguiente tabla:

Valor en PILAR	Valor en ENS
0	Sin Valorar
1	Bajo
4	Medio
5	Alto

Tabla 5-8. Métrica par avalorar activos en PILAR

En las siguientes imágenes tomadas de PILAR se muestran los resultados de trasladar la valoración del ENS de las dimensiones de seguridad a los activos de información y servicios en ambos sistemas:

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[I] Capa de Información [Negocio]					
[I_ACADE] Información Académica	[1]	[4]	[1]	[1]	[1]
[I_ECONO] Información Económica	[1]	[4]	[1]	[4]	[1]
[I_RRHH] Información sobre Recursos Humanos	[1]	[1]	[4]	[1]	[1]
[I_IDI] Información de Investigación, Desarrollo e Innovación	[1]	[1]	[1]	[1]	[0]
[S] Capa de Servicios [Negocio]					
[S_ACADE] Servicio ERP Académico	[1]	[4]	[1]	[4]	[1]
[S_ECONO] Servicio ERP Económico	[1]	[4]	[1]	[4]	[1]
[S_RRHH] Servicio ERP RRHH	[1]	[1]	[1]	[4]	[1]
[S_IDI] Servicio ERP Investigación, Desarrollo e Innovación	[1]	[1]	[1]	[4]	[0]

Ilustración 5-6. Valoración de la información y lo servicios en PILAR para el sistema ERP

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[I] Capa de Información [Negocio]					
[I_PUBLICACION] Información de publicaciones electrónicas	[4]	[4]	[0]	[4]	[1]
[I_SEDE] Información de hora oficial y acceso a los servicios	[4]	[4]	[0]	[4]	[0]
[I_TRAMITACION] Información de Tramitación electrónica	[1]	[4]	[4]	[4]	[4]
[S] Capa de Servicios [Negocio]					
[S_TABLON] Servicio Tablón Oficial	[4]	[4]	[0]	[4]	[1]
[S_TRAMITACION] Servicio de Tramitación Electrónica	[1]	[4]	[0]	[4]	[4]
[S_SEDE] Servicio de Sede Electrónica	[4]	[4]	[0]	[4]	[1]

Ilustración 5-7. Valoración de la información y lo servicios en PILAR para el sistema AE

Para ver el valor acumulado para el resto de para cada sistema así como las clases asociadas para cada uno de los activos y las relaciones entre los mismos para cada sistema consultar los documentos adjuntos titulados “Modelo de valor activos AE” y “Modelo de valor activos ERP”. En la

guía de elementos de Magerit v3 se pueden consultar los códigos de clases y subclases asociadas a cada activo.

5.4 Identificación y valoración de amenazas

PILAR incorpora el catálogo de amenazas de Magerit v3 las cuales se agrupan en 4 clases principales según su origen:

Clase de Amenaza	Origen	Descripción
[N] Desastres naturales	Natural (accidental)	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
[I] De origen industrial	Entorno (accidental), Humano (accidental o deliberado)	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.
[E] Errores y fallos no intencionados	Humano (accidental)	Fallos no intencionales causados por las personas.
[A] Ataques intencionados	Humano (deliberado)	Fallos deliberados causados por las personas.

Ilustración 5-8. Clases de amenaza en Magerit v3 según su origen

Para cada una de las amenazas del catálogo de Magerit v3 se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

Ilustración 5-9. Cuadro descriptivo de una amenaza en el catálogo de amenazas de Magerit v3

En la siguiente imagen se muestra un ejemplo del contenido de este cuadro para la amenaza de incendio natural no provocado:

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCENDIO	

Ilustración 5-10. Cuadro descriptivo la amenaza [N.1] Fuego del catálogo de amenazas de Magerit v3

Vemos que nos indica los tipos de activos afectados por dicha amenaza así como la dimensión de seguridad del activo a la que afecta que en este caso es la disponibilidad. Así pues la forma de seleccionar las amenazas pasa por ver los activos que se han dado de alta en PILAR y a continuación seleccionar las amenazas del catálogo en base a la clase de activos que tengan asociados los mismos. Para automatizar el proceso PILAR permite automáticamente asociar las amenazas a los activos en base a las clases que tenga asociadas. A continuación se muestra una imagen extraída de PILAR donde se puede ver la pantalla usada para asociar las amenazas a los activos:

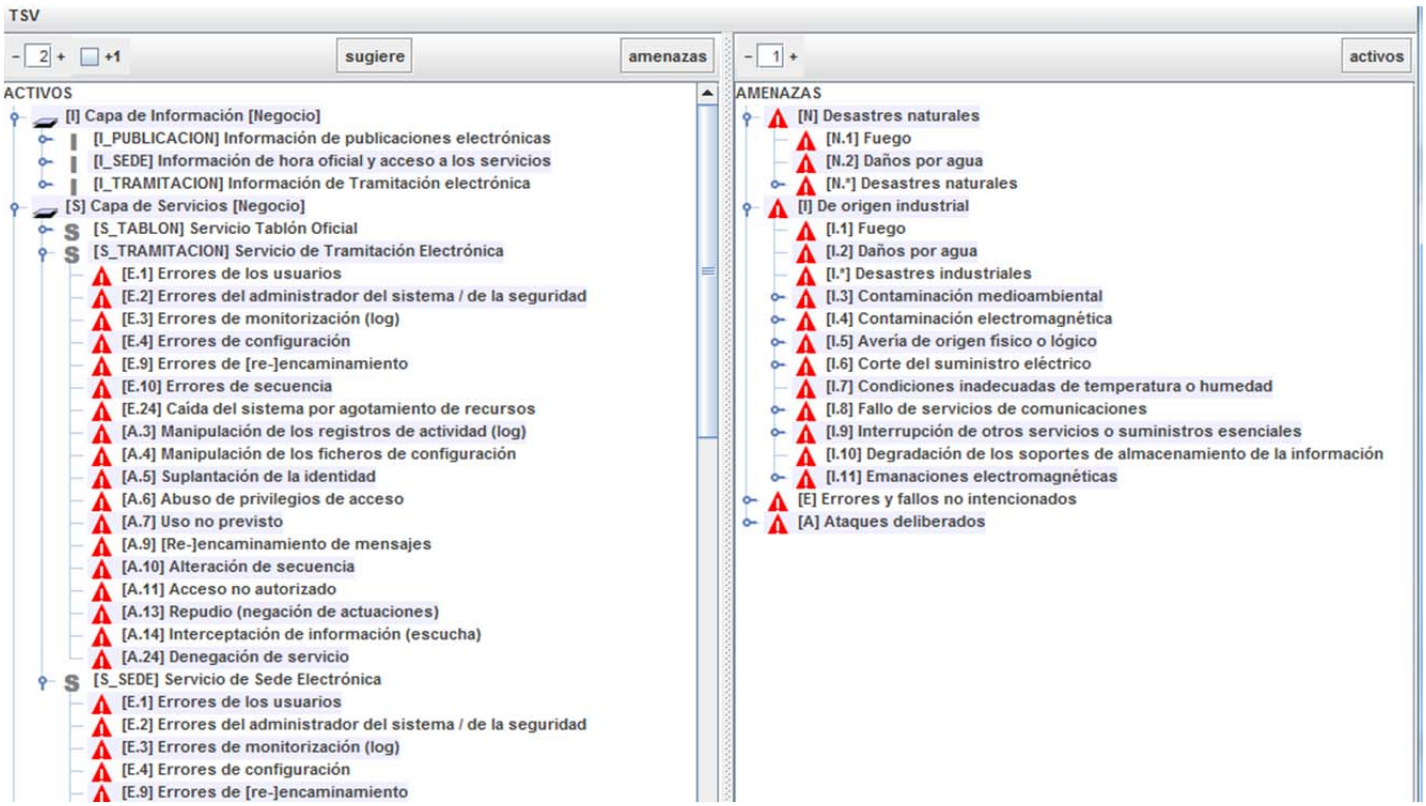

Ilustración 5-11. Asociación de amenazas a activos en PILAR

La valoración de las amenazas en Magerit v3 se hace en base a la frecuencia de ocurrencia y a la degradación que produce en el valor del activo según la siguiente escala:

Frecuencia de ocurrencia	Degradación del valor del activo
100 --> muy frecuente–a diario	**5% -->** Degradación Baja
10 --> frecuente–mensualmente	**30% -->** Degradación Media
1 --> normal–una vez al año	**50% -->** Degradación Alta
1/10 --> poco frecuente – cada varios años	**80% -->** Degradación Muy Alta
1/100--> muy infrecuente–cada varias décadas	**100% -->** Completa

Ilustración 5-12. Métrica para valorar amenazas

A la hora de valorar las amenazas PILAR nos permite seleccionar una serie de condiciones iniciales para el entorno que dan idea de su vulnerabilidad dentro de lo que se conoce como

"Dominios de seguridad". En la siguiente imagen extraída de PILAR se puede ver el menú asociado a esta funcionalidad:

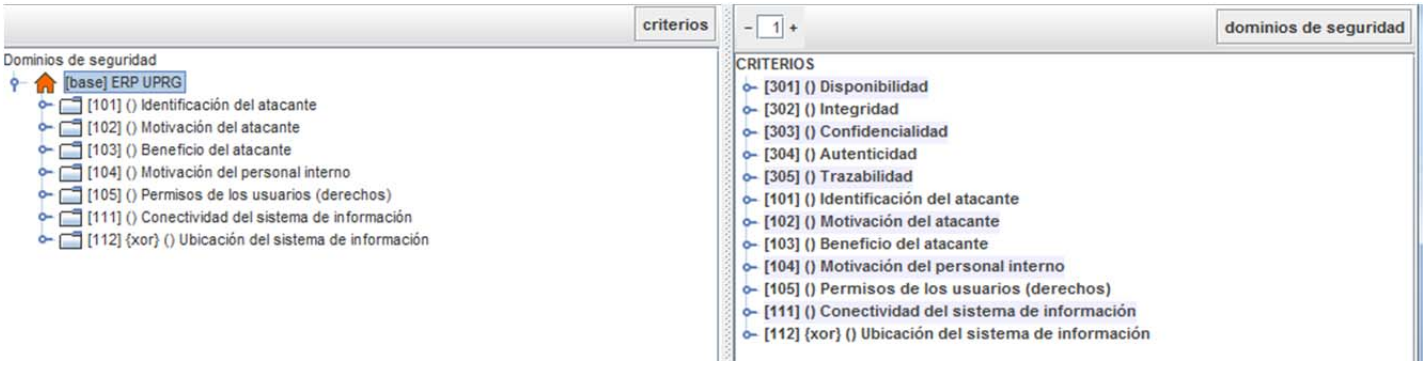

Ilustración 5-13. Dominios de vulnerabilidad en PILAR

Se ha decidido dejar los valores por defecto para que sirvan para Pilar que nos "sugiera" unos valores de frecuencia y degradación adecuados al dominio seleccionado y a partir de estos valores de referencia se introducirán las modificaciones que se consideren oportunas para particularizar cada sistema. A la hora de particular estos valores nos surgen los siguientes inconvenientes:

- Hay que valorar como si no hubiese salvaguardas (algo bastante complicado).
- Falta una base de datos que recoja de forma detallada todo el histórico de incidentes
- Además se puede pensar que hay amenazas que no se han producido nunca cuando en verdad lo que ha pasado es que:
    - Las han parado las salvaguardas que tenemos
    - No se han podido detectar que ocurran con los medios de los que se dispone

En base a estos inconvenientes el método a seguir para dicha valoración se ajustará a lo siguiente:

- Uso de los valores por defecto en los "Dominios de seguridad" para que sea PILAR la que nos sugiera unos valores iniciales sobre los que trabajar
- Reuniones con los empleados de donde sacar experiencia previa
- Cuando no se tiene experiencia previa de que haya sucedido, para el caso de la frecuencia la seleccionamos de acuerdo con lo probable que es que se produzca ese incidente aunque no haya pasado nunca.
- Cuando valoramos la degradación lo hacemos sin tener en cuenta ningún tipo de salvaguarda, por lo que cosas que ya han pasado provocarán una mayor degradación puesto que no está la salvaguarda que protegió en su momento

En la siguiente imagen extraída de PILAR se puede ver la pantalla de valoración de amenazas en donde se introducen los valores de frecuencia y degradación:

activo	frecuencia	[D]	[I]	[C]	[A]	[T]
ACTIVOS						
[I] Capa de Información [Negocio]						
[I_PUBLICACION] Información de publicaciones electrónicas		80%	100%		100%	50%
[E.1] Errores de los usuarios	10	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	30%	10%			
[E.3] Errores de monitorización (log)	1					10%
[E.4] Errores de configuración	1	10%	10%		30%	10%
[E.18] Destrucción de la información	1	10%				
[A.3] Manipulación de los registros de actividad (log)	1					50%
[A.4] Manipulación de los ficheros de configuración	1	50%	10%		10%	30%
[A.5] Suplantación de la identidad	1		50%		100%	
[A.6] Abuso de privilegios de acceso	0,1		30%			
[A.15] Modificación de la información	0,1		100%			
[A.18] Destrucción de la información	0,1	80%				
[I_SEDE] Información de hora oficial y acceso a los servicios		80%	100%		100%	50%
[E.1] Errores de los usuarios	1	10%	10%			
[E.2] Errores del administrador del sistema / de la seguridad	1	30%	10%			
[E.3] Errores de monitorización (log)	1					10%
[E.4] Errores de configuración	1	10%	10%		30%	10%
[E.18] Destrucción de la información	0,1	10%				
[A.3] Manipulación de los registros de actividad (log)	0,1					50%
[A.4] Manipulación de los ficheros de configuración	1	50%	10%		10%	30%
[A.5] Suplantación de la identidad	1		50%		100%	
[A.6] Abuso de privilegios de acceso	0,1		30%			
[A.15] Modificación de la información	0,1		100%			
[A.18] Destrucción de la información	0,1	80%				
[I_TRAMITACION] Información de Tramitación electrónica		80%	100%	100%	100%	50%
[E.1] Errores de los usuarios	10	10%	10%	10%		

Ilustración 5-14. Valoración de amenazas en PILAR

Las amenazas seleccionadas para cada activo junto con la valoración para cada una se pueden consultar en los documentos adjuntos titulados “Informe amenazas AE” y “Informe amenazas ERP”

5.5 Impacto y riesgo potencial

Una vez realizada la valoración de los activos y de las amenazas, PILAR se encarga de calcular los valores de impacto y riesgo acumulado y repercutido. En las siguientes imágenes extraídas de PILAR podemos ver como ejemplo los valores de impacto y riesgo acumulados para el sistema de AE:

activo	amenaza	dimensión	impacto
[I_PUBLICACION] Información de publi...	[A.15] Modificación de la información	[I]	[4]
[I_PUBLICACION] Información de publi...	[A.5] Suplantación de la identidad	[A]	[4]
[I_PUBLICACION] Información de publi...	[A.18] Destrucción de la información	[D]	[4]
[I_PUBLICACION] Información de publi...	[A.5] Suplantación de la identidad	[I]	[3]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[D]	[3]
[I_PUBLICACION] Información de publi...	[E.2] Errores del administrador del si...	[D]	[2]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[A]	[2]
[I_PUBLICACION] Información de publi...	[A.6] Abuso de privilegios de acceso	[I]	[2]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[D]	[1]
[I_PUBLICACION] Información de publi...	[E.1] Errores de los usuarios	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.18] Destrucción de la información	[D]	[1]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[A]	[1]
[I_PUBLICACION] Información de publi...	[E.2] Errores del administrador del si...	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[I]	[1]
[I_PUBLICACION] Información de publi...	[E.1] Errores de los usuarios	[D]	[1]
[I_PUBLICACION] Información de publi...	[A.3] Manipulación de los registros d...	[T]	[0]
[I_PUBLICACION] Información de publi...	[A.4] Manipulación de los ficheros de ...	[T]	[0]
[I_PUBLICACION] Información de publi...	[E.4] Errores de configuración	[T]	[0]
[I_PUBLICACION] Información de publi...	[E.3] Errores de monitorización (log)	[T]	[0]
[I_SEDE] Información de hora oficial y ...	[A.5] Suplantación de la identidad	[A]	[4]
[I_SEDE] Información de hora oficial y ...	[A.15] Modificación de la información	[I]	[4]
[I_SEDE] Información de hora oficial y ...	[A.18] Destrucción de la información	[D]	[4]
[I_SEDE] Información de hora oficial y ...	[A.5] Suplantación de la identidad	[I]	[3]
[I_SEDE] Información de hora oficial y ...	[A.4] Manipulación de los ficheros de ...	[D]	[3]
[I_SEDE] Información de hora oficial y ...	[E.4] Errores de configuración	[A]	[2]
[I_SEDE] Información de hora oficial y ...	[A.6] Abuso de privilegios de acceso	[I]	[2]
[I_SEDE] Información de hora oficial y ...	[E.2] Errores del administrador del si...	[D]	[2]
[I_SEDE] Información de hora oficial y ...	[A.4] Manipulación de los ficheros de ...	[I]	[1]

Ilustración 5-15. Impacto acumulado en PILAR por activo, amenaza y dimensión

activo	amenaza	dimensión	riesgo
[I_TRAMITACION] Información de Tra...	[A.5] Suplantación de la identidad	[A]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.6] Abuso de privilegios de acceso	[D]	{4,2}
[S_TRAMITACION] Servicio de Tramita...	[A.5] Suplantación de la identidad	[A]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.19] Revelación de información	[C]	{4,2}
[ALM.HW_NETALM] Red de Almacena...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[D]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[D]	{4,2}
[NETTOP.NETTOP_USUARIOS] LAN - Zo...	[A.24] Denegación de servicio	[D]	{4,2}
[I_TRAMITACION] Información de Tra...	[A.19] Revelación de información	[C]	{4,2}
[NETHW.NETHW_ROUTER_PERIMETRAL...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SRVWEB] Cluster de 6 VMs para s...	[A.14] Interceptación de información (...	[T]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.18] Destrucción de la información	[D]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[C]	{4,2}
[H_SGBD] Cluster de 3 host físicos de...	[A.5] Suplantación de la identidad	[A]	{4,2}
[IT_CORREO] Servicio de Correo Elect...	[A.5] Suplantación de la identidad	[C]	{4,2}
[IT_CORREO] Servicio de Correo Elect...	[A.14] Interceptación de información (...	[C]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[I]	{4,2}
[NETHW.NETHW_ROUTER_PERIMETRAL...	[A.24] Denegación de servicio	[D]	{4,2}
[IT_DIRECTORIO] Servicio LDAP	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_DNS_NTP] Cluster de 3 VMs para D...	[A.22] Manipulación de programas	[T]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[I]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.15] Modificación de la información	[I]	{4,2}
[NETHW.NETHW_ROUTER_INTERNO] Eq...	[A.5] Suplantación de la identidad	[A]	{4,2}
[A_TRAMITACION] Aplicación Tablón E...	[A.5] Suplantación de la identidad	[A]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.5] Suplantación de la identidad	[C]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[I]	{4,2}
[ALM.HW_CABINA] Cabina de Almace...	[A.4] Manipulación de los ficheros de ...	[C]	{4,2}
[H_SSO] Clusters de 3 VMs para servi...	[A.4] Manipulación de los ficheros de ...	[T]	{4,2}
[H_DIRECTORIO] Clúster de 3 VMs de ...	[A.5] Suplantación de la identidad	[A]	{4,2}

Ilustración 5-16. Riesgo acumulado en PILAR por activo, amenaza y dimensión

Vemos que PILAR ha calculado los valores de impacto y riesgo por cada amenaza que afecta a una de las dimensiones de un activo algo que si se tuviera que hacer de forma manual resultaría muy pesado. Vemos que a la hora de mostrar los valores de impacto y riesgo usa una escala de valores incluyendo colores que se corresponde con la siguiente y que se denomina “niveles de criticidad”:

Ilustración 5-17. Niveles de criticidad en PILAR

La valoración para ambos sistemas de todos los impactos y riesgos acumulados y repercutidos se puede consultar en los documentos adjuntos titulados “Análisis de riesgos potenciales AE” y “Análisis de riesgos potenciales ERP”.

5.6 Identificación y valoración de Salvaguardas. Auditoría interna

En este punto del análisis de riesgos se identificarán y evaluará el grado de implantación las salvaguardas con los que cuenta la organización. Para ello se llevará a cabo una auditoría interna ordinaria que nos permitirá identificar las salvaguardas y recopilar las evidencias necesarias para justificar el nivel de implantación de las mismas. Se usará PILAR para reflejar dichas salvaguardas así como su grado de implantación.

A la hora de identificar salvaguardas PILAR contempla salvaguardas y grupos de salvaguardas que se pueden clasificar en función de diferentes criterios:

Criterio	Valores
1 .- Aspecto que se protegerá	• **G:** Aspecto de gestión. • **T:** Aspecto técnico: medidas más concretas que la de gestión • **P:** Aspecto de Personal. • **F:** Aspecto de Seguridad física (instalaciones)
2.- Estrategia que adopta la salvaguarda ante el incidente:	• **CR:** Correctivas (gestión de incidentes) • **IM:** Minimizar impacto (desconexión de equipos) • **RC:** Recuperación del incidente (copias de seguridad) • **DT:** Detección (detectores de incendios) • **MN:** Monitorización (registros de actividad) • **EL:** Eliminación (Eliminar cuentas de usuarios que ya no emplean) • **PR:** Preventiva (autorización previa de usuarios) • **DR:** Disuasoria (vallas, guardias de seguridad) • **AD:** Administrativas (inventario de activos) • **AW:** Concienciación (cursos de concienciación) • **std:** basadas en normas • **proc:** basadas en procedimientos • **cert:** basadas en productos certificados (Firewalls)
3 .- Clase de activo que protegerá (Grupo principal/raíz)	

4.- Importancia de la salvaguarda:	
5.- Forma en la que se aplica:	• **{and}:** Deberían aplicarse todas las salvaguardas. • **{or}:** Debería aplicarse al menos una de las salvaguardas • **{xor}:** Debería aplicarse sólo una de las salvaguardas (la que mejor aplique à la más recomendada).
6.- Recomendación de su implantación:	• **1 (blanco):** no recomendable por que no aplica • **2,3 (azul):** recomendable • **4,5 (amarillo):** bastante recomendable • **6,7 (rojo pálido):** muy recomendable • **8,9 (rojo):** necesaria
7.- Consideración sobre su aplicación:	• **[Vacío]:** Aplica la salvaguarda o no, según tenga configurado en las "Opciones". • **n.a.:** No aplica la salvaguarda y, por lo tanto, no se mostrará a la hora de evaluar las salvaguardas. Si se la pongo a un grupo afecta a todo lo que hay por debajo • **…:** Indica que se trata de un grupo de salvaguardas que contiene a alguna salvaguarda en "n.a.".
8.- Consideración sobre su estado:	• **On**: Quiero usarla para el análisis • **Off**: Aunque aplique a mi sistema, en este análisis no la quiero considerar

Tabla 5-9. Criterios de Valoración de Salvaguardas en PILAR

Dichas salvaguardas también permiten las siguientes consideraciones sobre su aplicación y su estado:

Consideración	Valores
1.- Aplicación	• **[Vacío]:** Aplica la salvaguarda o no, según tenga configurado en las "Opciones". • **n.a.:** No aplica la salvaguarda y, por lo tanto, no se mostrará a la hora de evaluar las salvaguardas. Si se la pongo a un grupo afecta a todo lo que hay por debajo • **…:** Indica que se trata de un grupo de salvaguardas que contiene a alguna salvaguarda en "n.a.".

2.- Uso en el análisis	• **On**: Quiero usarla para el análisis • **Off**: Aunque aplique a mi sistema, en este análisis no la quiero considerar

Tabla 5-10. Consideraciones sobre Salvaguardas en PILAR

A la hora de seleccionar las salvaguardas PILAR presenta una cantidad muy elevada de las mismas de las cuales para el presente análisis de Riesgos me interesan únicamente las que se aplican al ENS. LA forma de quedarse con estas salvaguardas es aplicar lo que en PILAR se denomina un perfil de seguridad Usar perfil de seguridad del ENS que consiste en una selección de un subconjunto de salvaguardas que se ofrecen en Pilar y que son de aplicación al ENS. Además PILAR distingue dentro del perfil ENS entre los siguientes apartados:

Apartado	Descripción
Controles	Se corresponden con los apartados principales que aparecen en la normativa del ENS. Sirven para agrupar preguntas y salvaguardas
Preguntas	Se corresponden con los comentarios y subapartados que aparecen en la norma del ENS. Sirven para evaluar el nivel de cumplimiento de la norma pero no tienen influencia sobre los valores del riesgo
Salvaguardas	Se corresponden con las que aparecen en el apartado T.2.1 y que Pilar ha seleccionado para dar cumplimiento a los controles y preguntas de la norma. Si tiene una influencia sobre los valores del riesgo

Tabla 5-11. Apartados en el perfil de seguridad ENS de PILAR

PILAR nos permite indicar las siguientes consideraciones sobre la aplicación de los controles y preguntas:

Consideración	Valores
Aplicación de controles y preguntas	• **M:** Es obligatorio a cumplir según la norma. • **[Vacío]:** Es un control que no hay que cumplir según el nivel de la dimensión o se trata de un grupo de controles donde hay uno que no tiene que cumplirla. Ejemplo: [mp.if.9] Instalaciones alternativas • **Gris:** No tiene que cumplir según la norma porque no se han incluido categorías de activos que contempla esa norma Ejemplos: [mp.eq.3] Equipos portátiles • **n.a.:** Es obligatorio según la norma pero en nuestro caso se dan condiciones por las que no se va a cumplir à no influye sobre la gestión del riego

Tabla 5-12. Consideraciones sobre aplicación de controles y preguntas en el perfile ENS de PILAR

En lo que se refiere al grado de implantación de las salvaguardas PILAR de acuerdo con Magerit v3 utiliza niveles de madurez según el modelo de madurez (CMM) usado para calificar la madurez de procesos:

eficacia	nivel	significado	administrativo
0%	**L0**	inexistente	inexistente
10%	**L1**	inicial / ad hoc	iniciado
50%	**L2**	reproducible, pero intuitivo	parcialmente realizado
90%	**L3**	proceso definido	en funcionamiento
95%	**L4**	gestionado y medible	monitorizado
100%	**L5**	optimizado	mejora continua

Tabla 5-13.Escala de niveles de madurez de Salvaguardas en PILAR

Así pues en base a Magerit v3 y usando la herramienta PILAR se ha llevado a cabo una auditoría interna en la cual se han identificado los siguientes niveles de madurez para cada uno de los controles de seguridad recogidos en el Anexo II del ENS y que corresponde a sistemas con categoría media. Esta valoración se ha hecho de forma global sin diferenciar entre sistemas identificando únicamente si la medida es o no de obligaría implementación de acuerdo al nivel o categoría del sistema y sus dimensiones de seguridad. Así pues tras realizar dicha auditoría los valores de madurez de los controles de seguridad del ENS a fecha de Mayo de 2017 son:

Código	Descripción	Nivel de madurez	Sistema ERP	Sistema AE
org.1	Política de seguridad	L0-L3	aplica	aplica
org.2	Normativa de seguridad	L0-L1	aplica	aplica
org.3	Procedimiento de seguridad	L1	aplica	aplica
org.4	Proceso de autorización	L0-L2	aplica	aplica
op.pl.1	Análisis de riesgos	L3	+	+
op.pl.2	Arquitectura de seguridad	L0-L2	aplica	aplica
op.pl.3	Adquisición de nuevos componentes	L0-L2	aplica	aplica
op.pl.4	Dimensionamiento / Gestión de capacidades	L1-L2	n.a	aplica
op.pl.5	Componentes certificados	L0	n.a	n.a
op.acc.1	Identificación	L2	aplica	aplica
op.acc.2	Requisitos de acceso	L2	aplica	aplica
op.acc.3	Segregación de funciones y tareas	L2	aplica	aplica
op.acc.4	Proceso de gestión de derechos de acceso	L2	aplica	aplica
op.acc.5	Mecanismo de autenticación	L2	+	+
op.acc.6	Acceso local (local logon)	L0-L2	+	+
op.acc.7	Acceso remoto (remote login)	L0-L2	+	+
op.exp.1	Inventario de activos	L2	aplica	aplica

op.exp.2	Configuración de seguridad	L1	aplica	aplica
op.exp.3	Gestión de la configuración	L1-L2	aplica	aplica
op.exp.4	Mantenimiento	L1	aplica	aplica
op.exp.5	Gestión de cambios	L1-L2	aplica	aplica
op.exp.6	Protección frente a código dañino	L1-L2	aplica	aplica
op.exp.7	Gestión de incidencias	L1	aplica	aplica
op.exp.8	Registro de la actividad de los usuarios	L0-L1	n.a	n.a
op.exp.9	Registro de la gestión de incidencias	L1	aplica	aplica
op.exp.10	Protección de los registros de actividad	L0-L1	n.a	n.a
op.exp.11	Protección de claves criptográficas	L1-L2	aplica	aplica
op.ext.1	Contratación y SLAs	L3	aplica	aplica
op.ext.2	Gestión diaria	L0-L1	aplica	aplica
op.ext.9	Medios alternativos	L0	n.a	n.a
op.cont.1	Análisis de impacto	L1	n.a	n.a
op.cont.2	Plan de continuidad	L0	n.a	n.a
op.cont.3	Pruebas periódicas	L0	n.a	n.a
op.mon.1	Detección de intrusión	L2	aplica	aplica
op.mon.2	Sistema de métricas	L0-L3	n.a	n.a
mp.if.1	Áreas separadas y con control de acceso	L1-L3	aplica	aplica
mp.if.2	Identificación de las personas	L3	aplica	aplica
mp.if.3	Acondicionamiento de los locales	L3	aplica	aplica
mp.if.4	Energía eléctrica	L3	aplica	+
mp.if.5	Protección frente a incendios	L3	aplica	aplica
mp.if.6	Protección frente a inundaciones	L0-L2	n.a	aplica
mp.if.7	Registro de entrada y salida de equipamiento	L0	aplica	aplica
mp.if.9	Instalaciones alternativas	L0	n.a	n.a
mp.per.1	Caracterización del puesto de trabajo	L1-L2	aplica	aplica
mp.per.2	Deberes y obligaciones	L2	aplica	aplica
mp.per.3	Concienciación	L1	aplica	aplica
mp.per.4	Formación	L0-L2	aplica	aplica
mp.per.9	Personal alternativo	L0	n.a	n.a
mp.eq.1	Puesto de trabajo despejado	L1-L2	+	+
mp.eq.2	Bloqueo de puesto de trabajo	L1	aplica	aplica
mp.eq.3	Protección de equipos portátiles	L1	aplica	aplica
mp.eq.9	Medios alternativos	L0	n.a	aplica
mp.com.1	Perímetro seguro	L3	aplica	aplica
mp.com.2	Protección de la confidencialidad	L3	aplica	aplica
mp.com.3	Protección de la autenticidad y de la integridad	L3	+	+
mp.com.4	Segregación de redes	L3	n.a	n.a
mp.com.9	Medios alternativos	L3	n.a	n.a
mp.si.1	Etiquetado	L2	aplica	aplica

mp.si.2	Criptografía	L2	aplica	aplica
mp.si.3	Custodia	L2	aplica	aplica
mp.si.4	Transporte	L2	aplica	aplica
mp.si.5	Borrado y destrucción	L0	aplica	aplica
mp.sw.1	Desarrollo	L2-L3	aplica	aplica
mp.sw.2	Aceptación y puesta en servicio	L2	+	+
mp.info.1	Datos de carácter personal	L1-L2	aplica	aplica
mp.info.2	Calificación de la información	L1-L2	+	+
mp.info.3	Cifrado	L0	n.a	n.a
mp.info.4	Firma electrónica	L0-L2	+	+
mp.info.5	Sellos de tiempo	L0-L2	n.a	n.a
mp.info.6	Limpieza de documentos	L0	aplica	aplica
mp.info.9	Copias de seguridad (backup)	L2-L3	aplica	aplica
mp.s.1	Protección del correo electrónico	L0-L3	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	L1-L2	+	+
mp.s.8	Protección frente a la denegación de servicio	L2	n.a	aplica
mp.s.9	Medios alternativos	L2	n.a	n.a

Tabla 5-14. Niveles de madurez de los controles de seguridad

A continuación se muestra una tabla que presenta el nivel de madurez y el grado de cumplimiento actual del ENS por cada sistema agrupado por categorías de medidas teniendo en cuenta los controles que les son de obligado cumplimiento por cada sistema en base a su categoría y el nivel de sus dimensiones de seguridad:

Sistema	Familia de Medidas	Valoración actual	
		Nivel de madurez	Porcentaje de cumplimiento
Sistema ERP	Medidas Organizativas	L0-L3	26%
	Medidas Operativas	L0-L3	37%
	Medidas Técnicas	L0-L3	48%
	Cumplimiento total	**L0-L3**	**37%**

Tabla 5-15. Sistema ERP: Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

Sistema	Familia de Medidas	Valoración actual	
		Nivel de madurez	Porcentaje de cumplimiento
Sistema AE	Medidas Organizativas	L0-L3	26%
	Medidas Operativas	L0-L3	37%
	Medidas Técnicas	L0-L3	47%
	Cumplimiento total	**L0-L3**	**37%**

Tabla 5-16. Sistema AE: Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

El documento anexo "Informe de Auditoría" contiene el grado de madurez y porcentaje de cumplimiento de cada medidas así como la justificación de su valor para cada uno de los controles en base a las evidencias recogidas.

Vemos como en ambos sistemas tanto el nivel de madurez de las medidas como el nivel de cumplimiento global del ENS es del 35%. En base a estos valores podemos sacar en conclusión que ambos sistemas evaluados presenta una madurez media-baja en la gestión de la seguridad de la información, detectándose un esfuerzo significativo en el desarrollo de los principios básicos exigibles por parte del Esquema Nacional de Seguridad como el desarrollo de una política de seguridad , así como la existencia de gran parte de las medidas de protección técnicas a nivel de red. Sin embargo, el sistema presenta deficiencias muy significativas en dos grandes áreas:

- Deficiencias muy significativas en las medidas de seguridad exigibles en la explotación diaria del sistema por parte de la unidad de TI debido en parte a la falta de la existencia de una normativa de seguridad a nivel de toda la organización.

- Deficiencias muy significativas en las medidas asociadas a protección de los recursos informáticos del personal de la Organización y aquellas derivadas de la importancia de la concienciación y formación en materia de seguridad de la información.

Seguridad en la explotación del sistema de información:

Estas medidas atañen fundamentalmente a la unidad de TI y están estrechamente relacionadas con la capacidad de la misma para atender las necesidades de seguridad de la información que el trabajo diario requiere: configuración y mantenimiento de sistemas seguros, seguimiento de vulnerabilidades, actualización y aplicación de parches de seguridad, homogeneidad en la gestión de la seguridad, aplicación proactiva de la seguridad, etc.

Estas medidas, en contra de otro tipo de medidas que tienen una naturaleza muy técnica, están principalmente ligadas a la disponibilidad de personal para atender esta gestión.

Medidas de protección del personal y sus recursos informáticos:

Estas medidas atañen a la organización en su conjunto, y trascienden con mucho, el alcance de la Unidad de TI como garante de la seguridad de los sistemas de información. Las medidas de protección de la información gestionada por el personal y sus recursos informáticos, están íntimamente relacionadas con dos aspectos:

- La capacidad de la organización de involucrarse globalmente en la gestión de la seguridad de la información

- La existencia de acciones de formación y concienciación sobre el personal.

Únicamente la existencia de ambos aspectos permitirá desplegar medidas de seguridad sobre los recursos informáticos del personal (equipos, soportes, portátiles, teléfonos, etc.); así como prevenir que el personal sea víctima de ataques informáticos sobre la información que gestiona (virus, troyanos, robos de información, etc.).

5.7 Impacto y Riesgo residuales

Los valores residuales de impacto y riesgo para los activos se corresponden con los valores resultantes una vez que se considera la aplicación de las salvaguardas con un determinado nivel de madurez. En este apartado es necesario aclarar la diferencia entre el grado de cumplimiento del ENS que se ha estimado en el apartado 5.6 como resultado de la auditoría interna y los valores de impacto y riesgo residual resultantes de aplicar en nuestro análisis de riesgos los niveles de madurez evaluados en dicha auditoría interna. En el RD 3/2010 los controles que indica el ENS como obligatorios para un sistema en función de su categoría y nivel de dimensiones de seguridad se deben considerar como los mínimos requeridos de cara a determinar el grado de cumplimiento del ENS. Así pues el hecho de que un control no sea de obligado cumplimiento para el nivel de un sistema no quiere decir que no se pueda usar en dicho sistema contribuyendo a reducir el riesgo residual.

En base a esto PILAR permite diferenciar entre los valores de riesgo residual resultantes de aplicar una determinada medida de seguridad y el grado de cumplimiento de una normativa (en nuestro caso el RD 3/2010). Por ejemplo el uso de medios alternativos para proteger los servicios al ser una medida de aplicación únicamente a los sistemas de nivel alto no es tenida en cuenta por PILAR a la hora de aumentar o disminuir el grado de cumplimiento del ENS por parte de dicho sistema pero sí se considera su contribución en la reducción del riesgo en los resultados del informe de análisis de riesgos.

Centrándonos en los resultados obtenidos para estos valores residuales en el Análisis de Riesgos de los sistemas de la UPRG y en base al grado , nos encontramos con los siguientes aspectos que merece la pena destacar:

- La UPRG cuenta con un sistema de información heterogéneo, enfocado a la prestación de servicios a la comunidad universitaria. Este sistema de información está gestionado desde unos principios básicos donde la usabilidad, la operativa abierta y la correcta funcionalidad son fundamentales y donde la seguridad, hasta la fecha, no ha sido una directriz transversal, sino un conjunto de medidas de aplicación puntual realizadas por el personal de la sección de TI en respuesta a sus propias necesidades.

- Nos encontramos en un entorno donde globalmente la exigencia en materia de seguridad es de nivel medio, medio-bajo.

- Como consecuencia del primer punto, se detectó baja madurez y baja homogeneidad en las salvaguardas existentes.

- Estamos valorando tres dimensiones por encima del resto:

    - Integridad y autenticidad, tanto del servicio como de la información,

    - Confidencialidad de la información.

    - La disponibilidad aparece más vinculada a la imagen y a la reputación que a una necesidad efectiva por exigencias del negocio.

- Por último la trazabilidad permanece como una dimensión secundaria excepto que actualmente está cobrando protagonismo en los servicios de administración electrónica.

- Aunque no nos encontremos en un entorno de seguridad con exigencias altas, la existencia de algunas dimensiones concretas con exigencias medias, sumada a la ausencia de homogeneidad en las salvaguardas, deriva en la existencia de riesgos altos o muy altos para la totalidad de las dimensiones, según la dominancia del sistema.

- Como muestra de esto último, presentamos un conjunto de gráficos que indican el nivel de riesgo de cada uno de los sistemas; los ejes representan a cada una de las dimensiones de seguridad y la escala es de 0 (nivel de riesgo nulo) a 5,5 (nivel de riesgo total).

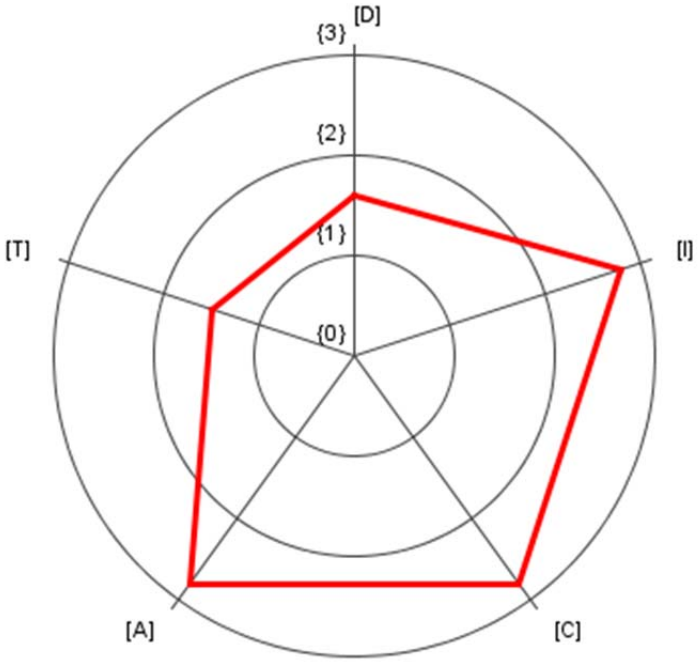

Ilustración 5-18. Riesgo acumulado. Sistema ERP

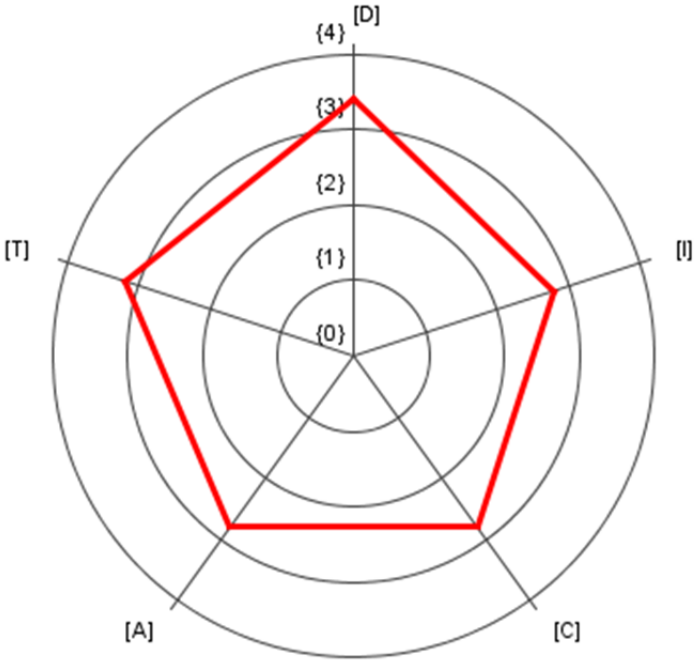

Ilustración 5-19. Riesgo acumulado. Sistema AE

El informe detallado con todos los valores acumulados y repercutidos del análisis de riesgos se puede consultar en los documentos adjuntos titulados “Análisis de riesgos AE” y “Análisis de riesgos ERP. Estos documentos incluyen también los valores deseados después de la aplicación de Plan de mejora de seguridad que se trata en el siguiente apartado.

6 Plan de mejora de la Seguridad

El Análisis de Riesgos no ha permitido realizar una prospección y determinar los niveles de riesgo de nuestro sistema después de haber aplicado un conjunto de medidas y salvaguardas. El establecimiento de un plan para la mejora de la seguridad basado en realizar un tratamiento de riesgos y la implantación de unas salvaguardas alineadas completamente con el ENS y sus criterios de aplicación nos servirá, además de para lograr el cumplimiento formal del ENS, para realizar una valoración del mismo y de su efectividad en la reducción del riesgo en la organización.

Tomando como punto de partida por un lado el informe de auditoría interna usado para valorar el nivel de madurez de las salvaguardas y el grado de cumplimiento del ENS (las evidencias, opiniones y recomendaciones reflejadas en el informe) y por el otro las conclusiones del análisis de riesgos una vez aplicada la valoración de todas las salvaguardas existentes se propone el siguiente plan de actuación para la mejora de la gestión de la seguridad de las TI en la organización.

6.1 Alcance y Objetivos

Analizadas las conclusiones del informe de auditoría, las actuaciones definidas en este plan deben ir orientadas a mejorar en dos áreas fundamentales:

- **La gestión interna del Sistema**, que se refiere a aspectos sobre la organización interna del trabajo y la gestión de la Seguridad en la sección de TI.

- **El Gobierno corporativo de la Seguridad TI**, desarrollando normativas de seguridad para el tratamiento de la información y fomentando acciones corporativas de concienciación y formación en Seguridad TI.

Además, en este plan también se incluye un conjunto de actuaciones, que no están recogidas dentro de ninguno de los puntos anteriores, pero que nos permitirán mejorar el nivel de madurez de algunas medidas del ENS en las que así se requiera. Por lo tanto, las actuaciones incluidas en este plan están orientadas al cumplimiento de los siguientes objetivos generales:

- **Gestión interna del Sistema**. Incluyendo aspectos como:

    - Redacción de los procedimientos de seguridad a seguir por los empleados de TI para la gestión de la seguridad

    - Configurar sistemas seguros, manteniéndolos en el tiempo, reportando y registrando los incidentes de seguridad que se vayan produciendo sobre estos sistemas

- **Gobierno corporativo de la Seguridad**. Se deberá abordar:

    - Redactar y difundir normativas de seguridad de obligado cumplimiento por todos los miembros de la organización

  - Definir y poner en marcha medidas organizativas y corporativas de concienciación y formación (tanto de usuarios como de técnicos) y también de calificación de la información.

- **Otras acciones concretas** para mejorar el nivel de madurez en medidas del marco de protección y de operación tales como la mejora del acondicionamiento del CPD o la destrucción y borrado de soportes.

Aparte, también se han definido algunas deficiencias como “no asumibles” o difíciles de asumir debido a distintas circunstancias:

- **Registro de E/S de equipamiento:** La flexibilidad requerida tanto por alumnos como por PID hace inviable el llevar un registro continuo y autorizado de los dispositivos móviles y soportes que entran o salen de las instalaciones. Lo que si se hará será mantener actualizado un inventario de los diferentes equipos y la persona responsable final del mismo.

- **Protección frente a las inundaciones:** La capacidad presupuestaria y organizativa de la entidad puede llegar a condicionar la mejora de las instalaciones actuales

- **Equipamiento alternativo:** La capacidad presupuestaria y organizativa de la entidad puede llegar a condicionar la mejora de este aspecto.

Las acciones definidas en este plan se ejecutarán a partir del 1 de Octubre de 2017 y finalizarán el 31 de Septiembre de 2019, momento en el cual se realizará una auditoría para medir y analizar los resultados obtenidos.

6.2 Plan de actuación

Las acciones se van a estructurar en tres bloques, correspondiendo cada uno de ellos con los objetivos generales definidos en el punto anterior.

Código	Bloque
B1	Gestión Interna de la seguridad
B2	Gestión Corporativa de la seguridad
B3	Acciones para madurez de medidas concretas

Tabla 6-1. Bloques de acciones del Plan de Seguridad

Dentro de cada bloque, el orden en el que se presentan las medidas es significativo sobre su prioridad estableciéndose además los siguientes plazos para tener cada una de las tareas:

Plazos	Duración (a ejecutar antes de)
corto	6 meses
medio	1 año
largo	2 años

Tabla 6-2. Plazos del Plan de Seguridad

A continuación se presentan dichas tareas ordenadas por bloques, según orden propuesto de prioridad y plazos de ejecución de cada una:

Código (Bloque.Prioridad)	Tarea	Descripción	plazos
B1.1	Mejora de procedimiento de Gestión del Cambio	La sección de TI deberá revisar y mejorar su procedimiento de Gestión del cambio (basado en ITIL) de tal forma que permita gestionar conjuntamente los aspectos que cubre hasta ahora, y que incluya al menos los siguientes aspectos: • Información de capacidad para dimensionamiento sistemático de los cambios que se quieran implementar. • Garantizar la actualización del actual de Inventario de Activos (CMDB) y del responsable de cada uno de ellos.. • Definir un ciclo de cambio-entrega que garantice la ejecución de pruebas, previas a la puesta en explotación. • Gestionar actualizaciones de seguridad de los activos (al menos de los más críticos o de las actualizaciones más importantes) mediante este proceso. • Revisión del proceso y mejora según la experiencia hasta el momento.	corto
B1.2	Gestión de incidentes de seguridad	La sección de TI deberá implantar un proceso y herramienta para la gestión de incidentes de seguridad, basado en la herramienta LUCIA, adaptada para el ENS por el CCN-CERT.	corto

B1.3	Procedimientos de seguridad	Los responsables del Sistema deberán redactar los siguientes procedimientos por escrito y ponerlos en conocimiento del personal responsable y encargado de su ejecución: • Procedimiento de Gestión de Usuarios: altas, bajas, identificación, autenticación y control de acceso lógico los cambios que se quieran implementar. • Procedimiento de clasificación y tratamiento de la información clasificada del correo electrónico • Procedimiento de generación de copias de respaldo y de recuperación de la información	corto
B1.4	Protección de aplicativos web	Los responsables del Sistema deberán mejorar la protección de aplicativos web, implementando de forma sistematizada varias capas de seguridad: filtrado en cabecera de red (cortafuegos) y técnicas de filtrado a nivel de aplicación y/o servidor	corto
B1.5	Arquitectura de seguridad	El responsable de seguridad deberá redactar un Documento de Arquitectura de seguridad, según lo especificado en el ENS.	corto
B1.6	Gestión de claves privadas	Los responsables del Sistema deberán definir un procedimiento para la gestión de claves privadas de servidores y sello de órgano (solicitudes CSR y gestión de certificados: generación, custodia en explotación, etc.).	corto
B2.1	Difundir política de seguridad	El Equipo de Gobierno, los Responsables del Sistema y el Responsable de Seguridad deberán revisar y actualizar la Política de la UPRG y darle máxima difusión dentro de la Universidad.	corto

B2.2	Normativas de seguridad	El Equipo de Gobierno, los Responsables del Sistema y el Responsable de Seguridad deberán redactar al menos las siguientes normativas de seguridad y darle máxima difusión dentro de la Universidad. • Deberes y obligaciones del personal en materia de seguridad y las consecuencias su incumplimiento • Uso correcto de equipos, servicios e instalaciones y lo que se considera un uso indebido. • Política de contraseñas de la UPRG	corto
B2.3	Política de calificación de la información	El equipo de Gobierno deberá aprobar una Política de calificación de la información y lo que se puede o no se puede hacer con ella, partiendo de la base de lo que ya hay establecido para el ENS y el cumplimiento de la LOPD. La política debe cubrir aspectos tales como: • Calificación de la información, según su grado de confidencialidad. • Condiciones en el tratamiento de cada tipo de información, según su calificación. • Requisitos para la transmisión de la información. • Restricciones sobre la difusión y almacenamiento.	medio
B2.4	Política de firma y de sellado de tiempo	El Equipo de Gobierno deberá aprobar una Política de Firma y sellado de tiempo que explicite los motivos por los que la información debe, o no, ser firmada digitalmente y los mecanismos usados para ello en cada caso.	medio
B2.5	Control de calidad de las contraseñas	El responsable del Sistema correspondiente, a instancias del Equipo de Gobierno, deberá implementar mecanismos de control de calidad de las contraseñas que garanticen, al	corto

		menos, una longitud y complejidad mínimas y un tiempo de vida limitado.	
B2.6	Plan de concienciación en seguridad TI	El equipo de Gobierno, con el apoyo de los Responsables del Sistema y del Responsable de Seguridad, deberá aprobar y ejecutar un plan de concienciación en Seguridad TI para todo el personal de la organización; este plan incluirá la organización de pequeños talleres y jornadas a lo largo del año, centradas en actividades eminentemente prácticas, así como el envío periódico de píldoras informativas.	largo
B2.7	Plan de formación	Tal y como establece el RD 3/2010 de 8 de enero de 2010, el Equipo de Gobierno deberá aprobar un Plan de formación que explícitamente cubra los requisitos en materia de seguridad de la información deseables para el personal de la Unidad de TI; además deberá dotarlo con los recursos necesarios, ya sea incorporándolo al plan de formación del PAS de la UPRG o reservando una partida económica en el presupuesto anual.	largo
B2.8	Protección en los equipos de usuario	Los responsables del Sistema y el Responsable de Seguridad, con la aprobación del Equipo de Gobierno, deberán definir e implementar la homogenización de medidas de protección en los equipos de usuario y en los equipos portátiles, definiendo, según el tipo de equipo, puesto de trabajo e información tratada aspectos de la configuración de seguridad tales como: antivirus, política de actualización de escritorio, cortafuegos personal,	medio

		bloqueo, encriptación, etc.	
B3.1	Acceso remoto	Incluirlo en Normativa de seguridad y definir procedimiento de acceso.	corto
B3.2	Acondicionamiento del CPD	Mejorar el acondicionamiento del CPD: retirar el material que no debe estar allí como cajas y, fundamentalmente, informar al Área de Infraestructuras sobre el riesgo de las tuberías en el techo (inundación) para solucionar este riesgo.	medio
B3.3	Correo electrónico	Uso obligatorio de protocolos sobre SSL/TLS en el interior de la organización.	medio
B3.4	Pruebas de recuperación	Ejecución de una prueba de recuperación completa de un servicio al menos, una vez cada dos años.	largo
B3.5	Ataques de DoS	Para evitar ataques de DoS activar filtros en firewall de cabecera y también sobre la plataforma de monitorización.	corto
B3.6	Borrado y destrucción de soportes	Evaluar soluciones para el desarrollo de un procedimiento de borrado y destrucción de soportes utilizados en la Unidad de TI y ofrecer un servicio de destrucción de soportes al usuario del sistema de información.	medio
B3.7	Limpieza de metadatos	Establecer un servicio centralizado de limpieza de metadatos.	medio
B3.8	Estaciones de trabajo alternativas	Siempre que sea posible a nivel monetario se instalarán y configurarán puestos de trabajo alternativos dentro de las mismas instalaciones para que los empleados puedan seguir trabajando. El número de	largo

		estaciones alternativas se establecerá en función de la disponibilidad presupuestaria recomendando una instalación alternativa lista para funcionar por cada 6 empleados.	

Tabla 6-3. Tareas del Plan de Seguridad. Prioridad y duración

A continuación se muestra el responsable y los recursos requeridos en cada una de dichas tareas:

Código (Bloque.Prioridad)	Tarea	Responsable	Recursos
B1.1	Mejora de procedimiento de Gestión del Cambio	• Gestor del Cambio	• 1 empleado de la sección de TI con rol de Gestor del Cambio • 1 empleado de la sección de TI con rol de Gestor de la Configuración
B1.2	Gestión de incidentes de seguridad	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad
B1.3	Procedimientos de seguridad	• Responsable del Sistema de AE • Responsable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP
B1.4	Protección de aplicativos web	• Responsable del Sistema de AE • Responsable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI encargado de la gestión de la seguridad en red

B1.5	Arquitectura de seguridad	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad
B1.6	Gestión de claves privadas	• Responsable del Sistema de AE • Responsable del Sistema de ERP	• 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI encargado de la gestión de la infraestructura PKI
B2.1	Difundir política de seguridad	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad

B2.2	Normativas de seguridad	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad
B2.3	Política de calificación de la información	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado Responsable de la Información y Servicios de ERP • 1 empleado Responsable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad

B2.4	Política de firma y de sellado de tiempo	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado Responsable de la Información y Servicios de ERP • 1 empleado Responsable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad
B2.5	Control de calidad de las contraseñas	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad
B2.6	Plan de concienciación en seguridad TI	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad

B2.7	Plan de formación	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable de Seguridad
B2.8	Protección en los equipos de usuario	• Equipo de Gobierno	• 1 Componente del equipo de Gobierno (Vicerrector de nuevas tecnologías o similar) • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad • 4 empleados de la sección de TI encargados de dar soporte al usuario
B3.1	Acceso remoto	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad
B3.2	Acondicionamiento del CPD	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad
B3.3	Correo electrónico	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI a la órdenes del Responsable de Seguridad

B3.4	Pruebas de recuperación	• Responsable de Seguridad	• 1 empleado Responsable de la Información y Servicios de ERP • 1 empleado Responsable de la información y Servicios de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de AE • 1 empleado de la sección de TI con rol de Responsable del Sistema de ERP • 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI encargado de la Gestión de copias de seguridad y recuperaciones
B3.5	Ataques de DoS	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI encargado de la Gestión de la seguridad en red
B3.6	Destrucción de soportes	• Responsable de Seguridad	• 1 empleado de la sección de TI con rol de Responsable de Seguridad • 1 empleado de la sección de TI encargado del soporte al usuario

Tabla 6-4. Tareas del Plan de Seguridad. Responsables y recursos

Una vez cumplidas las tareas de cada bloque se deberá hacer una revisión para controlar que se han cumplido con todas las tareas incluidas en dicho bloque. Finalmente, para determinar el grado de ejecución de este plan y el impacto producido sobre el grado de cumplimiento del ENS, a la finalización del mismo (Septiembre de 2019) se realizará un nuevo control consistente en nueva auditoría de Seguridad TI en la organización.

Así, la aplicación de las medidas determinadas según este plan, nos llevarían a una reducción de los riesgos según la evolución que se refleja en los siguientes gráficos:

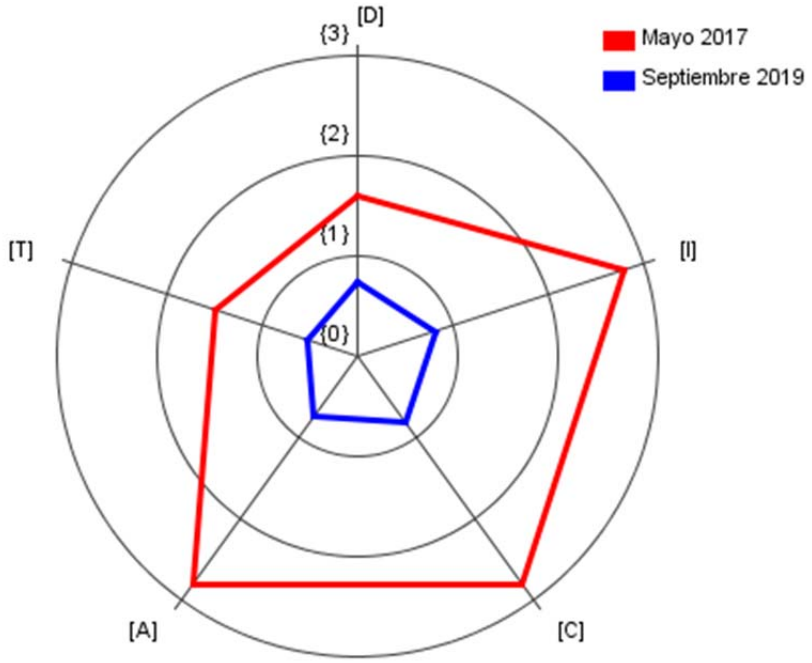

Ilustración 6-1. Mejora en Riesgo acumulado. Sistema ERP

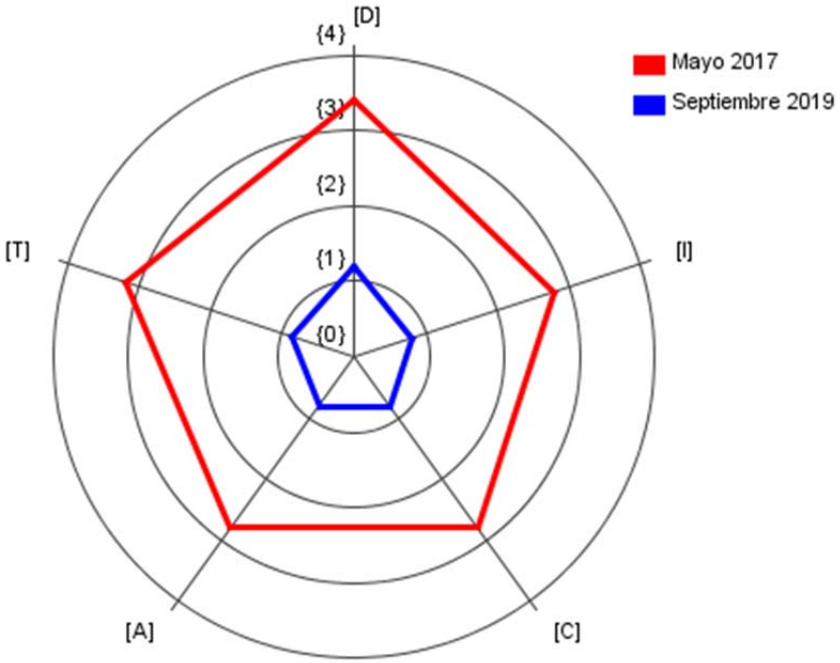

Ilustración 6-2. Mejora en Riesgo acumulado. Sistema AE

Por otro lado la aplicación de dicho plan permitirá avanzar en el grado de cumplimiento del ENS en la UPRG. No daremos la información detallada pero sí un resumen para las tres categorías de medidas para cada sistema:

Sistema	Familia de Medidas	Mayo 2017		Septiembre 2019	
		Nivel de madurez	Porcentaje de cumplimiento	Nivel de madurez	Porcentaje de cumplimiento
Sistema ERP	Medidas Organizativas	L0-L3	26%	L3	90%
	Medidas Operativas	L0-L3	37%	L2-L3	90%
	Medidas Técnicas	L0-L3	48%	L1-L3	88%
	Cumplimiento total	**L0-L3**	**37%**	**L1-L3**	**89%**

Tabla 6-5. Sistema ERP: Mejora Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

Sistema	Familia de Medidas	Mayo 2017		Septiembre 2019	
		Nivel de madurez	Porcentaje de cumplimiento	Nivel de madurez	Porcentaje de cumplimiento
Sistema AE	Medidas Organizativas	L0-L3	26%	L3	90%
	Medidas Operativas	L0-L3	37%	L1-L3	70%
	Medidas Técnicas	L0-L3	47%	L1-L3	87%
	Cumplimiento total	**L0-L3**	**37%**	**L1-L3**	**82%**

Tabla 6-6. Sistema AE: Mejora Nivel de madurez de grupos de medidas y grado de cumplimiento del ENS

También se presenta de forma un poco más detallada en el siguiente gráfico (debido a la similitud de ambas gráficas se muestra únicamente para el sistema ERP):

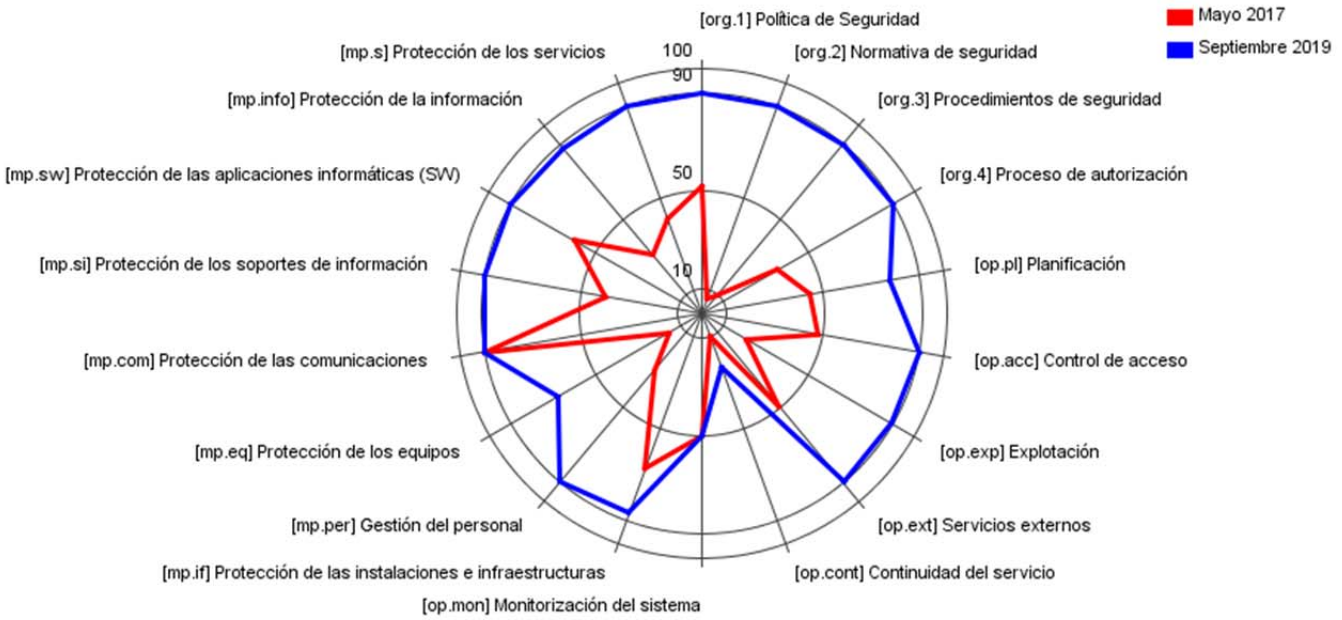

Ilustración 6-3. Mejora en grado de cumplimiento del ENS de las medidas para sistema ERP

6.3 Aprobación

Este plan será aprobado por el Comité de Seguridad TIC, dentro de la Comisión de Nuevas Tecnologías.

7 Conclusiones

El presente TFM ha permitido poner en práctica los conocimientos adquiridos a lo largo del máster relacionado con el análisis de riesgos y la gestión de la seguridad en los sistemas de información. Dichos conocimientos han sido aplicados a un caso de un Universidad Pública para la adaptación de sus sistemas de información a los requisitos demandados por el Esquema Nacional de Seguridad.

Se ha aprendido a manejar la herramienta PILAR para el análisis de riesgos y se han afrontado problemas reales que aparecen en análisis de riesgos como la necesidad de modelar los activos o de recopilar información sobre las amenazas y las salvaguardas existentes. Para la valoración de dichas salvaguardas se ha llevado a cabo una auditoría interna para la que ha sido necesario recoger evidencias que sustenten los niveles de madurez asignados a las salvaguardas.

Se ha visto que actualmente existe una gran falta de concienciación en materia de seguridad que lleva a que muchos organismos tanto públicos como privados opten por implantar medidas de seguridad puntuales y no a nivel global siendo estas medidas puntuales propuestas por el personal de TI y no por el propio órgano de gobierno de la institución.

Como líneas futuras se propone:

- Realizar una revisión de la implantación de las recomendaciones de seguridad fijadas en el plan de mejora de la seguridad.

- Usar el perfil de PILAR de la ISO 27000 y la ISO 27001 y valorar dichas salvaguardas comparando su cumplimiento con el cumplimiento del ENS.

8 Bibliografía

- “Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.”
    - https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
    - https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566
- “Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas”
    - https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565
- Guías de Seguridad publicadas por el CCN-CERT dentro de la serie CCN-STIC:
    - Guía “CCN-STIC 825. Esquema Nacional de Seguridad Certificaciones 27001”. Versión de Noviembre de 2013.
    - Guía “CCN-STIC 802. Esquema Nacional de Seguridad: Guía de auditoría”. Versión de Junio de 2010
    - Guía “CCN-STIC 803. Esquema Nacional de Seguridad Valoración de los sistemas”. Versión de Enero de 2011.
    - Guía “CCN-STIC 470/G1. Manual de usuario de PILAR 5.4 para el análisis y gestión de riesgos”. Versión de Agosto de 2014
- “Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.”
    - https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330
- MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método
- MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos