Guía general de adecuación al Esquema Nacional de Seguridad en una Universidad.

Plan de estudios del Estudiante: Master Universitario en Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)

Estudiante: Francisco Jose Muñoz Torrijos

Nombre del consultor: Ana Maria Chulia Cebolla

Fecha entrega: 11 de Junio de 2018

AGRADECIMIENTOS

Quiero dedicar este trabajo a mi familia, especialmente a mis padres, a Maria y a Nacho por la merma en el tiempo familiar.

Quiero agradecer también a Ana Chulia, la ayuda, la paciencia y el tratamiento durante la práctica debido a los retrasos en las entregas y a Jose Antonio Mañas por su predisposición para solucionar los problemas sobre la herramienta de gestión de riesgos PILAR.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Guía de adecuación al Esquema Nacional de Seguridad.
Nombre del autor:	Francisco Jose Muñoz Torrijos
Nombre del consultor:	Ana Maria Chulia Cebolla
Fecha de entrega (mm/aaaa):	06/2018
Área del Trabajo Final:	TFM – Aspectos legales de la Seguridad informática
Titulación:	*Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*

Resumen del Trabajo (máximo 250 palabras):

Vivimos en la sociedad de la información, un mundo cada vez más dependiente de los sistemas de información que ofrecen día a día nuevas capacidades al usuario con los riesgos asociados.

Uno de los activos más valiosos es la información perteneciente a estos usuarios, que puede ser utilizada con muy diversos fines.

La Administración Pública cuenta con la información más sensible de los ciudadanos, y corresponde a esta proteger y garantizar que se utiliza únicamente para los fines para los cuales fue recogida, evitando y persiguiendo cualquier otro uso.

Este objetivo será cubierto en la Administración Púbica española con la implantación del Esquema Nacional de Seguridad (ENS), de obligado cumplimiento.

Ante la dificultad que está suponiendo en las distintas AAPP su implantación debida a falta de recursos y experiencia, este Trabajo fin de Master tratará de realizar una guía de implantación y adecuación al Esquema Nacional de Seguridad de propósito general y de carácter práctico basándose en un caso de estudio aplicado a una universidad.

Esta guía estará basada principalmente en Esquema Nacional de Seguridad, Real Decreto 3/2010 de 8 de Enero y su modificación según el Real Decreto 951/2015 de 23 de Octubre, teniendo en cuenta el Real Decreto 1720/2007 de 21 de Diciembre, respecto al reglamento LOPD, la Ley Orgánica 15/1999 de 13 de diciembre respecto a la LOPD, la Ley 11/2007 de 22 de Junio en su artículo 42, las guías STIC serie 800 y el software desarrollado por el Centro Criptológico Nacional.

Abstract (in English, 250 words or less):

We live in the information society, a world that is increasingly dependent on information systems that offer new capabilities to the user day by day with the associated risks.

One of the most valuable assets today is the information belonging to these users, which can be used for many different purposes.

The Public Administration has the most sensitive information of the citizens, and it corresponds to this protect and guarantee that it is used only for the purposes for which it was collected, avoiding and pursuing any other use.

This objective will be covered by the Spanish Public Administration with the implementation of the National Security Scheme (ENS), which is mandatory.

Given the difficulty that is being assumed in the various Public Administrations due to lack of resources and experience, this Final Master's Project will try to make a guide to implementation and adaptation to the National Security Scheme of general purpose and practical nature based on a case practical applied to a university.

This guide will be based mainly on National Security Scheme, Royal Decree 3/2010 of January 8 and its modification according to Royal Decree 951/2015 of October 23, taking into account Royal Decree 1720/2007 of December 21, regarding to the LOPD regulation, the Organic Law 15/1999 of December 13 with respect to the LOPD, Law 11/2007 of June 22 in its article 42 and the STIC 800 series guides and the software developed by the National Cryptological Center.

Palabras clave (entre 4 y 8):
Esquema Nacional de Seguridad, Real decreto 3/2010 de 8 de enero, Real Decreto 951/2015 de 23 de Octubre, Ley 11/2007 de 22 de Junio, PILAR, Centro Criptológico Nacional, CCN-CERT, Universidad, ENS.

Índice

Lista de figuras

1. Introducción

1.1. Contexto y justificación del Trabajo

El esquema nacional de seguridad tiene como objeto establecer de las condiciones necesarias de confianza en el uso de los medios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios entre los ciudadanos y las Administraciones públicas.

Es de obligado cumplimiento para todas las organizaciones que forman parte de la Administración Publica y lo constituyen una serie de principios básicos y requisitos mínimos con el fin de proteger adecuadamente la información, para ello, se tendrán en cuenta las recomendaciones de la Unión Europea y la situación tecnológica de las diferentes Administraciones públicas.

Este esquema se regula según el Real Decreto 3/2010 de 8 de Enero, modificado según el Real Decreto 951/2015 de 23 de Octubre y fue establecido en el artículo 42 de la Ley 11/2007 del 22 de Junio (LAECSP), y de lo recogido en el texto de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), de acceso electrónico de los ciudadanos a los Servicios Públicos.

El esquema Nacional de Seguridad es una norma legal de obligado cumplimiento para el sector público salvo por los sistemas que tratan información clasificada regulada en la Ley 9/1968, de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

Su ámbito de aplicación pasa por la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, las entidades de derecho público vinculadas o dependientes de las mismas, las relaciones entre ellas y finalmente a los ciudadanos y su relación con la Administración Pública.

Su conformidad se alcanza satisfaciendo los mandatos contenidos en su texto articulado y mediante la adecuada implantación de las medidas de seguridad contempladas en el Anexo II de la norma, previa categorización de los sistemas a proteger según el Anexo I.

Aunque el plazo de aplicación inicial del ENS es de 12 meses, ampliable a 48 meses bajo circunstancias justificadas, son muchas las Administraciones Públicas que a día de hoy o bien no cumplen adecuadamente con el ENS o bien están todavía en proceso de adecuación de alguno de sus procesos.

La necesidad a cubrir del TFM está basada en la dificultad encontrada en las Administraciones Públicas en su adaptación al ENS por lo heterogéneo de los entornos debido al crecimiento de cada una de las Administraciones Públicas en base a sus propias necesidades y posibilidades, los recursos disponibles y los servicios ofrecidos al usuario, así como las herramientas de gestión internas.

También ha dificultado su adaptación el hecho de que históricamente la seguridad no ha sido percibida en general como un valor añadido al negocio, esto ha provocado que la seguridad haya sido relegada continuamente a un segundo lugar, y no se ha tenido en cuenta hasta la obligatoriedad de la norma o hasta encontrarse directamente con un incidente de seguridad, trabajando de forma totalmente reactiva en lugar de trabajar proactivamente para minimizar los riesgos y el impacto de los posibles incidentes de seguridad como indica el ENS.

Tampoco ha ayudado el hecho de que resulta complicado aunar toda la información disponible para estandarizar una metodología general de aplicación.

Por todo ello, el presente documento tratará de ofrecer una solución mediante la realización de la presente memoria, analizando el problema en todas sus facetas con un caso de estudio, para obtener finalmente un producto o resultado en forma de guía de actuación al ENS, estableciendo de forma sencilla cada uno de los pasos.

1.2. Objetivos del Trabajo

Como se ha indicado el presente trabajo realiza el análisis de los elementos relacionados con la adecuación al ENS (Real Decreto 3/2010 de 8 de Enero y su modificación según el Real Decreto 951/2015 de 23 de Octubre) en un caso de estudio de una universidad pública española.

El objetivo del trabajo tras el análisis de la problemática de una universidad es la creación de una guía de adecuación al Esquema Nacional de Seguridad de fácil aplicación, tratando de consolidar en un documento los aspectos principales de las normativas, los procedimientos, las guías del Centro Criptológico Nacional y el software relacionado para el tratamiento de la información que permita el cumplimiento de la norma.

Para satisfacer este propósito principal, se han definido unos objetivos específicos:

- Definir un marco normativo
- Definir un caso de estudio. Universidad Exempli Gratia
- Análisis de requisitos para el cumplimiento de ENS.

- Revisión de las guías de apoyo CCN-STIC serie 800

- Análisis de la adaptación al ENS en el caso de estudio de la universidad Exempli Gratia

- Creación de la propia guía de adecuación al ENS como producto.

1.3. Enfoque y método seguido

El documento trata de dar solución a las dificultades que pueden encontrar en las distintas AAPP para adecuarse a la normativa relacionada con el ENS. Para conseguir la conformidad y adecuación al ENS se utilizarán principalmente las guías CCN-STIC elaboradas por el Centro Criptológico Nacional, entre otras la 804 como guía de implantación, la 809 como guía de conformidad, 802 como guía de auditoria, 808 como guía de verificación de cumplimiento, etc.

El enfoque utilizado para la adecuación al ENS, será de forma general como un proyecto de puesta en marcha en una organización, tratando de cohesionar los elementos entre si y de la manera más secuencial posible para facilitar el trabajo posterior en las organizaciones con el seguimiento del producto resultante de esta memoria.

Para conseguir el objetivo, se parte de un caso de estudio que será la adecuación al ENS de determinados servicios clave y representativos en una Universidad Pública, de la que una vez encontrados y solucionados los retos, se obtendrá un documento que aúne todos los pasos requeridos a modo de guía para cumplir con éxito los requerimientos para la adecuación al ENS de forma general.

1.4. Planificación del Trabajo

La memoria deberá de planificarse y dimensionarse correctamente para poder llevarla a cabo con éxito, se presenta la siguiente propuesta de planificación del trabajo. Se ha tratado de unificar en lo posible las entregas de las PEC y los propios hitos del proyecto:

Fase I. Recogida de información	
Días de la tarea:	11
Objetivo:	Reunir la información relativa al desarrollo del TFM. En el proyecto actual información sobre El Esquema Nacional de Seguridad. Elaboración de un primer índice provisional y calendario de trabajo.

Fase II. Introducción al Proyecto	
Días de la tarea:	11
Objetivo:	Revisión de capítulos a tratar. Enfoque y selección de la organización objeto de estudio. Delimitar el alcance del Esquema Nacional de seguridad. Revisión de contexto, justificación, objetivos, enfoque, método y planificación.

Fase III. Situación inicial	
Días de la tarea:	11
Objetivo:	Revisión de Anexos ENS y Guías STIC para realizar análisis y categorización de la información y los servicios del caso de estudio, establecimiento de valoraciones. Revisión implicaciones de los Datos de carácter personal y categorización del sistema.

Fase IV. Política de seguridad de la organización	
Días de la tarea:	8
Objetivo:	Revisión procedimientos y guías STIC. Definición de roles y responsabilidades. Creación de la política de seguridad del caso de estudio.

Fase V. Análisis de riesgos	
Días de la tarea:	5
Objetivo:	Análisis de la metodología Magerit v3. Descarga e instalación de software de gestión de riesgos PILAR, gestión de licencia trial, estudio funcionamiento. Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, niveles aceptables y riesgo residual.

Fase VI. Documentos adicionales	
Días de la tarea:	5
Objetivo:	Creación de la declaración de aplicabilidad del Anexo II del ENS, revisión de las insuficiencias del sistema (gap analysis), creación del plan de mejora de la seguridad y documento de conformidad.

Fase VII. Auditoría de seguridad	
Días de la tarea:	5
Objetivo:	Revisión de guías STIC y creación de auditoria de seguridad sobre el caso de estudio.

Fase VIII. Revisión memoria	
Días de la tarea:	5
Objetivo:	Revisión del formato del documento, elección de guía de estilo, tipo de letra. Creación de la bibliografía, glosario, anexos, listado de figuras, revisión del documento final.

Fase IX. Elaboración Producto	
Días de la tarea:	8
Objetivo:	Creación de la guía de adecuación al ENS con los conocimientos adquiridos durante la elaboración de la presente Memoria.

Fase X. Creación de presentación y grabación video	
Días de la tarea:	8
Objetivo:	Elaboración de una presentación sobre la memoria y/o producto obtenido.

Se muestra la cronología de las tareas en un diagrama de Gant:

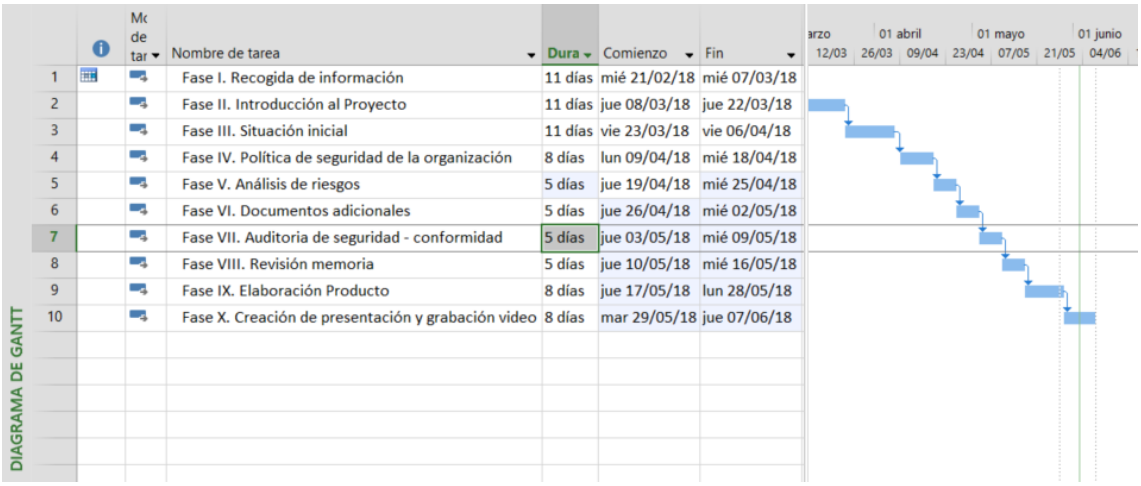


Ilustración 1: Diagrama de Gantt de tareas a realizar

1.5. Breve sumario de productos obtenidos

La presente memoria y el análisis del caso de estudio permitirán pasar por todos los hitos necesarios para adaptarse al marco normativo del ENS. Para ello se tendrá en cuenta la situación inicial y deseada de una Administración Publica, así como las necesidades derivadas definiendo los distintos responsables de los procesos, la información manejada, los servicios ofrecidos, el análisis de riesgos, las auditorias que verifiquen el cumplimiento, etc. Utilizando para ello todo el soporte y material ofrecido por instituciones como Centro Criptológico Nacional.

La realización de la presente memoria dará como resultado la guía genérica de adaptación al ENS indicada, permitiendo a cualquier Administración Pública adecuarse a los requisitos de seguridad de la información del Esquema Nacional de Seguridad de manera rápida, sencilla y estructurada, al margen de la mayor o menor complejidad de los procesos que tengan que ser implementados en cada una de sus fases.

Como producto secundario adicional se habrá obtenido el caso de estudio de una Universidad pública española, que tendrá aplicación real.

1.6. Breve descripción de los otros capítulos de la memoria

La presente memoria revisará los aspectos más relevantes del Real Decreto 3/2010 de 8 de Enero y de la modificación según el Real Decreto 951/2015 de 23 de Octubre por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Para la ubicación del lector en la temática, el documento realizará una introducción sobre los principios básicos del ENS. Los artículos que lo componen serán descritos en cada uno de los apartados que son objeto de su

aplicación y respecto a los dos anexos con los que cuenta el ENS serán trabajados en profundidad durante el desarrollo de la memoria, ya que son la base y piedra angular de la implantación del ENS.

El primero de los trabajos a realizar para la adecuación al ENS de cualquier organización, será la de establecer la política de seguridad, en el documento deben de figurar aspectos como su aprobación y entrada en vigor, el alcance, los servicios objeto de análisis, el marco normativo, la organización, los roles y responsabilidades que se han de asumir, etc.

Una vez tenemos el personal asignado para la aplicación del ENS y el objeto de análisis o servicios implicados, se indicarán los criterios de evaluación para dimensionar los activos de la organización según las dimensiones descritas en el Anexo I del ENS. Los activos valorados serán información y servicios de la organización.

Para realizar los análisis necesarios se describirá el caso de estudio de la universidad ficticia llamada Exempli Gratia, pudiendo ser representativa de cualquier universidad pública española, donde se realizará el trabajo de adecuación al ENS.

Descrito el caso de estudio se procederá a la categorización de la información y servicios que la Universidad Exempli Gratia ofrece.

En este punto se realizará una parada para poner de manifiesto los datos de carácter personal en las organizaciones y la relación con el ENS, ya que su análisis puede en determinados casos, realizarse conjuntamente. En la presente memoria se trabajara únicamente sobre el ENS, dejando de lado lo relacionado con los datos de carácter personal.

Obtenida la categorización del sistema se deberá de analizar los aspectos de seguridad correspondientes a la categorización del sistema de información mediante los grados de madurez.

Tras categorizar el sistema según el Anexo II del ENS, se procede a indicar la obligación de realizar un análisis de riesgos, apartado donde se justifica su realización mediante el articulo asociado, la metodología Magerit v3 utilizada con carácter general para su realización y la herramienta PILAR para realizar el análisis de riesgos.

El trabajo con la herramienta PILAR parametrizada con los datos del caso de estudio será mostrado con las ilustraciones del proceso y se mostrará como resultado un análisis de riesgos que se muestra en el Anexo III.

Realizado el análisis de riesgos se tendrán identificados cuales de esos riesgos afectan a la información y a los servicios de la organización y como se pueden extrapolar a las medidas de seguridad del Anexo II. La información obtenida deberá de ser indicada en el documento “Declaración de aplicabilidad” donde se mostraran si son de aplicación o no las medidas de seguridad.

El paso siguiente será la elaboración del documento “Informe de insuficiencias” o “gap analysis”, donde se declararan las insuficiencias del documento anterior y las situación del cumplimiento de las medidas de seguridad estableciendo la comparativa entre la situación ideal frente a la situación real.

Una vez completado el informe de insuficiencias, se establecerá el plan de mejora de la seguridad, donde se indicara tanto los plazos, como los recursos y las tareas necesarias para solucionar los riesgos puestos de manifiesto en el análisis de riesgos que permitan acortar la brecha existente definida anteriormente entre la situación ideal frente a la real.

Finalizados los trabajos será redactado el documento de conformidad con el ENS, que indicará que la organización ha puesto en marcha las medidas apropiadas para la correcta protección de la información y los servicios según los criterios del Esquema Nacional de Seguridad.

El paso siguiente será comunicar los resultados de los trabajos realizados de adecuación al Centro Criptólogico Nacional mediante la herramienta INES puesta a disposición de las AA.PP. por el CCN-CERT.

Solo quedará mantener, mejorar y adaptarse a los nuevos servicios puestos en marcha por la organización. Para su control se establecerán Auditorias periódicas que permitan mantener la calidad y adaptación de los procesos en el tiempo así como los servicios ofrecidos por la organización.

2. Esquema Nacional de Seguridad.

Con el objetivo de acercar la administración pública al ciudadano, el 22 de Junio de 2007 se aprueba la Ley 11/2007, de acceso Electrónico de los ciudadanos a los Servicios Públicos, reconociendo el derecho de los ciudadanos a relacionarse con las Administraciones Publicas por medios electrónicos y regulando los aspectos básicos de la utilización de la información en la actividad administrativa, en las relaciones entre Administraciones Públicas y en las relaciones de las mismas con los ciudadanos con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica. Todo ello asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Como indica en su artículo 42.2 la Ley 11/2007, para establecer la política de seguridad que regule la utilización de medios electrónicos se establece el Esquema Nacional de Seguridad, constituido por una serie de principios básicos y requisitos mínimos que permitan la adecuada protección de la información.

Con lo expuesto, su materialización en el 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 y la posterior modificación según el Real Decreto 951/2015 de 23 de Octubre, indican 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 permitan a los ciudadanos y a las Administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La articulación de la Ley 11/2007 de 22 de Junio y por extensión el Real Decreto 3/2010 de 8 de Enero, se realiza atendiendo a la normativa nacional sobre:

- administración electrónica,
- protección de datos de carácter personal,
- firma electrónica y documento nacional de identidad electrónico,
- Centro Criptológico Nacional,
- Sociedad de la información,
- Reutilización de la información en el sector público y órganos colegiados
- Responsables de la Administración Electrónica
- Regulación de diferentes instrumentos y servicios de la Administración, las directrices y guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, es el referente legal imprescindible de cualquier regulación administrativa, donde se determina la configuración de numerosos ámbitos de confidencialidad administrativos, diferentes a la información clasificada y a los datos de carácter personal, que necesitan ser materialmente protegidos. También determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones realizadas por vía electrónica.

Y a la normativa internacional como:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, también llamada RGPD que obliga a que cuando se traten datos de carácter personal se realice un análisis de riesgos para los derechos y libertades de los ciudadanos y hace depender la aplicación de todas las medidas de cumplimiento que prevé (entre ellas las de seguridad) del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados.

2.1. ENS – Principios básicos

Los principios básicos del ENS establecen los puntos de referencia para la toma de decisiones y son los fundamentos que deben regir toda acción orientada a asegurar la información y los servicios

Se establecen los siguientes principios básicos descritos en el ENS:

2.1.1. Principios básicos

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.

b) Gestión de riesgos.

c) Prevención, reacción y recuperación.

d) Líneas de defensa.

e) Reevaluación periódica.

f) Función diferenciada.

2.1.2. Seguridad como un proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

2.1.3. Gestión de seguridad basada en los riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

2.1.4. Prevención, reacción y recuperación.

La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

2.1.5. Líneas de defensa.

El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

c) Minimizar el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

2.1.6. Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de

protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

2.1.7. Función diferenciada.

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

3. Real Decreto 951/2015 de 23 de octubre. Cambios en la regulación del ENS en el ámbito de la administración electrónica.

Dada la rápida evolución de las tecnologías de aplicación y la experiencia derivada de la implantación del Esquema Nacional de Seguridad, en 2015 la norma es actualizada en alcance y contenido, orientándose a precisar, profundizar y contribuir al mejor cumplimiento de los mandatos normativos.

Se establece mediante disposición transitoria un plazo de veinticuatro meses contados a partir de la entrada en vigor para la adecuación de los sistemas a lo dispuesto en la modificación.

Las principales medidas adicionales introducidas son:

- En el artículo 11, la gestión continuada de la seguridad como un aspecto clave que ha de acompañar a los servicios disponibles por medios electrónicos 24 horas al día.

- En el artículo 15, la exigencia, de manera objetiva y no discriminatoria, de profesionales cualificados a las organizaciones que presten servicios de seguridad a las Administraciones Públicas.

- En el artículo 18, la utilización, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, de aquellos productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

- En el artículo 24, el despliegue de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.

- En el artículo 27, la formalización de las medidas de seguridad en un documento denominado 'declaración de aplicabilidad' y la posibilidad de reemplazar medidas de seguridad por otras compensatorias cuando se justifique documentalmente.

- En el artículo 29, la figura de las "Instrucciones técnicas de seguridad" que regularán aspectos tales como el informe del estado de la seguridad, la auditoría de la seguridad, la conformidad con el Esquema, la notificación de incidentes de seguridad, la adquisición de productos de seguridad, la criptología empleada en el ámbito del Esquema y los requisitos de seguridad en entornos externalizados, entre otras.

- En el artículo 35, referencias expresas a la articulación de los procedimientos necesarios para la recogida y consolidación de la información para el informe anual de estado de la seguridad y organismos responsables de su realización.

- En el artículo 36, la notificación al Centro Criptológico Nacional de aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados.

- En el artículo 37, las evidencias necesarias para la investigación de incidentes de seguridad por parte del Centro Criptológico Nacional.

- La mejora de diversas medidas de seguridad para mejorar su eficacia y para adecuarse a lo previsto 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 y por el que se deroga la Directiva 1999/93/CE. En particular, los apartados 3.4, 4.1.2, 4.1.5, 4.2.1, 4.2.5, 4.3.3, 4.3.7, 4.3.8, 4.3.9, 4.3.11, 4.4.2, 4.6.1, 4.6.2, 5.2.3, 5.3.3, 5.4.2, 5.4.3, 5.5.2, 5.5.5, 5.6.1, 5.7.4, 5.7.5, 5.7.7 y 5.8.2.

4. ¿Por dónde empezar? – Plan de adecuación

Para que todo lo indicado con anterioridad empiece a tomar forma. El presente punto trata de arrojar luz indicando los aspectos que se trataran para cumplir con el Esquema Nacional de Seguridad.

Como trabajo inicial se deberá de cumplir con los pasos del Anexo I del ENS, en el que deberemos de identificar y valorar nuestros activos esenciales y categorizar nuestro sistema o sistemas, para ello se propone el caso de estudio que describimos en el siguiente apartado.

Una vez identificado nuestro sistema, se procede a determinar las medidas del anexo II del ENS que resulten de aplicación, realizando una primera evaluación de su madurez.

Es en este momento cuando empieza realmente el trabajo de adaptación al ENS y donde se hace imprescindible hablar de la figura del Centro Criptologico Nacional, ya que tiene una relevancia especial en el Esquema Nacional de Seguridad como se indica a continuación.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Se partirá del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, y de diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Sera imprescindible disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Para ello el Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte del CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en

ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

La serie de guías CCN-STIC-800 trabajan directamente sobre el Esquema Nacional de Seguridad, y son la ayuda base creada por el Centro Nacional Criptológico para la adecuación al ENS.

Dado lo numeroso y extenso de algunas de estas, el presente documento extrae la información más relevante de cada una de ellas con el fin de elaborar un procedimiento genérico de adecuación que contenga una serie de pasos o secuencia lógica para el tratamiento de la información como se ha indicado anteriormente.

El plan de adecuación estará basado principalmente en dos de las guías del CCN:

- CCN-STIC 806 de adecuación al ENS

- CCN-STIC 815 sobre las métricas e indicadores del ENS

El primero de los documentos indica la información necesaria en el plan de adecuación, información que deberá de ser aprobada por los órganos superiores competentes:

1. La política de seguridad

2. Información que se maneja, con su valoración

3. Servicios que se prestan, con su valoración

4. Datos de carácter personal

5. Categoría del sistema

6. Análisis de riesgos

7. Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera

8. Insuficiencias del sistema *(gap analysis)*

9. Plan de mejora seguridad, incluyendo plazos estimados de ejecución

El segundo de los documentos es la guía CCN-STIC 815, donde se trata sobre las métricas en indicadores. Como todas las guías de métricas e indicadores, estas son prolijas y esta no es una excepción, esto que permite abarcar multitud de situaciones con un entendimiento común para comparar los distintos sistemas.

Dada la dificultad del análisis de los sistemas y que tratar de alcanzar la perfección futura puede impedir el comienzo, se debe de ver el proceso con una perspectiva evolutiva, desde un sistema de métricas rudimentario a un sistema maduro. Será el proceso de mejora continua el que permita conseguir la excelencia y adaptarse dinámicamente a los cambios que se produzcan en los sistemas en las organizaciones.

Se tendrá en cuenta que cuando los sistemas de nuestra organización manejan información de terceros o presten sus servicios a terceros, la valoración de la información será la determinada por este, y si son incrementadas, se hará necesaria la realización de un “plan de adecuación incremental”, que contemple las deficiencias derivadas del nuevo escenario.

El mismo tratamiento será realizado en el caso contrario, la valoración de los sistemas propios será impuesta al tercero en su propio plan de adecuación.

5. Descripción del caso de Estudio

Una vez indicadas las metas que debemos de cumplir, con el objetivo de analizar cada uno de los puntos a tratar para cumplir con el Esquema Nacional de Seguridad y obtener una guía de aplicación, se propone utilizar como caso de estudio la adecuación de una Universidad Pública y los servicios más representativos ofrecidos.

La descripción de la infraestructura, aunque a priori puede parecer que tenga aspectos poco significativos o irrelevantes, permitirá categorizar algunos aspectos del trabajo desarrollado más rápidamente evitando entrar en ciertos aspectos, para focalizar el análisis en otras áreas de más interés.

La Universidad “Exempli Gratia” cuenta con dos campus separados varios kilómetros entre ellos, el gran peso educativo y administrativo recae en el primero de ellos, incluyendo rectorado, ubicándose en el segundo algunos estudios y facultades con sus secretarias.

Respecto a los sistemas informáticos y los servicios ofrecidos por estos, la Universidad cuenta con un alto grado de madurez en sus recursos tecnológicos, con dos CPD´s Activo-Activo donde residen los principales recursos informáticos centrales de la Universidad, ubicándose en una DMZ o zona desmilitarizada parte de los servicios ofrecidos al público en general y de uso externo tanto al estudiante como al PDI o PAS (p.ej. Servicios Web públicos o Aula Virtual).

Internamente se establecen Vlans privativas donde únicamente se tiene acceso interno que previamente se ha dado de alta para acceder a determinados recursos como las Aulas informáticas, bibliotecas, etc.

Existen otras áreas donde además el acceso requiere de un alta previa y la gestión adecuada del routing en las comunicaciones como la red de gestión.

También se controla el acceso con sistemas de Detección de Intrusiones y existen adicionalmente áreas especialmente protegidas donde se ubican los servicios de nóminas, gabinetes médicos, expedientes académicos, etc.

El servicio de informática ha realizado un esfuerzo notable los últimos años y toda la información reside en servidores que se encuentran virtualizados, algunos trabajando en clúster, sistemas de Fault Tolerance o High Availavility, lo que permite en muchos de los casos y sistemas críticos la resiliencia ante un fallo hardware, perdida de corriente o inundaciones, con técnicas de balanceo de carga entre los dos CPD´s sin pérdida de servicio.

Todos los servidores cuentan con sistemas de Backup y con amplios periodos de retención de las copias de seguridad, tanto del continente (máquinas virtuales) como del contenido (información del sistema operativo, aplicaciones y datos), y están protegidos siempre que el sistema operativo lo permite con antivirus que se actualizan regularmente.

Todos los sistemas son actualizados según fabricantes tanto hardware como software y cuentan con fuertes políticas de seguridad, tanto de la seguridad física a las instalaciones con tarjetas de proximidad como del control de la información por parte de los responsables.

Este esfuerzo realizado por el personal del servicio de informática se debe de ver complementado ahora con la adecuación al ENS, donde se amplía la cubertura de la seguridad de la información desde otras perspectivas de carácter más normativo y normalizadas entre los distintos entornos.

La Universidad ofrece muchos y muy variados servicios con distintos niveles de seguridad requeridos en cada uno de ellos, para la adecuación al ENS nos basaremos en los más significativos y relevantes que ofrece una universidad dado lo extenso de los análisis a realizar.

Los servicios que ofrece la Universidad “Exempli Gratia” clasificados por grupos según su propio desarrollo histórico funcional y crecimiento de infraestructuras que serán objeto de análisis son los siguientes:

Área Docente

- Soporte a las aulas informáticas de libre acceso y de docencia.

  El servicio requiere de la Instalación y configuración de equipos así como el software utilizado en aulas de uso docente y ubicaciones de acceso libre.

- Soporte a las aulas multimedia.

  Este servicio incluye la instalación y configuración de equipos y Software además de contar con equipamiento audiovisual como pizarras y proyectores.

- Gestión de licenciamiento.

  El servicio gestiona la Adquisición y validación centralizada de licencias de software de uso docente

- Aula Virtual

  Este servicio cubre las necesidades de la docencia en accesos Web, áreas de compartición de ficheros, contenidos multimedia y acceso a la mensajería entre docentes y alumnado en las Aulas incluyendo la realización de pruebas y exámenes.

Área de investigación

- Supercomputación

  Gestión de los recursos de altas prestaciones para el cálculo y procesamiento de datos científicos.

- Consultoría

  Servicios de consultoría con soporte al despliegue de aplicaciones y servicios especializados de alto rendimiento, conectividad de infraestructuras, licenciamiento de los productos y gestión del soporte técnico especializado orientado a la investigación.

Área de Gestión

- Gestión Académica

  Gestiona la actividad académica de los estudiantes universitarios, incluye Grados, Postgrados, Actas, Automatrículas, Becas, y todo lo referente a titulaciones (horarios, secretarias, prácticas, etc.) tanto oficiales homologados por ANECA como propias.

- Gestión económica y tesorería

  Aplicaciones para la gestión económica de la Universidad, incluyendo donaciones de cualquier organización, la gestión de fondos de financiación europea, gestión de las tasas universitarias y cualquier otro ingreso.

- Contratación y presupuestos

  Se encarga de la gestión de los contratos que establece la Universidad con terceros y la gestión de los presupuestos.

- Tesorería

  Se encarga de la gestión de la tesorería económica de la Universidad.

- Gestión de RR.HH.

  Realiza la gestión de los procedimientos relacionados con los Recursos Humanos en la Universidad, relación de puestos de trabajo, plantilla, control horario, convocatorias de acceso, procesos de formación, revisiones médicas, retribuciones al personal, etc.

- Extensión Universitaria

  Gestión de todas las actividades y procesos gestionados por el Servicio de Deportes, alquiler de viviendas, enseñanzas no regladas, etc.

- Archivo

  Gestión y mantenimiento del Archivo universitario en los diferentes soportes como documentos, fichas, DVD, negativos y positivos fotográficos, cuadernos, películas o impresos.

- Secretaria General.

  Gestión de todos los procesos pertenecientes a la institución, actos protocolarios, registro universitario (presencial y telemático), gestión documental, convenios, normativa universitaria y procesos electorales.

- Gestión de infraestructuras

  Aplicaciones de gestión de infraestructuras, control de acceso a edificios, aparcamientos, zonas deportivas, gestión de almacenes, pedidos y materiales, gestión de los riesgos laborales asociados a las instalaciones universitarias y gestión de espacios.

- Servicio de bibliotecas

  Gestión de los procesos soportados por bibliotecas y repositorio institucional.

- Comunicación

  Gestión de la televisión universitaria, prensa universitaria, cartelería digital, eventos y congresos.

- Calidad

  Gestión de los recursos y aplicaciones para la gestión de la calidad, generación, difusión y evaluación de las encuestas destinadas a la comunidad educativa, evaluación del profesorado, evaluaciones y autoevaluaciones de la calidad.

- Análisis de datos

Aplicaciones de análisis de datos e información institucional (Datawarehouse).

- Atención al usuario (CAU)

  Aplicaciones para la gestión de peticiones e incidencias.

- Gestión de publicaciones

  Gestión de los procesos de publicaciones de la Universidad.

Área de correo, herramientas colaborativas y publicación Web.

- Gestión del correo electrónico

  Gestión de correo electrónico institucional PDI/PAS, alumnado, pre alumnado y egresado, listas de distribución, notificaciones SMS, redes sociales, espacios colaborativos, servicios FTP y servicios de videoconferencia.

- Web institucional.

  Sitio web de información académica, investigación y servicios universitarios

- Sede electrónica

  Acceso electrónico de los ciudadanos a los Servicios Públicos según lo establecido en la Ley 11/2007 de 22 de Junio.

- Intranet.

  Publicación de información académica de investigación y servicios universitarios de acceso restringido a la comunidad universitaria incluyendo el colectivo investigador.

- Portal del empleado

  Recursos y servicios dirigidos a los empleados de acceso restringido a este colectivo.

- Secretaria Virtual

  Recursos y servicios dirigidos a los estudiantes de la universidad sobre un sitio web de acceso restringido al colectivo.

- Contenidos digitales

Soporte a la generación, almacenamiento y difusión de material audiovisual y soporte a la elaboración, creación y difusión de contenidos para uso docente.

Soporte y equipamiento del puesto de Trabajo

- Servicio integral Workplace

  Soporte y equipamiento del puesto de Trabajo (renovación del parque informatico adecuado al puesto), mantenimiento software corporativo, servicios de impresión y asesoramiento técnico. Tareas de alto nivel no asignadas bajo incidencia o petición al servicio del CAU.

Servicio de Comunicaciones

- Servicio de telefonía fija, móvil y fax

  Diseño, administración y gestión de las comunicaciones de voz basadas en el uso de terminales fijos, móviles y fax.

- Servicio de red cableada, inalámbrica

  Diseño, administración y gestión de las comunicaciones soportadas sobre la red de cableado estructurado y red inalámbrica de la universidad, así como los accesos VPN.

Gestión de identidades

- Servicios de directorio

  Diseño, administración y gestión de la plataforma que almacena, organiza y publica información de contacto sobre los usuarios de la Universidad, gestión de Active Directory, OpenLdap y gestión de la Infraestructura de clave pública (PKI).

6. Política de seguridad

Una vez ubicados en el caso de estudio, para comenzar la adecuación al ENS, el primer ítem que se debería de abordar es la política de seguridad, es el documento que definirá todo lo aplicable y relacionado en términos de la seguridad de la información en la organización para su protección y prestación de servicios, adoptando para ello las medidas necesarias.

El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

El Esquema Nacional de Seguridad (ENS) hace referencia en varios puntos a la Política de Seguridad.

Artículo 11. Requisitos mínimos de seguridad:

> *"Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente."*

Artículo 12. Organización e implantación del proceso de seguridad

> *"La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa."*

ENS. Disposición transitoria. Adecuación de sistemas.

> *"Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo."*

ENS. Anexo II Medidas de Seguridad

> *"Marco organizativo [org]*
> *Política de seguridad [org.1]*
> *La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:*
>
> > *a) Los objetivos o misión de la organización.*
> > *b) El marco legal y regulatorio en el que se desarrollarán las actividades.*
> > *c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.*
> > *d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.*
> > *e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.*
> > *La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda."*

La política de seguridad es un documento imprescindible para cualquier organización que necesite adaptarse al ENS y debe de cumplir unos principios básicos:

> Artículo 5. La seguridad como un proceso integral.
>
> Artículo 6. Gestión de la seguridad basada en los riesgos.

Artículo 7. Prevención, reacción y recuperación.

Artículo 8. Líneas de defensa.

Artículo 9. Reevaluación periódica.

Artículo 10. La seguridad como función diferenciada.

Para la elaboración de la política, el CCN ha elaborado el documento de apoyo 805-ENS_politica, donde se detalla su elaboración de manera generalista en el Anexo III.

Para la mejor comprensión de la finalidad e información de la política de seguridad se muestra su elaboración sobre el caso de estudio de la universidad Exempli Gratia en el Anexo I del presente documento.

7. Revisión de la situación inicial

La situación inicial es la referencia y línea base que tomaremos como partida y que compararemos con el estado recomendado por el ENS, estas diferencias nos indicaran las acciones futuras a realizar.

Para obtener la línea base respecto al supuesto se realizara la evaluación con el marco de referencia o pautas de carácter general descrito en la guía “STIC 803 ENS-valoración” según lo establecido en el ENS respecto de las categorías de los sistemas descritas en el Anexo I y las medidas de seguridad descritas en el Anexo II.

Tal como se recomienda, se procederá a la valoración de los activos esenciales que son los que exigirán las valoraciones más restrictivas en las dimensiones de seguridad y determinaran la categoría del sistema.

7.1. Criterios de valoración

La finalidad de los criterios de valoración es establecer una categoría a los sistemas de información, cada Administración Publica ofrece unos servicios al ciudadano y está expuesta a unos riesgos, para homogeneizar su tratamiento y necesidades de protección de la información se establecen estos criterios que finalmente tras su tratamiento y aplicación al tipo de información y servicios ofrecidos por la organización se materializaran en una categoría del sistema de información.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para:

a. Alcanzar sus objetivos.
b. Proteger los activos a su cargo.
c. Cumplir sus obligaciones diarias de servicio.
d. Respetar la legalidad vigente.
e. Respetar los derechos de las personas.

Para lo que se deberá de valorar el impacto que tendría un incidente que afecte a la seguridad de la información y los sistemas. Para determinar ese impacto hay que tener en cuenta las dimensiones de la seguridad: Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T], en adelante [DICAT].

El impacto que tendría un incidente que pudiese ocurrir sobre cada información o cada servicio pueden afectar a una o más de sus dimensiones de seguridad y 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.

Un grupo de Información y/o Servicio formarán un sistema de información a categorizar, por tanto podemos confeccionar una tabla como la que sigue en donde para cada información y/o servicio de los que formarían nuestro sistema, establecemos como sería el nivel del impacto (Bajo, Medio o Alto) que un incidente produciría en cada una de las dimensiones de seguridad a tener en cuenta.

1- Nivel BAJO.

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

Se entenderá por perjuicio limitado:

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

- Que los activos de la organización sufrieran un daño menor.

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

- Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.

- Otros de naturaleza análoga.

2- Nivel MEDIO.

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

Se entenderá por perjuicio grave:

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

- Que los activos de la organización sufrieran un daño significativo.

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

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

- Otros de naturaleza análoga.

3- Nivel ALTO.

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

Se entenderá por perjuicio muy grave:

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

- Que los activos de la organización sufrieran un daño muy grave, e incluso irreparable.

- El incumplimiento grave de alguna ley o regulación.

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

- Otros de naturaleza análoga

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

- Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.

- 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.

- Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

Se destacan algunos aspectos que se tendrán en cuenta para realizar el análisis del caso de estudio:

- 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.

7.1.1. Valoración de la información

Como se ha indicado, el primero de los activos a valorar será el tipo de información manejada. No se valorarán directamente datos auxiliares que no son objeto directo del proceso administrativo y sólo aparecen como instrumentales para la prestación de los servicios. Por ejemplo, servicios de directorio, claves de acceso, etc.

La información suele imponer requisitos relevantes en las dimensiones de confidencialidad, integridad, autenticidad y trazabilidad. No suelen haber requisitos relevantes en la dimensión de disponibilidad.

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.

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.

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 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.

7.1.2. Valoración de los servicios

El segundo aspecto importante a valorar son los servicios de la organización. Se entiende por servicio cada actividad llevada a cabo por la Administración o, bajo un cierto control y regulación de esta, por una organización, especializada o no, y destinada a satisfacer necesidades de la colectividad.

El Esquema Nacional de Seguridad se limita a valorar aquellos servicios que son relevantes para el proceso administrativo. Algunos de estos servicios pueden estar identificados en algún tipo de ordenamiento general, mientras que otros serán particulares del organismo. En cualquier caso, los servicios aquí contemplados tienen identidad propia con independencia de los medios que se empleen para su prestación, asumiendo el organismo que los presta unas obligaciones con respecto a los mismos.

Como norma general, no se valoran servicios internos o auxiliares tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc. Como excepción a la norma, en el caso particular de una Universidad como Exempli Gratia tendremos algunos de estos servicios en consideración como el correo electrónico por dar cobertura al alumnado y subcontratas externas en algunos casos (además de PDI y PAS), dejando de ser considerado servicio interno.

La valoración de un servicio la determina el responsable del mismo teniendo en cuenta la naturaleza del servicio y la normativa que pudiera serle de aplicación. Esta valoración requiere un conocimiento legal de la materia de que se trate.

Habitualmente los servicios establecen requisitos relevantes en términos de disponibilidad. También es habitual que los demás requisitos de seguridad sobre los servicios deriven de los de la información que se maneja.

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.

Cuando un aspecto no requiere medidas de seguridad, en el apartado de valoración se indicará SIN VALORAR

7.2. Análisis del caso de estudio Universidad Exempli Gratia – Categorización de los sistemas

Teniendo en cuenta las pautas anteriores se realiza el análisis del caso de estudio de la Universidad Exempli Gratia.

En noviembre de 2017 el CCN elabora el Anexo I de la guía de seguridad CCN-STIC 803 que introduce criterios de valoración específicos del ámbito universitario, con un catálogo de información y servicios habituales, indicando que estos pueden ser extendidos o personalizados según sus propias necesidades.

La guía debe de ser utilizada como apoyo únicamente, ya que las soluciones planteadas no son únicas y no se diluye la responsabilidad de las entidades afectadas en el deber de categorizar adecuadamente los sistemas de información.

Con esta perspectiva se ajustan los servicios ofrecidos por la Universidad Exempli Gratia caso de estudio con su propia organización interna.

Conviene comenzar por los activos de tipo información, valorando en este orden: confidencialidad (indicado en la matriz como [C]), integridad [I], autenticidad [A], trazabilidad [T] y, si fuera relevante, disponibilidad [D]. Es frecuente que la disponibilidad no sea un atributo relevante de la información y quede sin adscribir a ningún nivel. Cuando una dimensión no condiciona las medidas de seguridad, en el apartado de valoración se indicará como “NO ADSCRITA” o “N/A”.

Estos activos se corresponden con la información manejada por los distintos servicios ofrecidos por la Universidad Exempli Gratia, en función de los cuales se establecerán las dimensiones.

Se opta por la agrupación de activos de tipo información similares para la universidad Exempli Gratia, lo que simplificará la clasificación y la futura protección de los datos protegiendo la información con los mismos tratamientos.

DIMENSIONES UNIVERSIDAD “EXEMPLI GRATIA”

Activos de tipo Información y descripción		C	I	A	T
I1 – Información Aula Virtual	Información sobre los alumnos, contenidos de asignaturas, debates, ejercicios, etc. Pertenecientes al Aula Virtual	B	B	B	B
I2 - Licencias	Licencias software de los equipos corporativos	B	B	B	B
I3 – Expedientes	Información sobre los expedientes académicos, títulos, exámenes, Tesis y estudiantes con necesidades educativas especiales	M	M	M	M

I4 – Información supercomputación	Información sobre los datos manejados en proyectos de supercomputación	B	B	B	B
I5 - Asignaturas	Contenido de las distintas asignaturas de las titulaciones.	B	B	B	B
I6 – Plan Docente	Asignación de asignaturas a los docentes y horarios de docencia	B	B	B	B
I7 – Expedientes administrativos	Datos pertenecientes a los expedientes administrativos	B	B	B	B
I8 – Investigación	Datos de gestión de proyectos de investigación	B	B	B	B
I9 – Datos económicos	Datos de gestión económica de la Universidad, presupuestos, ingresos y contabilidad	N/A	B	B	B
I10 – Contratación	Datos relativos a los expedientes de contratación	B	B	B	B
I11 – Patrimonio e inventario	Bienes muebles e inmuebles de la Universidad e inventario de los mismos.	N/A	N/A	B	B
I12 - Personal	Datos del personal de la Universidad, selección, acceso, expedientes, relación de Puestos de Trabajo, Control Horario, Valoración del Desempeño y formación	M	B	B	B
I13 - Prevención	Datos de los procesos de prevención, incluyendo procesos de revisión médica de los recursos humanos de la Universidad	M	M	M	M
I14 - Retribuciones	Retribuciones del personal de la Universidad	M	M	M	M
I15 – Actividades deportivas	Datos gestionados por el Servicio de Deportes	B	B	B	B
I16 - Archivo	Datos del Archivo universitario en diferentes soportes como documentos, fichas, DVD, negativos y positivos fotográficos, cuadernos, películas e impresos.	B	B	B	B
I17 - Registro	Datos del Registro universitario, incluyendo procesos de entrada/salida, en modalidad presencial y telemática	M	M	M	M
I18 - Documentación	Datos de gestión documental institucional, convenios, normativa universitaria, procesos electorales, censo y publicaciones	B	B	B	B
I19 - Infraestructuras	Datos de los espacios universitarios, incluyendo procesos de reserva de los mismos, control de acceso a edificios e instalaciones	B	B	B	B
I20 - Biblioteca	Aplicaciones para la gestión de los procesos soportados por la Biblioteca universitaria, repositorio institucional de la Universidad y catálogo de Biblioteca.	B	B	B	B
I21 – Almacén de datos	Análisis de datos, e información institucional, como el Datawarehouse.	N/A	B	B	N/A
I22 – Atención al usuario (CAU)	Datos de peticiones e incidencias relacionadas con los servicios universitarios	B	B	B	B
I23 – Correo electrónico	Datos correo electrónico (mensajes, listas…) destinado al PAS, PDI, estudiantes universitarios, preuniversitarios y egresados.	N/A	N/A	N/A	N/A
I24 - Material audiovisual y fotográfico	Imágenes, voz, video, grabaciones de video-vigilancia.	B	B	B	B
I25 - Directorio	Información de contacto sobre los usuarios de la Universidad.	N/A	N/A	N/A	N/A
I26 – Registros de acceso y navegación	Registros de acceso a los sistemas, registros de navegación interna/Internet, etc.	N/A	N/A	N/A	N/A

Ilustración 2: Dimensiones información universidad Exempli Gratia

Una vez categorizados los datos, se obtiene el valor máximo para cada dimensión según el Anexo I del ENS.

En el caso de estudio se observan los siguientes valores máximos para cada dimensión:

- Confidencialidad [C]: M
- Integridad [I]: M
- Autenticidad [A] M
- Trazabilidad [T]: M

La evaluación se debe de realizar por cada sistema y subsistema, con lo que se puede realizar el análisis común de todos los sistemas, ya que prevalecerá el valor máximo.

Finalmente la categoría del sistema quedará establecida por el valor más alto de las dimensiones.

Categoría global final Aprobada: Categoría Media para los activos de tipo información.

Conviene seguir con los activos de tipo servicio, valorando para los mismos la Disponibilidad [D]. Los requisitos en materia de confidencialidad, integridad, Autenticidad y trazabilidad suelen venir impuestos por los tipos de información que maneja el servicio, asumiendo los establecidos en el párrafo anterior.

SERVICIOS UNIVERSIDAD "EXEMPLI GRATIA"

Áreas	Activo de tipo Servicio	D
A1 - Área Docente	A1-S1- Soporte a las aulas informáticas de libre acceso y de docencia.	B
	A1-S2- Soporte a las aulas multimedia.	B
	A1-S3- Gestión de licenciamiento.	M
	A1-S4- Aula Virtual	M
A2-Area investigadora	A2-S1- Supercomputación	M
	A2-S2- Consultoría	B
A3 – Área de gestión	A3-S1- Gestión académica	M
	A3-S2- Gestión económica y tesorería	B
	A3-S3- Contratación y presupuestos	B
	A3-S4- Gestión de RR.HH.	B
	A3-S5 -Extensión Universitaria	B
	A3-S6- Archivo	B
	A3-S7- Secretaria general	M
	A3-S8- Gestión de infraestructuras	B
	A3-S9- Servicio de bibliotecas	B
	A3-S10- Comunicación	B
	A3-S11- Calidad	B

	A3-S12- Análisis de datos	B
	A3-S13- Atención al usuario (CAU)	B
	A3-S14- Gestión de publicaciones	B
A4- Área de correo, herramientas colaborativas y publicación Web.	A4-S1- Gestión del correo electrónico	B
	A4-S2- Web institucional	M
	A4-S3- Sede electrónica	M
	A4-S4- Intranet	B
	A4-S5- Portal del empleado	B
	A4-S6- Secretaria virtual	B
	A4-S7- Contenidos digitales	B
A5- Soporte y equipamiento del puesto de trabajo	A5-S1- Servicio integral Workplace	N/A
A6- Servicio de comunicaciones	A6-S1- Servicio de Telefonía fija, móvil y fax	N/A
	A6-S2- Servicio de red cableada e inalámbrica	N/A
A7- Gestión de identidades	A7-S1- Servicios de directorio	N/A

Ilustración 3: Dimensiones servicios universidad Exempli Gratia

Al igual que en el caso de las dimensiones, categorizados los datos se obtiene el valor máximo para la dimensión [D] objeto de estudio.

Categoría final Aprobada: Categoría Media para los activos de tipo Servicio.

Por lo tanto:

La categoría final del sistema será categoría Media.

8. Datos de carácter personal. RGPD vs ENS.

Una de las problemáticas que surgen en el tratamiento de los activos del tipo de información es la conexión con los datos de carácter personal y su respectivo tratamiento.

Los datos de carácter personal son datos que hacen referencia a personas físicas registradas sobre cualquier soporte, informático o no, son tipos de datos de información del sistema de información, y como tal, hay que protegerlos, ahora bien, las medidas de seguridad sobre las que trabaja el ENS pueden ser compartidas o no, ya que los datos de carácter cuentan con su propio tratamiento y normativa.

A partir del 25 de mayo de 2018, cuando el sistema tenga por objeto el tratamiento de datos personales, se tendrá en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la normativa nacional que en su momento complemente lo dispuesto en dicha norma europea y por el que se deroga la Directiva 95/46/CE.

En el caso de estudio los datos de carácter personal quedarán fuera del documento de adecuación al ENS, y aunque se deben de tener en cuenta, bastará una referencia a partir del 25 de mayo al Documento de Seguridad requerido por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

9. Medidas de seguridad

Una vez analizados y valorados los activos pertenecientes a información y a los servicios, y obtenido una valoración para el sistema de información se tendrá que analizar las medidas de seguridad que deben de ser aplicadas según los resultados obtenidos.

Para definir su aplicación el ENS establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración (Anexo I) del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.

Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.

El grado de madurez caracterizara la implementación del proceso, midiendo el grado o nivel de profesionalización de la actividad. Se establecerán los siguientes:

Nivel	Descripción
L0	Inexistente. Esta medida no está siendo aplicada en este momento.
L1	Inicial / ad hoc. En el nivel L1 de madurez, el proceso existe, pero no se gestiona. La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de alta calidad.
L2	Repetible, pero intuitivo. En el nivel L2 de madurez, la eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
L3	Proceso definido. Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos

	garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece. Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.
L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel L3, la confianza era solamente cualitativa.
L5	Optimizado. El nivel L5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos. En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Ilustración 4: Grado de madurez

En el caso de estudio, tomaremos como referencia general una institución que se ha preocupado por adaptarse rápidamente tanto a los cambios tecnológicos en constante evolución como a la normativa vigente. Sin embargo, para poder tratar todos los procesos, especialmente el de auditoria y analizar toda la casuística posible, se indicara algún nivel por debajo del requerido, mostrando deficiencias para su estudio en otros apartados más adelante.

NIVELES UNIVERSIDAD EXEMPLI GRATIA

MARCO	ID	MEDIDAS DE SEGURIDAD/ARTICULO	NIVEL
Organizativo	**org.1**	Política de seguridad	L4
	org.2	Normativa de seguridad	L3
	org.3	Procedimientos de seguridad	L3
	org.4	Proceso de autorización	L1
Operacional	**op.pl**	Planificación	L2
	op.pl.1	Análisis de riesgos	L3
	op.pl2	Arquitectura de seguridad	L3
	op.pl3	Adquisición de nuevos componentes	L3
	op.pl4	Dimensionamiento / Gestión de capacidades	L2
	op.pl5	Componentes certificados	L2
	op.acc	Control de acceso	
	op.acc.1	Identificación	L3
	op.acc.2	Requisitos de acceso	L3
	op.acc.3	Segregación de funciones y tareas	L3
	op.acc.4	Proceso de gestión de derechos de acceso	L2

	op.acc.5	Mecanismo de autenticación	L2
	op.acc.6	Acceso local (local login)	L3
	op.acc.7	Acceso remoto (remote login)	L3
	op.exp	Explotación	
	op.exp.1	Inventario de activos	L3
	op.exp.2	Configuración de seguridad	L3
	op.exp.3	Gestión de la configuración	L2
	op.exp.4	Mantenimiento	L2
	op.exp.5	Gestión de cambios	L3
	op.exp.6	Protección frente a código dañino	L4
	op.exp.7	Gestión de incidencias	L4
	op.exp.8	Registro de la actividad de los usuarios	L3
	op.exp.9	Registro de la gestión de incidencias	L3
	op.exp.10	Protección de los registros de actividad	L3
	op.exp.11	Protección de claves criptográficas	L3
	op.ext	Servicios externos	
	op.ext.1	Contratación y acuerdos de nivel de servicio	L4
	op.ext.2	Gestión diaria	L4
	op.ext.9	Medios alternativos	L3
	op.mon	Monitorización del sistema	
	op.mon.1	Detección de intrusión	L4
	op.mon.2	Sistema de métricas	L3
Medidas de protección	**mp.if**	Medidas de Protección	
	mp.if.1	Áreas separadas y con control de acceso	L5
	mp.if.2	Identificación de las personas	L4
	mp.if.3	Acondicionamiento de los locales	L3
	mp.if.4	Energía eléctrica	L4
	mp.if.5	Protección frente a incendios	L4
	mp.if.6	Protección contra inundaciones	L2
	mp.if.7	Registro de entrada y salida de equipamiento	L3
	mp.if.9	Instalaciones alternativas	L5
	mp.per	Gestión del personal	
	mp.per.1	Caracterización del lugar de trabajo	L2
	mp.per.2	Deberes y obligaciones	L3
	mp.per.3	Concienciación	L3
	mp.per.4	Formación	L3
	mp.per.9	Personal alternativo	L2
	mp.eq	Protección de los equipos	
	mp.eq.1	Lugar de trabajo ordenado	L2
	mp.eq.2	Bloqueo de puesto de trabajo	L4
	mp.eq.3	Protección de equipos portátiles	L4
	mp.eq.9	Medios alternativos	L3
	mp.com	Protección de las comunicaciones	
	mp.com.1	Perímetro seguro	L4
	mp.com.2	Protección de la confidencialidad	L3
	mp.com.3	Protección de la autenticidad y de la integridad	L3
	mp.com.4	Segregación de redes	L5
	mp.com.9	Medios alternativos	L3
	mp.si	Protección de los soportes de información	
	mp.si.1	Etiquetado	L3

	mp.si.2	Criptografía	L3
	mp.si.3	Custodia	L3
	mp.si.4	Transporte	L3
	mp.si.5	Borrado y destrucción	L3
	mp.sw	Protección de las aplicaciones informáticas	
	mp.sw.1	Desarrollo	L3
	mp.sw.2	Aceptación y puesta en servicio	L3
	mp.info	Protección de la información	
	mp.info.1	Datos de carácter personal	L3
	mp.info.2	Calificación de la información	L3
	mp.info.3	Cifrado	L4
	mp.info.4	Firma electrónica	L4
	mp.info.5	Sellos de tiempo	L4
	mp.info.6	Limpieza de documentos	L3
	mp.info.9	Copias de seguridad (backup)	L5
	mp.s	Protección de los servicios	
	mp.s.1	Protección del correo electrónico	L3
	mp.s.2	Protección de servicios y aplicaciones web	L3
	mp.s.8	Protección frente a la denegación de servicio	L4
	mp.s.9	Medios alternativos	L3

Ilustración 5: Niveles universidad Exempli Gratia

Como ejemplo de tratamiento se observa que en el marco organizativo se debe de contar con una política de seguridad, id: org.1 independientemente de la categoría básica, media o alta que se tenga como resultado del análisis visto previamente. Este documento escrito, deberá de contener:

- Los objetivos o misión de la organización.

- El marco legal y regulatorio en el que se desarrollarán las actividades.

- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.

- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

El nivel de la política de seguridad será fijado en función del cumplimiento con los objetivos indicados. Para la tabla descrita anteriormente, se asume que en el marco organizativo con Identificador org.1 respecto de la política de

seguridad en el caso de estudio de la universidad Exempli Gratia que se obtiene un nivel L4:

L4	Gestionado y medible. Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel L3, la confianza era solamente cualitativa.

Este análisis será realizado para cada medida de seguridad.

10. Análisis de riesgos.

Una vez realizada la valoración del sistema de información y se cuenta con las medidas de seguridad aplicables, se deberá de valorar los riesgos asociados.

Dependemos fuertemente de los sistemas de información para cumplir nuestros objetivos y lo ideal sería que los sistemas no fallen. Pero lo cierto es que se hace necesario convivir con sistemas que están sujetos a fallos, errores, vulnerabilidades o malas praxis. El asunto no es tanto la ausencia de incidentes como la confianza en que están bajo control, ser conscientes que puede pasar y que se sabrá qué hacer si llega a pasar. Para ello, necesitaremos conocer los riesgos que pueden afectar a los sistemas de información para poder afrontarlos y controlarlos. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos.

En el Esquema Nacional de Seguridad [RD 3/2010], el Capítulo II Principios Básicos, dice:

> *Artículo 6. Gestión de la seguridad basada en los riesgos.*
>
> 1. *El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.*
>
> *2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.*

Para lidiar con la gestión del riesgo, el CCN pone a disposición de las administraciones públicas tanto el software necesario como los manuales de gestión de este software para su correcto tratamiento.

Aunque existen otras, la metodología común utilizada para el tratamiento de riesgos es Magerit en su versión 3 y responde a lo que se denomina “Proceso de Gestión de los Riesgos”, en otras palabras, implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de

gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Hay varias aproximaciones al problema de analizar los riesgos soportados por los sistemas TIC: guías informales, aproximaciones metódicas y herramientas de soporte. Todas buscan objetivar el análisis de riesgos para saber cuán seguros (o inseguros) son los sistemas y no llevarse a engaño. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

A grandes rasgos Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

10.1. Herramienta PILAR

CCN pone a disposición la herramienta PILAR, que soporta el análisis y tratamiento de riesgos de un sistema de información siguiendo la metodología indicada Magerit v3 (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). La herramienta se actualiza periódicamente y existen diversas versiones:

- 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

Para el caso de estudio se cuenta con μPILAR con una licencia para fines educativos con funcionalidades limitadas.

La herramienta analiza los riesgos en las dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

La parametrización del programa se realizará trasladando la valoración de activos de tipo información y servicios vistos anteriormente.

Para su comprensión, se muestran algunos pantallazos del proceso de parametrización de PILAR.

En primer lugar se incorporarán los activos de tipo información, en la figura se muestra para la universidad Exempli Gratia el primero de ellos, que es la Información sobre el Aula Virtual.

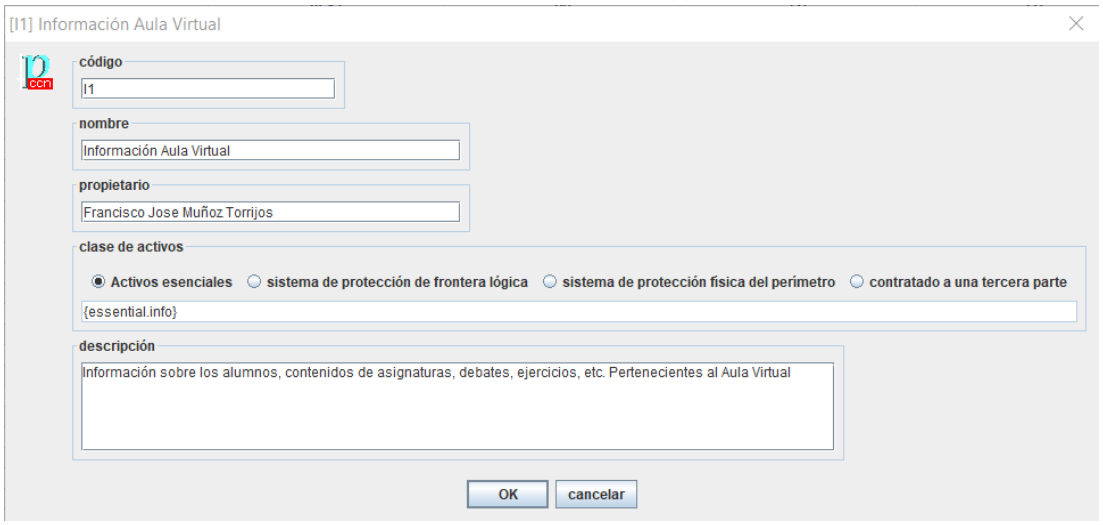


Ilustración 6: Herramienta PILAR. Activos de tipo información

Se incorporarán de igual manera los datos pertenecientes a los servicios, en el caso de Exempli Gratia el primero será el Soporte a las Aulas informáticas de libre acceso y de docencia.

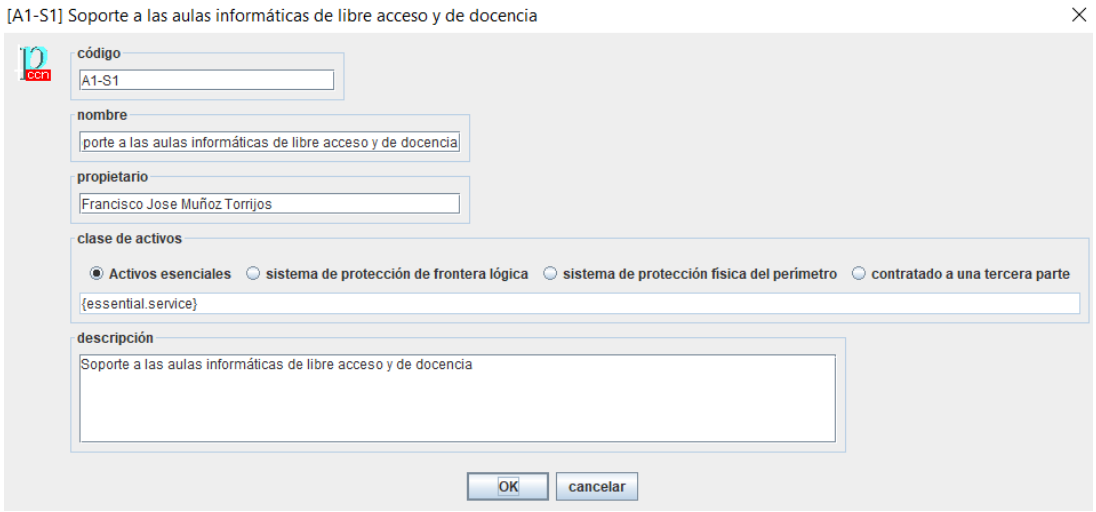
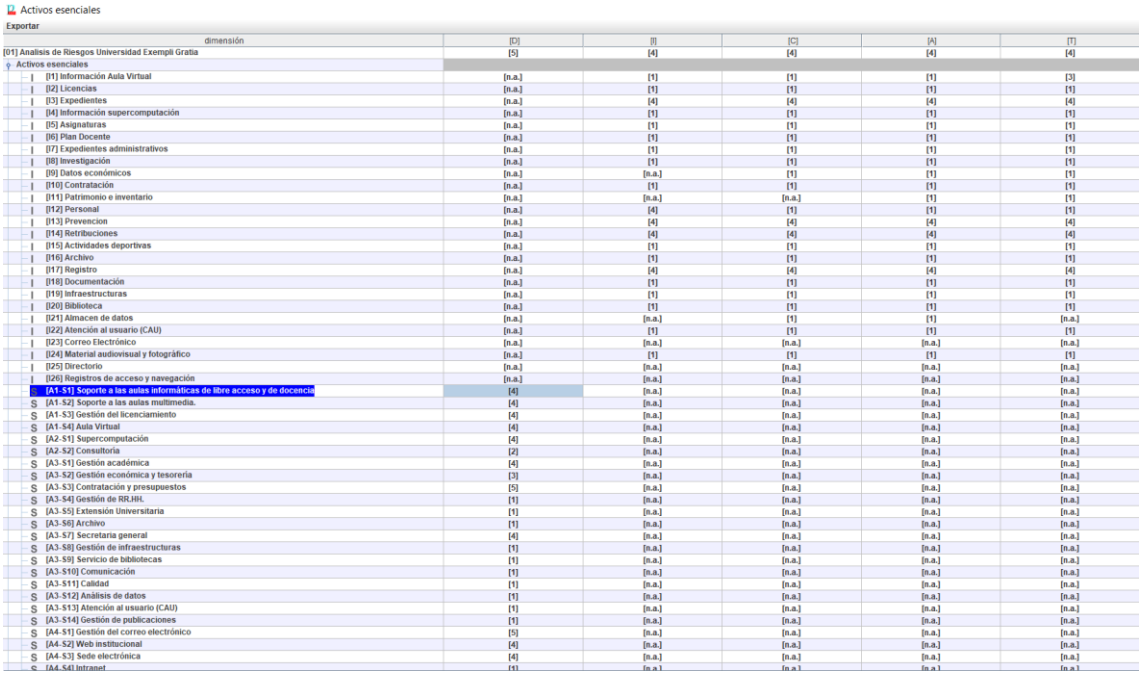


Ilustración 7: Herramienta PILAR. Activos de tipo servicio

Una vez creados los activos informacion y servicio se procederá al traslado de sus valoraciones en cada dimensión, se muestra el resultado del caso de estudio.



Activos esenciales

Exportar

dimensión	[D]	[I]	[C]	[A]	[T]
[01] Analisis de Riesgos Universidad Exempli Gratia	[5]	[4]	[4]	[4]	[4]
Activos esenciales					
[I1] Información Aula Virtual	[n.a.]	[1]	[1]	[1]	[3]
[I2] Licencias	[n.a.]	[1]	[1]	[1]	[1]
[I3] Expedientes	[n.a.]	[4]	[4]	[4]	[4]
[I4] Información supercomputación	[n.a.]	[1]	[1]	[1]	[1]
[I5] Asignaturas	[n.a.]	[1]	[1]	[1]	[1]
[I6] Plan Docente	[n.a.]	[1]	[1]	[1]	[1]
[I7] Expedientes administrativos	[n.a.]	[1]	[1]	[1]	[1]
[I8] Investigación	[n.a.]	[1]	[1]	[1]	[1]
[I9] Datos económicos	[n.a.]	[n.a.]	[1]	[1]	[1]
[I10] Contratación	[n.a.]	[1]	[1]	[1]	[1]
[I11] Patrimonio e inventario	[n.a.]	[n.a.]	[n.a.]	[1]	[1]
[I12] Personal	[n.a.]	[4]	[1]	[1]	[1]
[I13] Prevencion	[n.a.]	[4]	[4]	[4]	[4]
[I14] Retribuciones	[n.a.]	[4]	[4]	[4]	[4]
[I15] Actividades deportivas	[n.a.]	[1]	[1]	[1]	[1]
[I16] Archivo	[n.a.]	[1]	[1]	[1]	[1]
[I17] Registro	[n.a.]	[4]	[4]	[4]	[4]
[I18] Documentación	[n.a.]	[1]	[1]	[1]	[1]
[I19] Infraestructuras	[n.a.]	[1]	[1]	[1]	[1]
[I20] Biblioteca	[n.a.]	[1]	[1]	[1]	[1]
[I21] Almacen de datos	[n.a.]	[n.a.]	[1]	[1]	[n.a.]
[I22] Atención al usuario (CAU)	[n.a.]	[1]	[1]	[1]	[1]
[I23] Correo Electrónico	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[I24] Material audiovisual y fotográfico	[n.a.]	[1]	[1]	[1]	[1]
[I25] Directorio	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[I26] Registros de acceso y navegación	[n.a.]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A1-S2] Soporte a las aulas multimedia.	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A1-S3] Gestión del licenciamiento	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A1-S4] Aula Virtual	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A2-S1] Supercomputación	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A2-S2] Consultoría	[2]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S1] Gestión académica	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S2] Gestión económica y tesorería	[3]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S3] Contratación y presupuestos	[5]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S4] Gestión de RR.HH.	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S5] Extensión Universitaria	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S6] Archivo	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S7] Secretaria general	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S8] Gestión de infraestructuras	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S9] Servicio de bibliotecas	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S10] Comunicación	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S11] Calidad	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S12] Análisis de datos	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S13] Atención al usuario (CAU)	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A3-S14] Gestión de publicaciones	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A4-S1] Gestión del correo electrónico	[5]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A4-S2] Web institucional	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A4-S3] Sede electrónica	[4]	[n.a.]	[n.a.]	[n.a.]	[n.a.]
[A4-S4] Intranet	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]

Ilustración 8: Listado de activos información y servicios caso de estudio

Se deberá de valorar cada activo de tipo Información y de tipo servicio estableciendo un criterio de valoración según unos parámetros ofrecidos por la herramienta. Esto se realizará para cada una de las dimensiones en las que el activo este definido, adecuándolo de la siguiente forma:

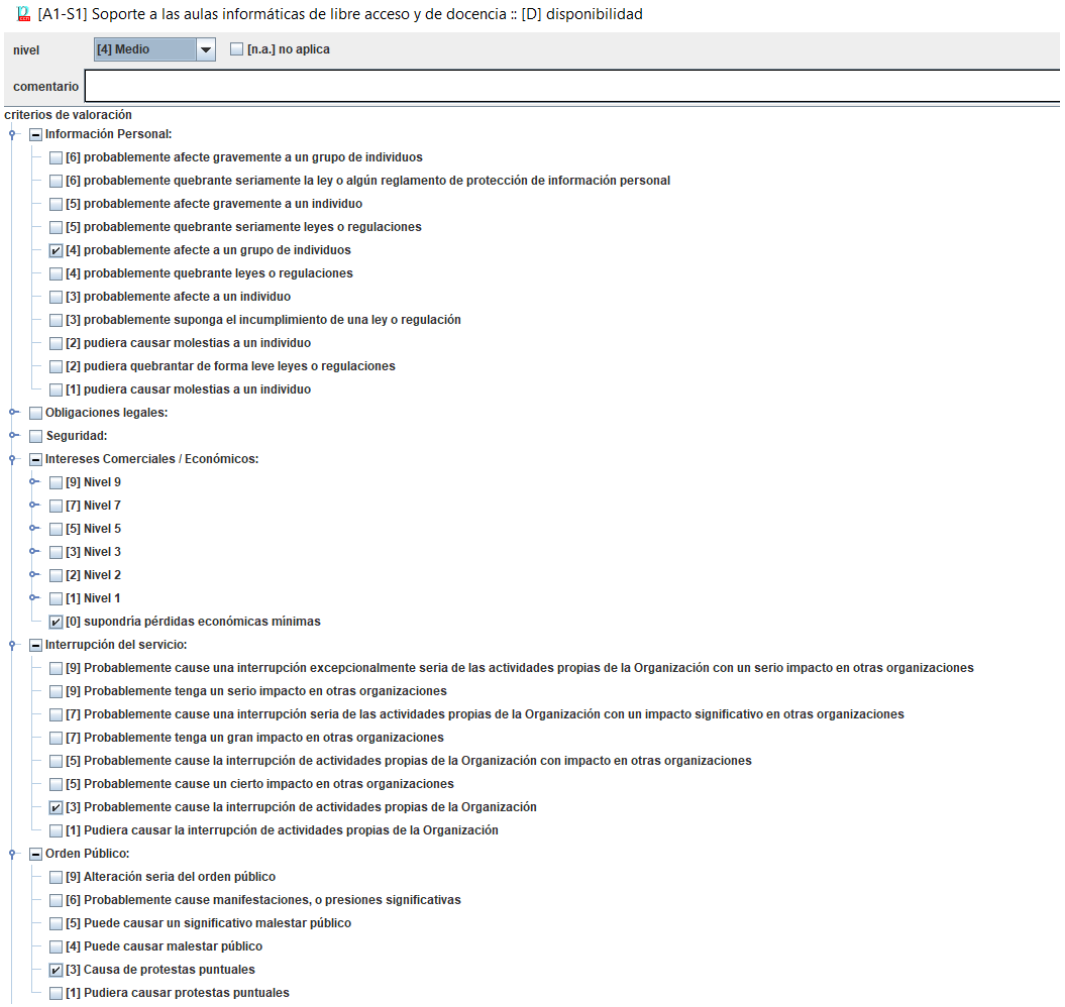


Ilustración 9: Herramienta PILAR. Valoración de activos

Lo siguiente será declarar otros tipos de activos presentes en la organización:

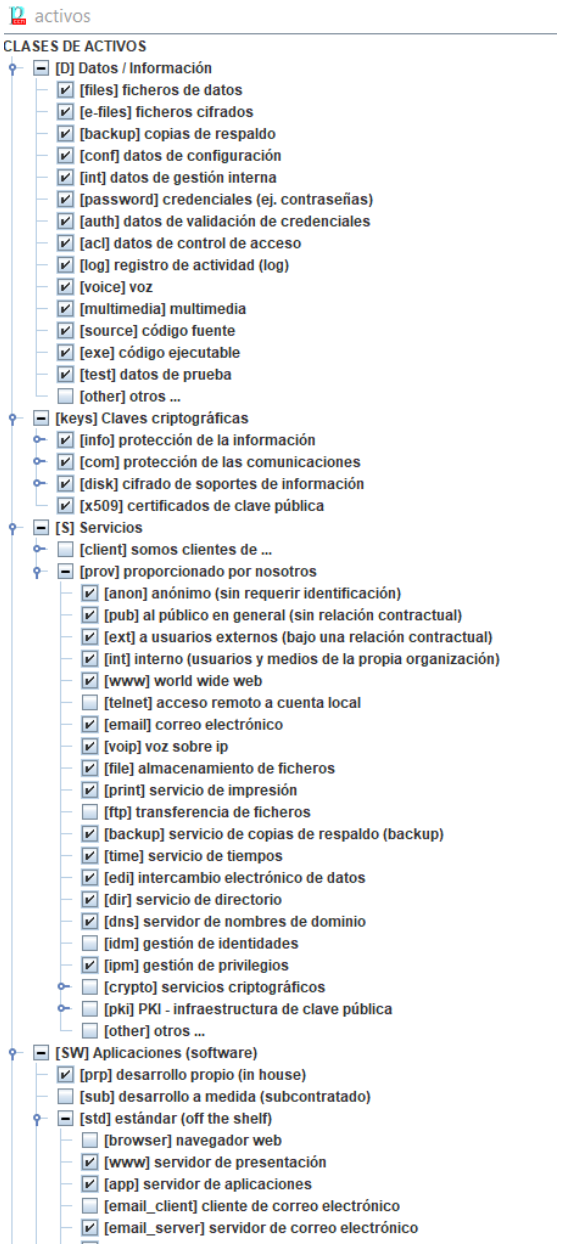


Ilustración 10: Herramienta PILAR. Clases de activos

Una vez establecidos se procede a establecer algunas características del sistema en terminos de agravantes o atenuantes. Cada organización por su propia naturaleza cuenta con un determinado riesgo respecto a la motivacion o atractivo para un posible atacante, personal interno, beneficios obtenidos, etc. Como se muestra a continuacion.

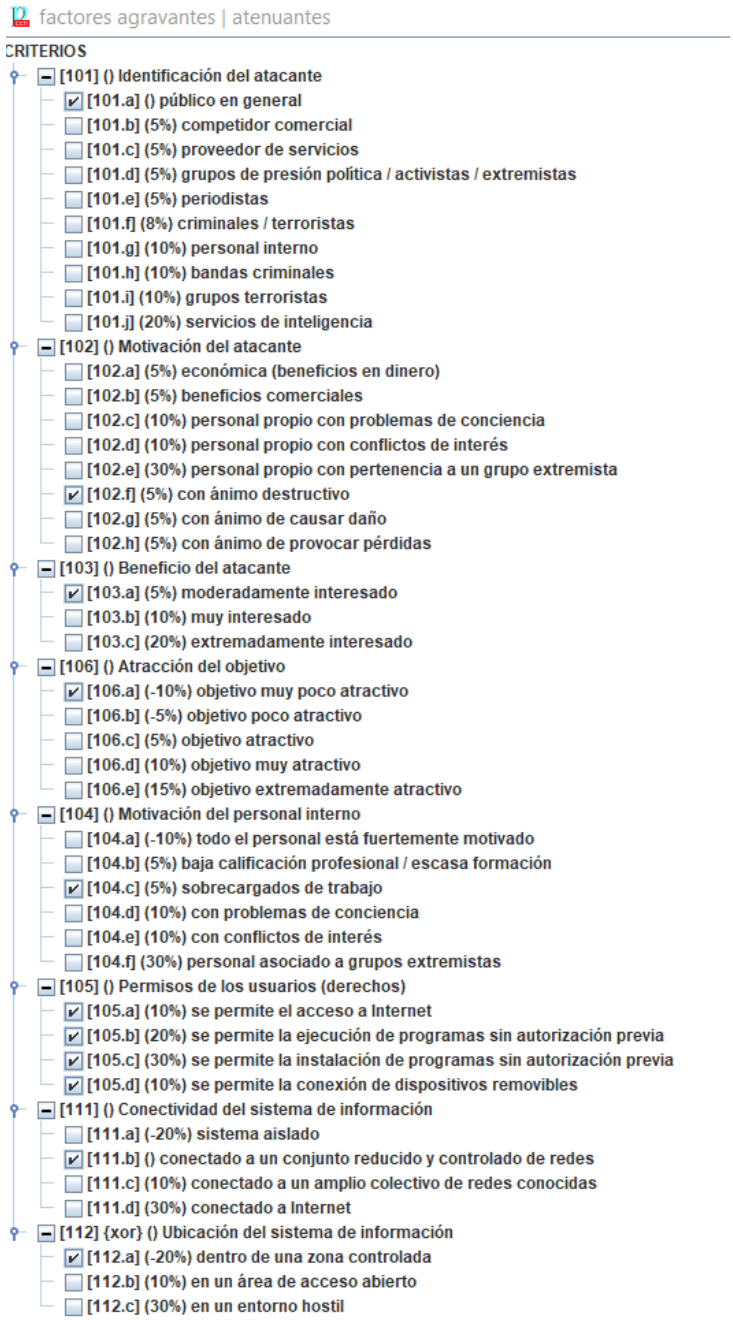


Ilustración 11: Herramienta PILAR. Factores agravantes y atenuantes

Finalizada la incorporacion de datos y caracterización de diversos factores se presenta el cumplimiento de un perfil de seguridad, este puede estar basado en el porcentaje del cumplimiento de los controles:

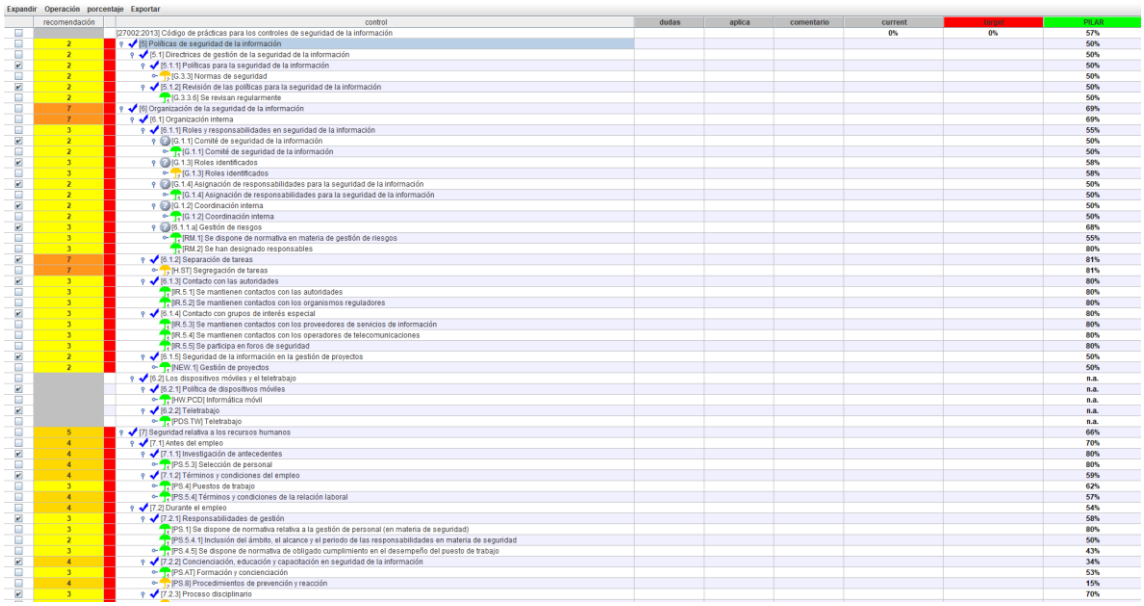


Ilustración 12: Herramienta PILAR. Porcentajes

O en la madurez de los controles:

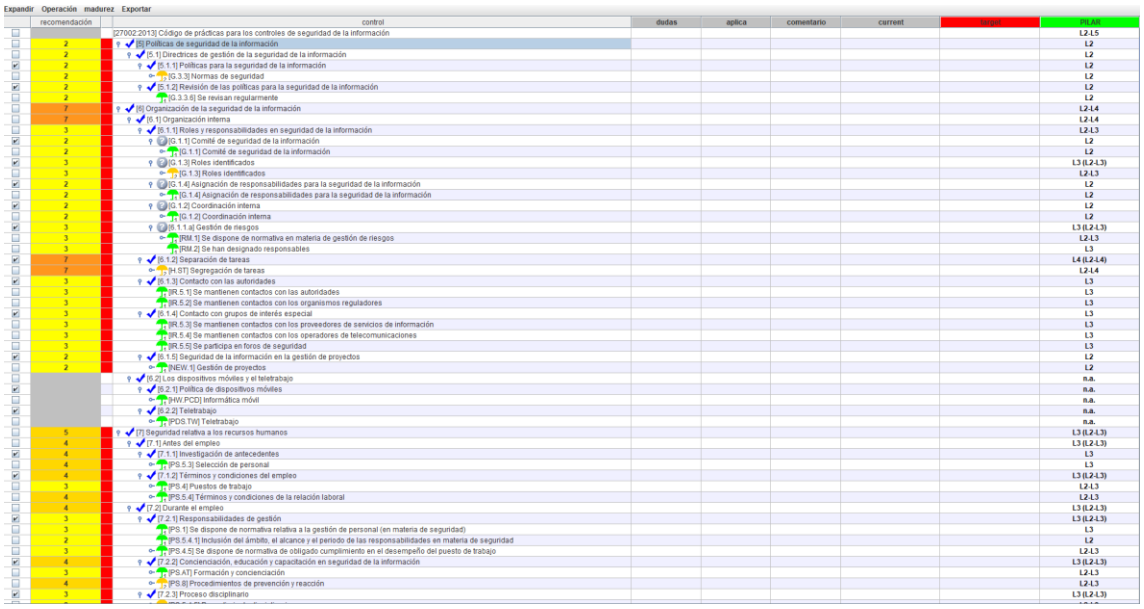
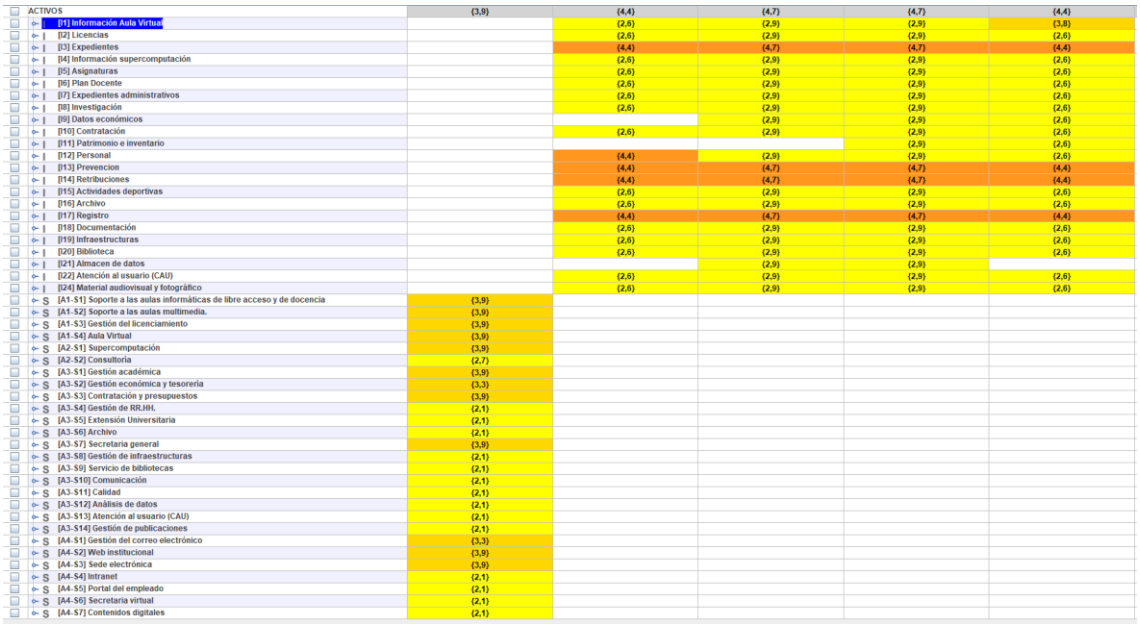


Ilustración 13: Herramienta PILAR. Madurez

Finalmente se obtiene la evaluacion de riesgos.



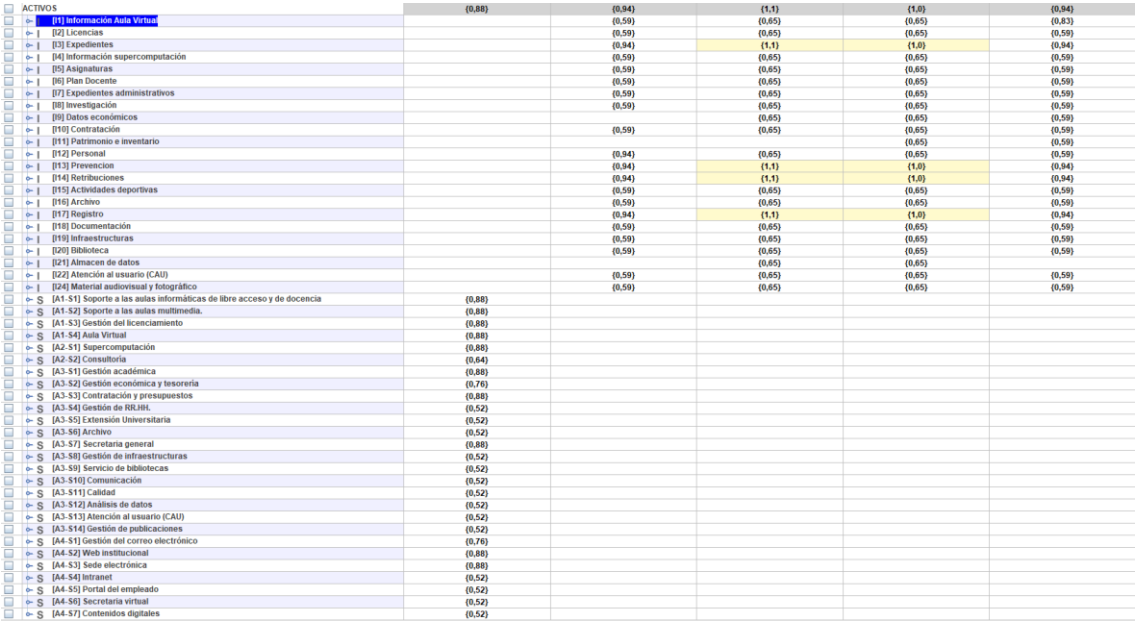
ACTIVOS	(3,9)	(4,4)	(4,7)	(4,7)	(4,4)
[I1] Información Aula Virtual		(2,6)	(2,9)	(2,9)	(3,8)
[I2] Licencias		(2,6)	(2,9)	(2,9)	(2,6)
[I3] Expedientes		(4,4)	(4,7)	(4,7)	(4,4)
[I4] Información supercomputación		(2,6)	(2,9)	(2,9)	(2,6)
[I5] Asignaturas		(2,6)	(2,9)	(2,9)	(2,6)
[I6] Plan Docente		(2,6)	(2,9)	(2,9)	(2,6)
[I7] Expedientes administrativos		(2,6)	(2,9)	(2,9)	(2,6)
[I8] Investigación		(2,6)	(2,9)	(2,9)	(2,6)
[I9] Datos económicos			(2,9)	(2,9)	(2,6)
[I10] Contratación		(2,6)	(2,9)	(2,9)	(2,6)
[I11] Patrimonio e inventario				(2,9)	(2,6)
[I12] Personal		(4,4)	(2,9)	(2,9)	(2,6)
[I13] Prevencion		(4,4)	(4,7)	(4,7)	(4,4)
[I14] Retribuciones		(4,4)	(4,7)	(4,7)	(4,4)
[I15] Actividades deportivas		(2,6)	(2,9)	(2,9)	(2,6)
[I16] Archivo		(2,6)	(2,9)	(2,9)	(2,6)
[I17] Registro		(4,4)	(4,7)	(4,7)	(4,4)
[I18] Documentación		(2,6)	(2,9)	(2,9)	(2,6)
[I19] Infraestructuras		(2,6)	(2,9)	(2,9)	(2,6)
[I20] Biblioteca		(2,6)	(2,9)	(2,9)	(2,6)
[I21] Almacen de datos			(2,9)	(2,9)	
[I22] Atención al usuario (CAU)		(2,6)	(2,9)	(2,9)	(2,6)
[I24] Material audiovisual y fotográfico		(2,6)	(2,9)	(2,9)	(2,6)
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	(3,9)				
[A1-S2] Soporte a las aulas multimedia.	(3,9)				
[A1-S3] Gestión del licenciamiento	(3,9)				
[A1-S4] Aula Virtual	(3,9)				
[A2-S1] Supercomputación	(3,9)				
[A2-S2] Consultoría	(2,7)				
[A3-S1] Gestión académica	(3,9)				
[A3-S2] Gestión económica y tesorería	(3,3)				
[A3-S3] Contratación y presupuestos	(3,9)				
[A3-S4] Gestión de RR.HH.	(2,1)				
[A3-S5] Extensión Universitaria	(2,1)				
[A3-S6] Archivo	(2,1)				
[A3-S7] Secretaría general	(3,9)				
[A3-S8] Gestión de infraestructuras	(2,1)				
[A3-S9] Servicio de bibliotecas	(2,1)				
[A3-S10] Comunicación	(2,1)				
[A3-S11] Calidad	(2,1)				
[A3-S12] Análisis de datos	(2,1)				
[A3-S13] Atención al usuario (CAU)	(2,1)				
[A3-S14] Gestión de publicaciones	(2,1)				
[A4-S1] Gestión del correo electrónico	(3,3)				
[A4-S2] Web institucional	(3,9)				
[A4-S3] Sede electrónica	(3,9)				
[A4-S4] Intranet	(2,1)				
[A4-S5] Portal del empleado	(2,1)				
[A4-S6] Secretaría virtual	(2,1)				
[A4-S7] Contenidos digitales	(2,1)				

Ilustración 14: Herramienta PILAR. Evaluación de Riesgos

Caracterizados en los siguientes niveles de criticidad:

Ilustración 15: Herramienta PILAR. Niveles de criticidad

La siguiente tabla muestra el riesgo residual que quedará si se persiguen las recomendaciones de PILAR para el caso de estudio:



ACTIVOS	{0,88}	{0,94}	{1,1}	{1,0}	{0,94}
[I1] Información Aula Virtual		{0,59}	{0,65}	{0,65}	{0,83}
[I2] Licencias		{0,59}	{0,65}	{0,65}	{0,59}
[I3] Expedientes		{0,94}	{1,1}	{1,0}	{0,94}
[I4] Información supercomputación		{0,59}	{0,65}	{0,65}	{0,59}
[I5] Asignaturas		{0,59}	{0,65}	{0,65}	{0,59}
[I6] Plan Docente		{0,59}	{0,65}	{0,65}	{0,59}
[I7] Expedientes administrativos		{0,59}	{0,65}	{0,65}	{0,59}
[I8] Investigación		{0,59}	{0,65}	{0,65}	{0,59}
[I9] Datos económicos			{0,65}	{0,65}	{0,59}
[I10] Contratación		{0,59}	{0,65}	{0,65}	{0,59}
[I11] Patrimonio e inventario				{0,65}	{0,59}
[I12] Personal		{0,94}	{0,65}	{0,65}	{0,59}
[I13] Prevencion		{0,94}	{1,1}	{1,0}	{0,94}
[I14] Retribuciones		{0,94}	{1,1}	{1,0}	{0,94}
[I15] Actividades deportivas		{0,59}	{0,65}	{0,65}	{0,59}
[I16] Archivo		{0,59}	{0,65}	{0,65}	{0,59}
[I17] Registro		{0,94}	{1,1}	{1,0}	{0,94}
[I18] Documentación		{0,59}	{0,65}	{0,65}	{0,59}
[I19] Infraestructuras		{0,59}	{0,65}	{0,65}	{0,59}
[I20] Biblioteca		{0,59}	{0,65}	{0,65}	{0,59}
[I21] Almacen de datos			{0,65}	{0,65}	
[I22] Atención al usuario (CAU)		{0,59}	{0,65}	{0,65}	{0,59}
[I24] Material audiovisual y fotográfico		{0,59}	{0,65}	{0,65}	{0,59}
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	{0,88}				
[A1-S2] Soporte a las aulas multimedia.	{0,88}				
[A1-S3] Gestión del licenciamiento	{0,88}				
[A1-S4] Aula Virtual	{0,88}				
[A2-S1] Supercomputación	{0,88}				
[A2-S2] Consultoría	{0,64}				
[A3-S1] Gestión académica	{0,88}				
[A3-S2] Gestión económica y tesorería	{0,76}				
[A3-S3] Contratación y presupuestos	{0,88}				
[A3-S4] Gestión de RR.HH.	{0,52}				
[A3-S5] Extensión Universitaria	{0,52}				
[A3-S6] Archivo	{0,52}				
[A3-S7] Secretaria general	{0,88}				
[A3-S8] Gestión de infraestructuras	{0,52}				
[A3-S9] Servicio de bibliotecas	{0,52}				
[A3-S10] Comunicación	{0,52}				
[A3-S11] Calidad	{0,52}				
[A3-S12] Análisis de datos	{0,52}				
[A3-S13] Atención al usuario (CAU)	{0,52}				
[A3-S14] Gestión de publicaciones	{0,52}				
[A4-S1] Gestión del correo electrónico	{0,76}				
[A4-S2] Web institucional	{0,88}				
[A4-S3] Sede electrónica	{0,88}				
[A4-S4] Intranet	{0,52}				
[A4-S5] Portal del empleado	{0,52}				
[A4-S6] Secretaria virtual	{0,52}				
[A4-S7] Contenidos digitales	{0,52}				

Ilustración 16: Recomendaciones PILAR. Riesgo residual

En el Anexo III se muestran los resultados del análisis de riesgo completo sobre la universidad Exempli Gratia.

11. Declaración de aplicabilidad.

Una vez finalizado el análisis de riesgos, se tendrán identificados cuales de estos riesgos afectan a la información y a los servicios de la organización.

La herramienta PILAR disponible no permite (debido a la licencia) una vez obtenido el análisis de riesgos, realizar un análisis de insuficiencia o diferencial con una nueva situación objetivo deseada, ya sea para un objetivo de la organización o para las recomendaciones ofrecidas por la herramienta PILAR.

El resultado del análisis ofrecerá la información necesaria para realizar la Declaración de aplicabilidad de las 75 medidas del Anexo II del ENS, y deberá de ser completada, de forma motivada para cada medida, si aplica o no, y cómo se implementará dicha medida de seguridad. Esta implantación tendrá consecuencias en las condiciones y ámbito de negocio de la organización o bien permitirá mitigar los riesgos detectados en el Análisis de Riesgos.

Es importante destacar que el modelo no es rígido, ya que tenemos la posibilidad de elegir alternativas de seguridad, siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos afectados.

Se crea un documento tipo que pueda cumplir con la norma y que pueda ser utilizado por el producto del TFM.

El documento podrá tener una estructura similar a la siguiente:

Declaración de aplicabilidad del plan de adecuación al Esquema Nacional de Seguridad

- Nombre del declarante: Universidad Exempli Gratia
- Dirección postal: Plaza Mayor, 1
- Dirección electrónica: seguridad@exempligratia.es

De acuerdo con el artículo 41 del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la universidad Exempli Gratia declara que los sistemas de información que conforman su Sede Electrónica han sido analizados siguiendo los criterios establecidos en dicho Real Decreto y su modificación según el Real Decreto 951/2015 de 23 de Octubre, completando el plan de Adecuación al ENS.

Para el logro de este objetivo se ha definido un Sistema de Gestión de la Seguridad de la Información que desarrolla los procedimientos que permiten la adecuación al Esquema Nacional de Seguridad. Como consecuencia, la universidad Exempli Gratia ha puesto en marcha las medidas apropiadas para posibilitar la correcta protección de los datos y Sistemas que conforman su Sede Electrónica y ha diseñado controles permanentes de revisión de la eficacia de tales mecanismos de protección.

El presente documento de aplicabilidad es uno de los elementos que componen la adecuación al ENS y manifiesta la aplicabilidad de las medidas de seguridad.

Situación y aplicabilidad de las medidas de seguridad durante el año 2018. (Se muestra el ejemplo de una medida de seguridad):

Marco Organizativo. Org.4	**Proceso de autorización**
Medida de seguridad requerido	Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información: a) Utilización de instalaciones, habituales y alternativas. b) Entrada de equipos en producción, en particular, equipos que involucren criptografía. c) Entrada de aplicaciones en producción. d) Establecimiento de enlaces de comunicaciones con otros sistemas. e) Utilización de medios de comunicación, habituales y alternativos. f) Utilización de soportes de información. g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.

Aplicabilidad de la medida de seguridad	Aplica
Motivación de la medida de seguridad	Falta de control, falta de documentación específica, sin trazabilidad.
Implementación de la medida de seguridad	Creación de los procesos de autorización específicos para cada una de las áreas indicadas en la medida.

Marco XXX. ID XXX	**XXX**
Medida de seguridad requerido	XXX
Aplicabilidad de la medida de seguridad	Aplica/No aplica
Motivación de la medida de seguridad	XXX
Implementación de la medida de seguridad	XXX

En Valencia, a 4 de junio de 2018

Persona que lo firma: Francisco José Muñoz Torrijos
Cargo que ostenta: Responsable de la seguridad
Firma: ……..

12. Informe de insuficiencias (Gap Analysis).

Completada la declaración de aplicabilidad, las desviaciones al cumplimiento de las medidas de seguridad deberán recogerse en un documento, denominado informe de insuficiencias del sistema. Este informe, simplemente recoge la situación de cumplimiento de las medidas de seguridad (estado ideal vs situación actual). Este informe deberá de ser aprobado por los Responsables de la Información y de los Servicios.

Se tiene que recordar que no existe la seguridad absoluta en los sistemas de información, es por ello que los riesgos deben ser gestionados de forma objetiva. En algunos casos podrán ser incluso asumidos, en ese caso serán denominados riesgos residuales.

De igual manera que en el caso anterior, no se ha localizado en las guías una plantilla del documento, se crea un documento tipo que pueda ser utilizado por el producto del TFM.

El documento podrá tener una estructura similar a la siguiente:

Informe de insuficiencias del plan de adecuación al Esquema Nacional de Seguridad

- Nombre del declarante: Exempli Gratia
- Dirección postal: Plaza Mayor, 1
- Dirección electrónica: seguridad@exempligratia.es

De acuerdo con el artículo 41 del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la universidad Exempli Gratia declara que los sistemas de información que conforman su Sede Electrónica han sido analizados siguiendo los criterios establecidos en dicho Real Decreto y su modificación según el Real Decreto 951/2015 de 23 de Octubre, completando el plan de Adecuación al ENS.

Para el logro de este objetivo se ha definido un Sistema de Gestión de la Seguridad de la Información que desarrolla los procedimientos que permiten la adecuación al Esquema Nacional de Seguridad.

El presente informe de insuficiencias es uno de los elementos que componen la adecuación al ENS y manifiesta el estado de cumplimiento de las medidas de seguridad que son de aplicación a la organización según la categorización del sistema de información.

Durante el presente año 2018 han sido detectadas las siguientes insuficiencias:

Insuficiencia 1- **Procesos de autorización**	**Situación actual**	**Situación deseada**
Medida de seguridad	Existencia de procesos genéricos. Personal gestiona a discreción.	Creación de los procesos de autorización específicos para cada una de las áreas indicadas en la auditoria.
Aplicabilidad de la medida de seguridad	Aplicable	
Motivación de la medida de seguridad	Falta de control, falta de documentación específica, sin trazabilidad.	
Implementación de la medida de seguridad	2018	
Estado	Pendiente - Planificada - No corregida	

Insuficiencia 1- XXX	**XXX**	**XXX**
Medida de seguridad	XXX	XXX
Aplicabilidad de la medida de seguridad	Aplicable	
Motivación de la medida de seguridad	XXX	
Implementación de la medida de seguridad	No aplica	
Estado	No corregida	

Las insuficiencias no corregidas serán consideradas “riesgo asumible”

En Valencia, a 4 de junio de 2018

Responsable de información: Francisco José Muñoz Torrijos

Firma: ……..

Responsable del servicio: Francisco José Muñoz Torrijos

Firma: ……..

13. Plan de mejora de la seguridad, plazos de ejecución.

Una vez completados los puntos anteriores, el plan de mejora de la seguridad se establecerá para solucionar los riesgos puestos de manifiesto en el análisis de riesgos. Para ello se tendrán en cuenta los documentos vistos respecto de la aplicabilidad de las medidas de seguridad propuestas para mitigar esos riesgos identificados, y que permitan reducir la brecha existente (mostrada en el informe de insuficiencias), entre la situación actual de los sistemas de información y la situación indicada por el ENS o por la organización.

Para ello, el documento deberá de definir las tareas necesarias para subsanar las insuficiencias detectadas, indicando plazos y recursos asignados para su ejecución. Todo ello será recogido en el documento Plan de Mejora de la Seguridad.

Al igual que los casos anteriores, se genera un documento para utilizarlo en producto del TFM.

El documento podrá tener una estructura similar a la siguiente:

Plan de mejora de la seguridad del plan de adecuación al Esquema Nacional de Seguridad

- Nombre del declarante: Exempli Gratia
- Dirección postal: Plaza Mayor, 1
- Dirección electrónica: seguridad@exempligratia.es

De acuerdo con el artículo 41 del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la Exempli Gratia declara que los sistemas de información que conforman su Sede Electrónica han sido analizados siguiendo los criterios establecidos en dicho Real Decreto, completando el plan de Adecuación al ENS.

Para el logro de este objetivo se ha definido un Sistema de Gestión de la Seguridad de la Información que desarrolla los procedimientos que permiten la adecuación al Esquema Nacional de Seguridad.

Como consecuencia, la universidad Exempli Gratia ha puesto en marcha las medidas apropiadas para posibilitar la correcta protección de los datos y

Sistemas que conforman su Sede Electrónica y ha diseñado controles permanentes de revisión de la eficacia de tales mecanismos de protección.

El presente plan de mejora de la seguridad tiene por objeto definir las tareas necesarias para subsanar las insuficiencias detectadas en el sistema de información de la organización, indicando plazos y recursos asignados para su ejecución.

Durante el presente año 2018 se proponen las siguientes actuaciones con el objetivo de mejorar la seguridad de los sistemas de información:

Mejora 1	**Procesos de autorización**
Medida de seguridad	Creación de los procesos de autorización específicos para cada una de las áreas indicadas en la auditoria.
Motivación de la medida de seguridad	Falta de control, falta de documentación específica, sin trazabilidad.
Implementación de la medida de seguridad	2018
Estado	Planificada Junio
Responsable y desarrollo	Definir responsable del proceso. Creación de documentación de los procesos de autorización para cada una de las áreas afectadas.
Plazos	3 meses
Recursos	Personal de los servicios afectados

Mejora 1	**XXX**
Medida de seguridad	XXX
Motivación de la medida de seguridad	XXX
Implementación de la medida de seguridad	XXX
Estado	XXX
Desarrollo	XXX
Plazos	XXX
Recursos	XXX

En Valencia, a 4 de junio de 2018

Responsable de información: Francisco José Muñoz Torrijos

Firma: ……..

14. Conformidad con el ENS

Completados los puntos anteriores, se debe de redactar un documento de conformidad como indica el artículo 41 del ENS:

> *"Artículo 41. Publicación de conformidad.*
> *Los órganos y Entidades de Derecho Público darán publicidad en las*

correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad."

El documento podrá ser similar al siguiente:

Declaración de conformidad con el Esquema Nacional de Seguridad

- Nombre del declarante: Exempli Gratia
- Dirección postal: Plaza Mayor, 1
- Dirección electrónica: seguridad@exempligratia.es

De acuerdo con el artículo 41 del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), la universidad Exempli Gratia declara que los sistemas de información que conforman su Sede Electrónica han sido analizados siguiendo los criterios establecidos en dicho Real Decreto y su modificación según el Real Decreto 951/2015 de 23 de Octubre, completando el plan de Adecuación al ENS.

Para el logro de este objetivo se ha definido un Sistema de Gestión de la Seguridad de la Información que desarrolla los procedimientos que permiten la adecuación al Esquema Nacional de Seguridad. Como consecuencia, la universidad Exempli Gratia ha puesto en marcha las medidas apropiadas para posibilitar la correcta protección de los datos y Sistemas que conforman su Sede Electrónica y ha diseñado controles permanentes de revisión de la eficacia de tales mecanismos de protección.

La universidad Exempli Gratia se someterá a las auditorías periódicas para garantizar el cumplimiento del objetivo anterior actualizándose periódicamente según la normativa aplicable.

En Valencia, a 4 de junio de 2018

Persona que lo firma:	Francisco José Muñoz Torrijos
Cargo que ostenta:	Responsable de la seguridad
Firma:	……..

15. Herramienta Inés

Para concluir con las tareas de adecuación al ENS quedará pendiente la comunicación de los datos.

El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de la seguridad de los sistemas por parte de las Administraciones Públicas.

“Artículo 35. El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas".
Asimismo, el ENS dispone la necesidad de establecer un sistema de medición de la seguridad del sistema estableciendo un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

a) Grado de implantación de las medidas de seguridad.

b) Eficacia y eficiencia de las medidas de seguridad.

c) Impacto de los incidentes de seguridad.”

INES es la herramienta proporcionada por el Centro Criptológico Nacional (CCN) para la recogida de información y análisis de indicadores sobre el Informe Nacional del Estado de Seguridad que permite conocer el estado de implantación del Esquema Nacional de Seguridad (ENS) en las distintas Administraciones Públicas.

Para poder utilizar INES el usuario debe estar previamente registrado y autorizado a acceder al portal CCN-CERT (www.ccn-cert.cni.es), dado que la aplicación INES se encuentra situada dentro de dicho portal y es accesible solo para los usuarios registrados.

El Responsable de la Seguridad será el encargado de la interfaz con INES, proporcionando, validando y analizando la información de seguridad propia de su organismo y consolidada a nivel de Administración Pública.

16. Auditoría

Una vez realizado el plan de adecuación al ENS, la auditoria es la encargada de la verificación de que los procesos son realizados correctamente, este grado de cumplimiento será expresado de la siguiente forma:

- Completo (100%): Si todos los requisitos de la medida de seguridad están satisfechos.

- Alto (50%-99%): Si sólo la mitad de los requisitos de la medida de seguridad están satisfechos.

- Bajo (1%-49%): Si menos de la mitad de los requisitos de la medida de seguridad están satisfechos.

- Nulo (0%): Si ninguno de los requisitos de la medida de seguridad están satisfechos.

Indicar que la auditoria solo será necesaria en el caso de sistemas de categoría media o alta, los sistemas de categoría baja solo requieren de un ejercicio de autoevaluación.

Es de especial relevancia que las personas designadas para realizar la auditoria sigan el principio de “separación de funciones”, para evitar posibles conflictos de intereses.

Para realizar el análisis de la Universidad Exempli Gratia caso de estudio, se exigirá un nivel de madurez en las medidas de seguridad en proporción al nivel de las dimensiones afectadas o de la categoría del sistema vistas con anterioridad.

Como se ha indicado anteriormente, en el caso de estudio, tomaremos como referencia general una institución que se ha preocupado por adaptarse rápidamente tanto a los cambios tecnológicos en constante evolución como a la normativa vigente. Sin embargo, para poder tratar todas las áreas de análisis y analizar toda la casuística posible, se trabajará con la deficiencia detectada en fases anteriores y que dará como resultado no conformidades que deberán de ser analizadas y resueltas.

Aunque no figura en las guías STIC, dado lo extenso del proceso de auditoría, se propone el siguiente resumen de auditoria de la universidad Exempli Gratia, donde se puede observar rápidamente el resultado del grado de cumplimiento.

AUDITORIA DE SEGURIDAD DE LA UNIVERSIDAD “EXEMPLI GRATIA”

MARCO	ID	MEDIDAS DE SEGURIDAD/ARTICULO	GRADO	OBSERVACIONES
Organizativo	**org.1**	Política de seguridad	Completo	-
	org.2	Normativa de seguridad	Alto	-
	org.3	Procedimientos de seguridad	Alto	-
	org.4	Proceso de autorización	Bajo	NC.org.4
Operacional	**op.pl**	Planificación		
	op.pl.1	Análisis de riesgos	Alto	-
	op.pl2	Arquitectura de seguridad	Alto	-
	op.pl3	Adquisición de nuevos componentes	Alto	-
	op.pl4	Dimensionamiento / Gestión de capacidades	Alto	-
	op.pl5	Componentes certificados	Alto	-
	op.acc	Control de acceso		
	op.acc.1	Identificación	Alto	-
	op.acc.2	Requisitos de acceso	Alto	-
	op.acc.3	Segregación de funciones y tareas	Alto	-
	op.acc.4	Proceso de gestión de derechos de acceso	Alto	-
	op.acc.5	Mecanismo de autenticación	Alto	-
	op.acc.6	Acceso local (local login)	Alto	-
	op.acc.7	Acceso remoto (remote login)	Alto	-
	op.exp	Explotación		

	op.exp.1	Inventario de activos	Alto	-
	op.exp.2	Configuración de seguridad	Alto	-
	op.exp.3	Gestión de la configuración	Alto	-
	op.exp.4	Mantenimiento	Alto	-
	op.exp.5	Gestión de cambios	Alto	-
	op.exp.6	Protección frente a código dañino	Alto	-
	op.exp.7	Gestión de incidencias	Alto	-
	op.exp.8	Registro de la actividad de los usuarios	Alto	-
	op.exp.9	Registro de la gestión de incidencias	Alto	-
	op.exp.10	Protección de los registros de actividad	Alto	-
	op.exp.11	Protección de claves criptográficas	Alto	-
	op.ext	Servicios externos		
	op.ext.1	Contratación y acuerdos de nivel de servicio	Alto	-
	op.ext.2	Gestión diaria	Alto	-
	op.ext.9	Medios alternativos	Alto	-
	op.mon	Monitorización del sistema	Alto	-
	op.mon.1	Detección de intrusión	Alto	-
	op.mon.2	Sistema de métricas	Alto	-
Medidas de protección	**mp.if**	Medidas de Protección		
	mp.if.1	Áreas separadas y con control de acceso	Alto	-
	mp.if.2	Identificación de las personas	Alto	-
	mp.if.3	Acondicionamiento de los locales	Alto	-
	mp.if.4	Energía eléctrica	Alto	-
	mp.if.5	Protección frente a incendios	Alto	-
	mp.if.6	Protección contra inundaciones	Alto	-
	mp.if.7	Registro de entrada y salida de equipamiento	Alto	-
	mp.if.9	Instalaciones alternativas	Alto	-
	mp.per	Gestión del personal		
	mp.per.1	Caracterización del lugar de trabajo	Alto	-
	mp.per.2	Deberes y obligaciones	Alto	-
	mp.per.3	Concienciación	Alto	-
	mp.per.4	Formación	Alto	-
	mp.per.9	Personal alternativo	Alto	-
	mp.eq	Protección de los equipos		
	mp.eq.1	Lugar de trabajo ordenado	Alto	-
	mp.eq.2	Bloqueo de puesto de trabajo	Alto	-
	mp.eq.3	Protección de equipos portátiles	Alto	-
	mp.eq.9	Medios alternativos	Alto	-
	mp.com	Protección de las comunicaciones	Alto	-
	mp.com.1	Perímetro seguro	Alto	-
	mp.com.2	Protección de la confidencialidad	Alto	-
	mp.com.3	Protección de la autenticidad y de la integridad	Alto	-
	mp.com.4	Segregación de redes	Alto	-
	mp.com.9	Medios alternativos	Alto	-
	mp.si	Protección de los soportes de información		
	mp.si.1	Etiquetado	Alto	-
	mp.si.2	Criptografía	Alto	-

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

Ilustración 17: Auditoria de seguridad de la universidad Exempli Gratia

Como se observa en el análisis, en el Proceso de Autorización existe una no conformidad expresada por la tarea de auditoria. El auditor deberá de indicar tanto la no conformidad como la recomendación para la subsanación del problema.

Se procede al análisis que da como resultado la no conformidad indicada en observaciones respecto al marco organizativo, org.4, respecto de la medida de seguridad del proceso de autorización.

Para comenzar se revisa la guía STIC 804 sobre las medidas de implantación del ENS donde se puede ver el detalle del Proceso de Autorización:

[ORG.4] PROCESO DE AUTORIZACIÓN

48. Ningún sistema de información con responsabilidades sobre la información que maneja o los servicios que presta debería admitir elementos no autorizados por cuanto la libre incorporación de elementos socavaría de raíz la confianza en el sistema, al modificar la superficie de ataque y dar pie a nuevas vulnerabilidades susceptibles de ser explotadas.

49. El ENS singulariza una serie de elementos, sin perjuicio de que se aplique siempre la regla de 'se requiere autorización previa' con carácter general a todos los componentes durante todo su ciclo de vida:

a. Utilización de instalaciones, habituales y alternativas.
b. Entrada de equipos en producción, en particular, equipos que involucren criptografía.
c. Entrada de aplicaciones en producción.
d. Establecimiento de enlaces de comunicaciones con otros sistemas.
e. Utilización de medios de comunicación, habituales y alternativos.
f. Utilización de soportes de información.

g. Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA3, u otros de naturaleza análoga.
h. Utilización de servicios de terceros, bajo contrato o Convenio.
i. Utilización de equipos propiedad del usuario (BYOD – Bring Your Own Device).

50. El proceso de autorización requiere:

- que esté definido en la normativa de seguridad la persona o punto de contacto para autorizar un determinado componente o actuación,
- que exista un mecanismo (por ejemplo, un formulario) para solicitar la autorización, indicando lo que se desea y la motivación; esta solicitud deberá incorporar los siguientes elementos:

- *descripción precisa del elemento o actuación para el que se solicita autorización,*
- *descripción precisa de las actividades para las que se requiere el nuevo componente,*
- *justificación de que nuevo componente no afecta a otras funcionalidades del sistema,*
- *si el nuevo componente introduce posibles vulnerabilidades (es decir, si expone al sistema a nuevas o renovadas amenazas), deberá anexarse un análisis de riesgos y las medidas que se toman para gestionarlo; este análisis de riesgos tendrá la intensidad proporcionada a la categoría del sistema, como se establece en [op.pl.1],*
- *justificación de que no se viola ninguna normativa de seguridad, o información de los procedimientos de seguridad que son aplicables al caso o, si fuere necesario, la necesidad de desarrollar algún nuevo procedimiento específico*

- que se requiera la aprobación formal de la petición (o sea, la firma del responsable) antes de la actuación

Esto será trasladado para el caso de estudio a una tabla tal como se indica en la guía STIC 808 de verificación del cumplimiento de las medidas de seguridad del ENS para una rápida visualización mediante checks de su estado:

Proceso de autorización:

Org.4	**Basica D, A, I, C, T**	X.- ¿Existe un proceso formal para las autorizaciones respecto a los sistemas de información? *Evidencia: La normativa de seguridad contempla, para cada tipo de componente o actuación, la persona o punto de contacto para su autorización.* *Existe un modelo de solicitud (formulario) que contiene: Descripción del elemento (componente) o actuación para la que se solicita la autorización, las actividades para las que se requiere el nuevo componente (motivación), el tiempo para el que se solicita la autorización (que puede ser temporal o permanente), justificación de que no afecta a otras funcionalidades del sistema, un análisis de riesgo conforme a la categoría del sistema (si el nuevo componente introduce posibles vulnerabilidades), justificación de que no viola ninguna normativa de seguridad, información de los procedimientos que son de aplicación así como de la necesidad de desarrollar nuevos si fuese necesario.* *A continuación se exponen los elementos sobre los cuales debe existir un proceso de autorización.* Respecto a dicho proceso de autorización: □ 1.1.- ¿Cubre la utilización de instalaciones, tanto habituales como alternativas? *Evidencia: La normativa contempla el proceso de autorización de utilización de instalaciones (p.ej: acceso al CPD, uso de un local alternativo para los servidores de respaldo ante desastres, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario*	Aplica: X Si □ No Lo audito: X Si □ No	Registros: X Documento: □ Muestreo: Observaciones: Existe documento general, la organización carece de documentos específicos o áreas de aplicación. Nivel de Cumplimiento: Bajo

		de solicitud y de que estos recursos han sido autorizados por el responsable pertinente antes de su entrada en explotación. □ 1.2.- ¿Cubre la entrada de equipos en producción, en particular, equipos que involucren criptografía? *Evidencia: La normativa contempla el proceso de autorización de entrada de equipos en producción, que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.3.- ¿Cubre la entrada de aplicaciones en producción? *Evidencia: La normativa contempla el proceso de autorización de entrada de aplicaciones en producción (p.ej: actualización de parches en el sistema operativo, instalación de nuevas aplicaciones, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.4.- ¿Cubre el establecimiento de enlaces de comunicaciones con otros sistemas? *Evidencia: La normativa contempla el proceso de autorización de enlaces de comunicaciones con otros sistemas (p.ej: para el intercambio de expedientes entre un organismo y otro), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.5.- ¿Cubre la utilización de medios de comunicación (tanto habituales como alternativos)? *Evidencia: La normativa contempla el proceso de autorización de utilización de medios de comunicación (p.ej: uso de una línea de datos para el acceso a Internet), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.6.- ¿Cubre la utilización de soportes de información? *Evidencia: La normativa contempla el proceso de autorización de utilización de soportes de información (p.ej: cintas de backup, DVD, memorias USB, etc.), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.7.- ¿Cubre la utilización de equipos móviles? *Evidencia: La normativa contempla el proceso de autorización de utilización de equipos móviles (p.ej: ordenadores portátiles, PDA u otros de naturaleza análoga), que cubre los requisitos antes indicados. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* □ 1.8.- ¿Ha sido difundido, así como cualquier actualización de los mismos, entre el personal afectado? *Evidencia: La normativa contempla el proceso de difusión, entre el personal afectado, de las nuevas versiones de los procesos de autorización, así como la persona responsable de ello. Existe evidencia documental del formulario de solicitud y de que estos recursos han sido autorizados por el responsable antes de su entrada en explotación.* *Consultar guías:* ***CCN-STIC-002*** *Coordinación criptológica* ***CCN-STIC-302*** *Interconexión de sistemas de las tecnologías de la información* *y las comunicaciones que manejan información nacional clasificada en la* *administración* ***Criterios de seguridad*** *Capítulo 13*		

Ilustración 18: Verificación del cumplimiento medidas de seguridad

Este será el análisis que deberá de realizarse para cada una de las 75 medidas de seguridad como muestra la tabla inicial de forma resumida.

Las no conformidades deben de ser expresadas con una posible recomendación que permita su cumplimiento.

RESULTADOS DE LA AUDITORIA DE SEGURIDAD DE LA UNIVERSIDAD "EXEMPLI GRATIA"

NO CONFORMIDAD	RECOMENDACION
NC.org.4	Creación de los procesos de autorización específicos para cada una de las áreas indicadas en la auditoria.

La auditoría finalizará con un resultado favorable o desfavorable similar al siguiente:

Opinión del auditor:	**FAVORABLE CON SALVEDADES**

17. Conclusiones

Considero una vez concluido finalizada la memoria, que no es un trabajo trivial la adaptación al ENS de una administración pública, tanto la propia adaptación al ENS como su mantenimiento en el tiempo.

Son muchos los componentes y variables manejadas si se pretende realizar un buen trabajo, ya que se deben de tomar en cuenta tanto aspectos normativos que son de aplicación, como la propia adecuación de la organización por su idiosincrasia y funcionamiento interno. A eso se le añade la dificultad debida a lo heterogéneo de los entornos debido a su crecimiento histórico, siendo distintos en cada organización.

Al margen del presente proyecto de adaptación al ENS se deberá de tener en cuenta la cohesión con toda la normativa y puesta en marcha funcional de otros ámbitos como el nuevo Reglamento general de Protección de datos (RGPD) o el Esquema Nacional de Interoperabilidad, esto puede obligar a un mayor trabajo inicial, y por otro lado permitir la optimización de los recursos y reutilización de parte del trabajo realizado.

En el apartado de lecciones aprendidas, he pecado de ponerme a redactar previamente a contar con toda la información disponible, como por ejemplo, el descubrimiento del anexo de universidades una vez tenía iniciada la memoria, teniendo que rehacer parte del trabajo realizado.

Con el proyecto he podido observar que al igual que la adaptación al ENS, la memoria ha resultado un proceso de mejora continua y que la mejor forma de abordarlo es "ponerse a andar" cuanto antes, eso sí, con unos conocimientos sobre la materia, un guion y unos objetivos definidos.

Inicialmente he abordado el proyecto con los conocimientos adquiridos tanto en el Master como en mi actividad laboral en las áreas de jefatura de proyecto, preventa y coordinación, tratando de aprovechar las distintas certificaciones en gestión de proyectos y servicios para darle un enfoque de proyecto, pero a medida que iba avanzando, reducía estas áreas al descubrir el gran Trabajo que está realizando el CCN con las Guías STIC de la serie 800 para facilitar esta adaptación y su normalización.

Pese a ello, también he descubierto determinadas necesidades no cubiertas especialmente respecto a plantillas de documentos generales y obligatorios que deberían de normalizarse para un uso general en las Administraciones Públicas.

He tenido la oportunidad en el trabajo de hablar con personal de distintas administraciones públicas con implicaciones directas o indirectas en la adecuación al ENS y he observado existen tantas aproximaciones y puntos de vista distintos respecto al proceso de adecuación como administraciones públicas, por un lado respecto a la documentación a generar por lo sujeto a interpretación de los contenidos y por otro, del tratamiento de la información y de los servicios, especialmente en el Análisis de riesgos con PILAR, debido a las distintas perspectivas para afrontarlo.

No obstante, una vez analizado lo denso de algunas de las guías, la relación entre algunas de ellas y la inexistencia de relación entre otras, pienso que en el caso de organizaciones pequeñas y con pocos recursos una guía de este estilo puede resultar de utilidad, tratando de simplificar y reducir el trabajo para su cumplimiento. En el producto se indicará en que guía figura la información para la ampliación de información de cada área si fuera necesario.

En cuanto a la planificación ofrecida inicialmente no ha sido seguida como sería deseable ni como acostumbro a hacer normalmente, debido a temas laborales, aunque pienso que no estaba mal dimensionada inicialmente, tras su revisión una vez finalizado el trabajo.

Respecto a las metas planteadas, en mi opinión se han cumplido, tras toda la fase de análisis y la elaboración de la memoria respecto del caso de estudio, se ha podido entregar un producto en forma de guía de adecuación al ENS como inicialmente estaba marcado.

Adicionalmente se ha cumplido con todos los objetivos secundarios que se planteaban al inicio del proyecto con la definición del marco normativo, el planteamiento del caso de estudio de la universidad Exempli Gratia, revisando todas las necesidades, requerimientos sobre el ENS, el trabajo realizado por el CCN con las guías STIC de la serie 800 y la entrega de la guía de adecuación como producto resultante de la memoria.

Aunque todo está siempre sujeto a mejora, estoy satisfecho con el trabajo realizado, creo que he podido crear un hilo conductor coherente para el lector, algo marcado personalmente como una meta tras el análisis de la ingente cantidad de información proporcionada por el CCN. A mi juicio, la

documentación esta falta de una imagen global para ubicarse al comienzo del proyecto y que permita actuar como referencia, estableciendo las necesidades y vínculos con las distintas guías, procedimientos, software y normativa.

Como trabajo futuro que podría ser interesante y con relación directa con el Esquema Nacional de Seguridad podrían estar la sustitución de LOPD por RGPD, el Esquema Nacional de Interoperabilidad o la normativa ISO 27000.

18. Glosario

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.

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditoría de la seguridad.

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad.

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema.

Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Centro Criptológico Nacional - CCN.

Es un organismo del estado español anexionado al Centro Nacional de Inteligencia que se dedica a criptoanalizar y descifrar por procedimientros manuales, medios electrónicos y criptofonía, así como realizar investigaciones tecnológico-criptográficas y formar al personal especializado en criptología. El CCN quedó legalmente regulado por el Real Decreto 421/2004 el 12 de marzo.

Confidencialidad.

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Disponibilidad.

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Firma electrónica.

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes.

Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos.

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Guías CCN-STIC

Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones.

Incidente de seguridad.

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Información

Caso concreto de un cierto tipo de información.

Integridad.

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Medidas de seguridad.

Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

Principios básicos de seguridad.

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso.

Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Proceso de seguridad.

Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

Requisitos mínimos de seguridad.

Exigencias necesarias para asegurar la información y los servicios. Riesgo. Estimación del grado de exposición a que una amenaza se

materialice sobre uno o más activos causando daños o perjuicios a la organización.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Seguridad de las redes y de la información

Es 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.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Servicios acreditados.

Servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación

Sistema de gestión de la seguridad de la información (SGSI).

Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de

planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. ENS.

Trazabilidad

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad.

Una debilidad que puede ser aprovechada por una amenaza.

19. Bibliografía

BOE. Real Decreto 4/2020, de 8 de enero, por lo que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. [Consulta realizada 20 de febrero de 2018]
https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330

BOE. Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. [Consulta realizada 20 de febrero de 2018]
https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881

BOE. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. [Consulta realizada 21 de febrero de 2018]
https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

BOE. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. [Consulta realizada 21 de febrero de 2018].
https://www.boe.es/buscar/act.php?id=BOE-A-2007-12352

BOE. Ley 9/1968, de 5 de abril, sobre secretos oficiales. [Consulta realizada 4 abril de 2018].
https://www.boe.es/buscar/doc.php?id=BOE-A-1968-444

Diario oficial de la Unión Europea. Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016. [Consulta realizada 25 de febrero de 2018]
https://www.boe.es/doue/2016/119/L00001-00088.pdf

CCN. Esquema Nacional de Seguridad. Valoración de los sistemas en el ENS [Consulta realizada 28 de febrero de 2018].
https://www.ccn-cert.cni.es/ens.html

CCN. Guía de seguridad (CCN-STIC 803) Esquema Nacional de Seguridad. Valoración de los sistemas en el ENS [Consulta realizada 28 de febrero de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html

CCN. Guía de seguridad (CCN-STIC 809) Esquema Nacional de Seguridad. Declaración de conformidad con el ENS [Consulta realizada 28 de febrero de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1279-ccn-stic-809-declaracion-de-conformidad-con-el-ens/file.html

CCN. Guía de seguridad (CCN-STIC 824) Esquema Nacional de Seguridad. Información del Estado de Seguridad [Consulta realizada 28 de febrero de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/542-ccn-stic-824-informaci%C3%B3n-del-estado-de-seguridad/file.html

CCN. Guía de seguridad (CCN-STIC 844) Esquema Nacional de Seguridad. Manual de usuario de INES [Consulta realizada 1 de marzo de febrero de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1063-ccn-stic-844-manual-de-usuario-de-ines/file.html

CCN. Guía de seguridad (CCN-STIC 804) Esquema Nacional de Seguridad. Guía de implantación [Consulta realizada 1 de marzo de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

CCN. Guía de seguridad (CCN-STIC 808) Esquema Nacional de Seguridad. Verificación del cumplimiento de las medidas en el ENS. [Consulta realizada 1 de marzo de 2018].
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

CCN. Guía de seguridad (CCN-STIC 802) Esquema Nacional de Seguridad. Auditoría del ENS. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html

CCN. Guía de seguridad (CCN-STIC 815) Esquema Nacional de Seguridad. Indicadores y métricas en el ENS. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html

CCN. Guía de seguridad (CCN-STIC 815) Esquema Nacional de Seguridad. Indicadores y métricas en el ENS. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/525-ccn-stic-815-indicadores-y-metricas-en-el-ens/file.html

CCN. Guía de seguridad (CCN-STIC 805) Esquema Nacional de Seguridad. Política de Seguridad de la Información. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html

CCN. Guía de seguridad (CCN-STIC 805) Esquema Nacional de Seguridad. Responsabilidades y Funciones en el ENS. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

CCN. Guía de seguridad (CCN-STIC 805) Esquema Nacional de Seguridad. Plan de Adecuación al ENS. [Consulta realizada 2 de marzo de 2018]. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/511-ccn-stic-806-plan-de-adecuacion-al-ens/file.html

CCN. Herramienta Pilar. [Consulta realizada 4 de abril de 2018]. https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar.html

Universidad de Valladolid. Política de seguridad. [Consulta realizada 2 de marzo de 2018]. http://www.uva.es/export/sites/uva/1.lauva/1.04.secretariageneral/_documentos/II.14.-Politica-Seguridad-UVa.pdf

Universidad Autónoma de Madrid. Política de seguridad. [Consulta realizada 2 de marzo de 2018]. http://www.uam.es/ss/Satellite/BOUAM/es/1234892145844/1242689930179/BOUAM_Boletin_FA/detalle/1242689930179.htm

Universidad de Castilla-La Mancha. Política de seguridad. [Consulta realizada 2 de marzo de 2018]. https://e.uclm.es/servicios/doc/?id=UCLMDOCID-12-1880

Universidad de Valencia. Política de seguridad. [Consulta realizada 2 de marzo de 2018]. https://www.uv.es/sgeneral/Reglamentacio/Doc/Adm_Electronica/Y10.pdf

20. Anexo I – Política de seguridad

POLITICA DE SEGURIDAD UNIVERSIDAD EXEMPLI GRATIA

1. APROBACION Y ENTRADA EN VIGOR

Texto aprobado el día 5 de Mayo de 2018 en consejo de Gobierno ACGUEG 1/2018.

Esta política de seguridad es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCION

Se elabora en cumplimiento de la exigencia del Real Decreto 3/2010, de 8 de enero, por el que se regula el esquema nacional de seguridad (ENS) en el ámbito de la administración electrónica que, en el artículo 11, establece la obligación para las administraciones públicas de disponer de una política de seguridad e indica los requisitos mínimos que debe cumplir. Esta política de seguridad sigue también las indicaciones de la guía CCNSTIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, consagra el derecho de los ciudadanos a comunicarse con las administraciones por medios electrónicos. La finalidad del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, por medio de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y en las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La adaptación al ENS implica que la Universidad Exempli Gratia y su personal deben aplicar las medidas mínimas de seguridad exigidas por la

ENS y realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes unidades de gestión de la Universidad deberán cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema de tramitación electrónica, desde la concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y los costes asociados deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

Las unidades de gestión de la Universidad Exempli Gratia deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 7 de la ENS.

2.1. PREVENCION

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se puede degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán

mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

    - Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

    - Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

La organización aplicará esta política de seguridad en aquellos sistemas de información que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

La política de seguridad es aplicable sobre los siguientes sistemas de información TIC y los servicios que los conforman:

Área Docente

- Soporte a las aulas informáticas de libre acceso y de docencia.

    El servicio requiere de la Instalación y configuración de equipos así como el software utilizado en aulas de uso docente y ubicaciones de acceso libre

- Soporte a las aulas multimedia.

    Este servicio incluye la instalación y configuración de equipos y Software además de contar con equipamiento audiovisual como pizarras y proyectores.

- Gestión de licenciamiento.

  El servicio gestiona la Adquisición y validación centralizada de licencias de software de uso docente

- Aula Virtual

  Este servicio cubre las necesidades de la docencia en accesos Web, áreas de compartición de ficheros, contenidos multimedia y acceso a la mensajería entre docentes y alumnado en las Aulas incluyendo la realización de pruebas y exámenes.

Área de investigación

- Supercomputación

  Gestión de los recursos de altas prestaciones para el cálculo y procesamiento de datos científicos.

- Consultoría

  Servicios de consultoría con soporte al despliegue de aplicaciones y servicios especializados de alto rendimiento, conectividad de infraestructuras, licenciamiento de los productos, gestión del soporte técnico especializado orientado a la investigación.

Área de Gestión

- Gestión Académica

  Gestiona la actividad académica de los estudiantes universitarios, incluye Grados, Postgrados, Actas, Auto-matriculas, Becas, y todo lo referente a titulaciones (horarios, secretarias, practicas, etc.) tanto oficiales homologados por ANECA como propias.

- Gestión económica y tesorería

  Aplicaciones para la gestión económica de la Universidad, incluyendo donaciones de cualquier organización, la gestión de Fondos de financiación europea, gestión de las tasas universitarias y cualquier otro ingreso.

- Contratación y presupuestos

  Se encarga de la gestión de los contratos que establece la Universidad con terceros y la gestión de los presupuestos

- Tesorería

  Se encarga de la gestión

- Gestión de RR.HH.

  Realiza la gestión de los procedimientos relacionados con los Recursos Humanos en la Universidad, relación de puestos de trabajo, plantilla, control horario, convocatorias de acceso, procesos de formación, revisiones médicas, retribuciones al personal, etc.

- Extensión Universitaria

  Gestión de todas las actividades y procesos gestionados por el Servicio de Deportes, alquiler de viviendas, enseñanzas no regladas, etc.

- Archivo.

  Gestión y mantenimiento del Archivo universitario en los diferentes soportes como documentos, fichas, DVD, negativos y positivos fotográficos, cuadernos, películas o impresos.

- Secretaria General.

  Gestión de todos los procesos pertenecientes a la institución, actos protocolarios, registro universitario (presencial y telemático), gestión documental, convenios, normativa universitaria y procesos electorales.

- Gestión de infraestructuras

  Aplicaciones de gestión de infraestructuras, control de acceso a edificios, aparcamientos, zonas deportivas, gestión de almacenes, pedidos y materiales, gestión de los riesgos laborales asociados a las instalaciones universitarias, gestión de espacios.

- Servicio de bibliotecas

  Gestión de los procesos soportados por bibliotecas y repositorio institucional.

- Comunicación

  Gestión de la televisión universitaria, prensa universitaria, cartelería digital, eventos, congresos.

- Calidad

  Gestión de los recursos y aplicaciones para la gestión de la calidad, generación, difusión y evaluación de las encuestas destinadas a la comunidad educativa, evaluación del profesorado, evaluaciones y autoevaluaciones de la calidad.

- Análisis de datos

  Aplicaciones de análisis de datos e información institucional (Datawarehouse).

- Atención al usuario (CAU)

  Aplicaciones para la gestión de peticiones e incidencias.

- Gestión de publicaciones

  Gestión de los procesos de publicaciones de la Universidad.

Área de correo, herramientas colaborativas y publicación Web.

- Gestión del correo electrónico

  Gestión de correo electrónico institucional PDI/PAS, alumnado, pre alumnado y egresado, listas de distribución, notificaciones SMS, redes sociales, espacios colaborativos, servicios FTP y servicios de videoconferencia.

- Web institucional.

  Sitio web de información académica, investigación y servicios universitarios

- Sede electrónica

  Acceso electrónico de los ciudadanos a los Servicios Públicos según lo establecido en la Ley 11/2007 de 22 de Junio.

- Intranet.

  Publicación de información académica de investigación y servicios universitarios de acceso restringido a la comunidad universitaria incluyendo el colectivo investigador.

- Portal del empleado

  Recursos y servicios dirigidos a los empleados de acceso restringido a este colectivo.

- Secretaria Virtual

  Recursos y servicios dirigidos a los estudiantes de la universidad sobre un sitio web de acceso restringido al colectivo.

- Contenidos digitales

Soporte a la generación, almacenamiento y difusión de material audiovisual y soporte a la elaboración, creación y difusión de contenidos para uso docente.

Soporte y equipamiento del puesto de Trabajo

- Servicio integral Workplace

  Soporte y equipamiento del puesto de Trabajo (renovación del parque informatico adecuado al puesto), mantenimiento software corporativo, servicios de impresión y asesoramiento técnico. Tareas de alto nivel no asignadas bajo incidencia o petición al servicio del CAU.

Servicio de Comunicaciones

- Servicio de telefonía fija, móvil y fax
  Diseño, administración y gestión de las comunicaciones de voz basadas en el uso de terminales fijos, móviles y fax.

- Servicio de red cableada, inalámbrica

  Diseño, administración y gestión de las comunicaciones soportadas sobre la red de cableado estructurado y red inalámbrica de la universidad, así como los accesos VPN.

Gestión de identidades

- Servicios de directorio

  Diseño, administración y gestión de la plataforma que almacena, organiza y publica información de contacto sobre los usuarios de la Universidad, gestión de Active Directory, OpenLdap y gestión de la Infraestructura de clave pública (PKI) de la universidad para la emisión de certificados digitales a sus usuarios.

4. MISION

Tal y como se refleja en sus Estatutos, la Universidad Exempli Gratia, como servicio público que es, tiene por misión impartir las enseñanzas necesarias para la formación de los estudiantes, la preparación para el ejercicio de actividades profesionales o artísticas y la obtención, en su caso, de los títulos académicos correspondientes, así como para la actualización permanente del conocimiento y de la formación de su personal y del profesorado de todos los niveles de enseñanza.

La Universidad Exempli Gratia fomenta la investigación, tanto básica como aplicada, y el desarrollo científico y tecnológico. Asimismo, con las garantías

de racionalidad y universalidad que le son propias, es una institución difusora de cultura en el seno de la sociedad.

La Universidad Exempli Gratia facilita, estimula y acoge las actividades intelectuales y críticas en todos los campos de la cultura y del conocimiento.

En el cumplimiento de todas estas funciones, la Universidad Exempli Gratia tiene presente la armonía los saberes, originados en el desarrollo del pensamiento humano y destinado al perfeccionamiento de las personas y de su convivencia en una sociedad plural y democrática.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifiesta la necesidad de una infraestructura TIC que prevalezca y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio a los usuarios, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

5. MARCO NORMATIVO

En el desarrollo y la implementación de esta política se tendrán en cuenta los Estatutos de la Universidad Exempli Gratia y las sedes normativas de desarrollo relacionadas con sus objetivos.

6. ORGANIZACIÓN DE LA SEGURIDAD

La gestión de la seguridad de la información en la Universidad Exempli Gratia estará organizada de acuerdo a la siguiente estructura:

- Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática, como unidad consultiva dependiente del Consejo de Gobierno.

- Comité de Seguridad de la Información.

- El Responsable de la Información.

- El Responsable de los Servicios.

- El Responsable del Sistema de Información.

- El Responsable de la Seguridad.

6.1. Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática

Entre las funciones de la Comisión de Tecnología de la Información y las Comunicaciones y de Seguridad Informática se encuentran:

- Aprobación previa de la Política de Seguridad antes de ser sometida a la aprobación definitiva por el Consejo de Gobierno.

- Aprobación de la normativa de seguridad.

- Divulgación de la política y normativa de seguridad.

- Aprobación de las iniciativas y de los objetivos estratégicos en seguridad de las TIC.

6.2. El Comité de Seguridad de la Información

Se crea el Comité de Seguridad de la Información, que estará formado por:

- El Secretario General, o vicerrector que ostente las competencias en materia de los sistemas de información, que será su presidente

- Un vicerrector designado por el rector

- El responsable de los Servicios

- El responsable del Sistema

- El responsable de la Seguridad, que actuará como secretario

Serán funciones propias de este Comité:

- Revisión anual de la política de seguridad.

- Desarrollo del procedimiento de designación de roles.

- Designación de roles y responsabilidades.

- Supervisión y aprobación de las tareas de seguimiento del ENS:

    a) Tareas de adecuación

    b) Análisis de riesgos

    c) Auditoría bienal

- Velar por el cumplimiento de la política de seguridad.

- Velar por el cumplimiento de las normativas en materia de seguridad.

- Definición y seguimiento de las iniciativas y los objetivos estratégicos en seguridad de las TIC.

- Fijar las condiciones para satisfacer los requisitos de seguridad de la información.

- Aprobar los procedimientos de seguridad.

- Velar por la disponibilidad de los recursos necesarios para desarrollar las iniciativas y objetivos estratégicos de seguridad necesarios.

- Impulsar la elaboración de directrices en materia de seguridad de la información.

- Promover la formación y concienciación en materia de seguridad de la información.

- Asesorar a la Comisión TIC y de Seguridad Informática en todo lo que solicite e informarle sobre el estado de la seguridad.

6.3. El Responsable de la Información

El Responsable de la Información será el Secretario General de la Universidad o vicerrector competente en materia de sistemas de información, que tendrá las siguientes funciones y responsabilidades:

- Establecimiento de los requisitos de seguridad que garanticen el tratamiento de la información.

- Trabajo en colaboración con el Responsable de Seguridad y el Responsable del Sistema en la valoración de la información en las diferentes dimensiones de seguridad y el mantenimiento de los sistemas catalogados según el Anexo I del ENS.

- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y por su cumplimiento.

6.4. El Responsable de los Servicios

El Responsable de los Servicios será el Gerente, que tendrá las siguientes funciones y responsabilidades:

- Establecimiento de los requisitos de los servicios prestados a través de medios electrónicos en materia de seguridad.

- Trabajo en colaboración con el Responsable de Seguridad y el Responsable del Sistema en la valoración de los servicios en las diferentes dimensiones de seguridad y el mantenimiento de los sistemas catalogados según el Anexo I del ENS.

6.5. El Responsable del Sistema de información

El Responsable del Sistema será el director del Área de Tecnología y Comunicaciones, que tendrá las siguientes funciones y responsabilidades:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.

- Además, puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con el Responsable de la Información, el Responsable del Servicio y el Responsable de Seguridad, antes de ser ejecutada.

6.6. El Responsable de la seguridad

El Responsable de Seguridad, que será designado por el Rector, tendrá las siguientes funciones y responsabilidades:

- Mantener la seguridad de la información manejada y de los servicios prestados siguiendo las directrices marcadas por el Comité de Seguridad de la Información y de acuerdo a lo establecido en la Política de Seguridad.

- Promover la formación y concienciación en materia de seguridad siguiendo las directrices marcadas por el Comité de Seguridad de la Información.

- Elaborar las propuestas de modificación y actualización de la política de seguridad de la información.

- Promover para su aprobación y seguimiento en el Comité de Seguridad de la Información las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.

- Desarrollar la política de seguridad de la información mediante la elaboración de la normativa de seguridad.

- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.

- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

- Proponer para su aprobación y seguimiento en el Comité de Seguridad de la Información, las líneas de actuación en materia de seguridad de la información.

7. DATOS DE CARÁCTER PERSONAL

La Universidad Exempli Gratia trata datos de carácter personal. Los documentos de seguridad de los distintos sistemas, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de la Universidad Exempli Gratia se ajustarán al Reglamento General de Protección de Datos (RGPD) para el tratamiento de los datos de carácter personal recogidos en el mencionado <Documento de Seguridad>.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta política de seguridad han de llevar a cabo un análisis de riesgos, en la que se evaluarán las amenazas y los riesgos a que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez cada dos años.

- Cuando cambie la información manejada.

- Cuando cambian los servicios prestados.

- Cuando tenga lugar un incidente grave de seguridad.

- Cuando se reportan vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política se desarrolla mediante normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesitan conocerla, en particular para aquellos que utilizan, operan o administran los sistemas de información y comunicaciones.

Otros documentos que complementan esta política de seguridad son:

- El documento de seguridad de la Universidad Exempli Gratia.

- Normas de uso personal de los recursos informáticos y telemáticos de la Universidad Exempli Gratia.

- Los acuerdos del Consejo de Gobierno de la Universidad posteriores a la aprobación de esta política en la medida en que puedan afectarla.

La normativa de seguridad deberá estar disponible en la intranet de la Universidad.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Universidad Exempli Gratia tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la Universidad Exempli Gratia atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Universidad Exempli Gratia, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. TERCERAS PARTES

Cuando la Universidad Exempli Gratia preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad Exempli Gratia utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está

adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

21. Anexo II – Informe de auditoría

INFORME DE AUDITORÍA

1. Introducción

Esta auditoría sobre el grado de cumplimiento del Esquema Nacional de Seguridad se encuadra dentro de lo previsto en el Artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y específicamente dentro de los requisitos del Artículo 34 (Auditoría de la Seguridad) y del Anexo III (Auditoría de la Seguridad) 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.

Cargo	Nombre completo	Fecha	Firma
Auditor Jefe	Francisco Jose Muñoz Torrijos	25/5/2018	
Responsable de Seguridad	Francisco Jose Muñoz Torrijos		
Responsable del Sistema	Francisco Jose Muñoz Torrijos		

2. Tipo de auditoría

Se trata de una auditoría ordinaria.

3. Objetivo

Dar cumplimiento a lo establecido en el Artículo 34 y en el Anexo III del RD 3/2010 y, por lo tanto, verificar el cumplimiento de los requisitos establecidos por el RD 3/2710 en los Capítulos II y III y en los Anexos I y II.

4. Alcance

El alcance de la presente auditoría se ciñe al sistema de expedientes, de categoría Media, de la Universidad Exempli Gratia.

Sin limitaciones al alcance.

5. Resumen ejecutivo

Se cumple con la normativa requerida y no se han encontrado deficiencias en los sistemas, el grado *de* cumplimiento del sistema es alto.

6. Criterio metodológico utilizado

Para la ejecución de la presente auditoría se ha seguido el criterio metodológico de la guía CCN-STIC 808 respecto del cumplimiento de las medidas del ENS.

7. Legislación que afecta al sistema de información

Para la ejecución de la presente auditoría se ha tenido en cuenta la legislación que afecta al sistema de información objeto de la misma a fecha de la auditoría, que es:

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
- 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
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [*si aplica la LOPD*]
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [*si aplica la LOPD*]
- ……

8. Equipo auditor

El equipo auditor ha estado compuesto por:

- Auditor jefe: Francisco Jose Muñoz Torrijos
- Experto: Francisco Jose Muñoz Torrijos

9. Personal entrevistado

Durante la auditoría se ha entrevistado a:

- Francisco Jose Muñoz Torrijos responsable de los sistemas de información.

10.Fecha y lugar de realización

La auditoría comenzó el 21 de Febrero de 2018, y ha finalizado el 4 de Junio de 2018 y se desarrolló en las instalaciones de la Universidad Exempli Gratia.

11.Idioma

La auditoría se realizó en español.

12. Documentación revisada

Para la correcta ejecución de la auditoría se revisó la siguiente documentación:

- Política de seguridad (CCN-STIC 808)

13. Resultado de la auditoría

- No se encuentra ninguna deficiencia importante en los sistemas auditados

14. Comentarios al informe por los participantes

Los responsables implicados expresan su conformidad antes los resultados de las revisiones y pruebas.

15. Conclusiones

El grado de cumplimiento en el sistema de información analizado es **Alto** salvo por alguna salvedad.

22. Anexo III – Análisis de riesgos con la herramienta µPILAR

Análisis de Riesgos Universidad Exempli Gratia

1 Introducción

Documento para anexar a la documentación de seguridad del sistema que se presenta para conseguir la aprobación o autorización de la autoridad responsable del sistema de información.

Datos del sistema sujeto a análisis:

Código: 01
Nombre: Análisis de Riesgos Universidad Exempli Gratia

Descripción:

TFM UOC MISTIC - Adaptación al ENS. Análisis de Riesgos del caso de estudio Universidad Exempli Gratia.

Datos administrativos:

- Organización: Universidad Exempli Gratia
- Descripción: TFM UOC MISTIC - Adaptación al ENS. Análisis de Riesgos Universidad Exempli Gratia
- Autor: Francisco Jose Muñoz Torrijos
- Versión: 01
- Fecha: 29-05-2018
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
- Responsable de la Seguridad de la Información: Francisco Jose Muñoz Torrijos
- Delegado de Protección de Datos: Francisco Jose Muñoz Torrijos

1.1 Dimensiones de valoración

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos
- [DP] Datos personales

2 Dominios de seguridad

dominios de seguridad
- [base] Base

2.1 Agravantes y atenuantes

[base] Base
- [101] Identificación del atacante
  - [101.a] público en general
- [102] Motivación del atacante
  - [102.f] con ánimo destructivo
- [103] Beneficio del atacante
  - [103.a] moderadamente interesado
- [106] Atracción del objetivo
  - [106.a] objetivo muy poco atractivo
- [104] Motivación del personal interno
  - [104.c] sobrecargados de trabajo
- [105] Permisos de los usuarios (derechos)
  - [105.a] se permite el acceso a Internet
  - [105.b] se permite la ejecución de programas sin autorización previa
  - [105.c] se permite la instalación de programas sin autorización previa
  - [105.d] se permite la conexión de dispositivos removibles
- [111] Conectividad del sistema de información
  - [111.b] conectado a un conjunto reducido y controlado de redes

- [112] {xor} Ubicación del sistema de información
  - [112.a] dentro de una zona controlada

2.2 Valoración de los activos

capa: [essential] Activos esenciales

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[DP]
[I1] Información Aula Virtual	[n.a.]	[1](1)	[1](2)	[1](3)	[3](4)	
[I2] Licencias	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I3] Expedientes	[n.a.]	[4]	[4]	[4]	[4]	
[I4] Información supercomputación	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I5] Asignaturas	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I6] Plan Docente	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I7] Expedientes administrativos	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I8] Investigación	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I9] Datos económicos	[n.a.]	[n.a.]	[1](5)	[1](6)	[1](5)	
[I10] Contratación	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I11] Patrimonio e inventario	[n.a.]	[n.a.]	[n.a.]	[1](5)	[1](5)	
[I12] Personal	[n.a.]	[4]	[1](5)	[1](5)	[1](5)	
[I13] Prevención	[n.a.]	[4]	[4]	[4]	[4]	
[I14] Retribuciones	[n.a.]	[4]	[4]	[4]	[4]	
[I15] Actividades deportivas	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I16] Archivo	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I17] Registro	[n.a.]	[4]	[4]	[4]	[4]	
[I18] Documentación	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I19] Infraestructuras	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I20] Biblioteca	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I21] Almacén de datos	[n.a.]	[n.a.]	[1](5)	[1](5)	[n.a.]	
[I22] Atención al usuario (CAU)	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[I24] Material audiovisual y fotográfico	[n.a.]	[1](5)	[1](5)	[1](5)	[1](5)	
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	[4](7)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A1-S2] Soporte a las aulas multimedia.	[4](8)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A1-S3] Gestión del licenciamiento	[4](9)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A1-S4] Aula Virtual	[4](10)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A2-S1] Supercomputación	[4](10)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A2-S2] Consultoría	[2](11)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S1] Gestión académica	[4](12)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S2] Gestión económica y tesorería	[3](13)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S3] Contratación y presupuestos	[4](14)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S4] Gestión de RR.HH.	[1](15)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S5] Extensión Universitaria	[1](12)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S6] Archivo	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	

[A3-S7] Secretaria general	[4](16)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S8] Gestión de infraestructuras	[1](17)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S9] Servicio de bibliotecas	[1](9)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S10] Comunicación	[1](18)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S11] Calidad	[1](19)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S12] Análisis de datos	[1](20)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S13] Atención al usuario (CAU)	[1](21)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A3-S14] Gestión de publicaciones	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S1] Gestión del correo electrónico	[3](22)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S2] Web institucional	[4](11)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S3] Sede electrónica	[4](23)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S4] Intranet	[1](18)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S5] Portal del empleado	[1](18)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S6] Secretaria virtual	[1](24)	[n.a.]	[n.a.]	[n.a.]	[n.a.]	
[A4-S7] Contenidos digitales	[1]	[n.a.]	[n.a.]	[n.a.]	[n.a.]	

(1) {1} pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
{0} supondría pérdidas económicas mínimas
{1} Pudiera causar protestas puntuales
{1} Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
{1} pudiera impedir la operación efectiva de una parte de la Organización

(2) {1} pudiera causar molestias a un individuo
{1} pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

(3) {1} pudiera causar molestias a un individuo
{1} pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
{0} no supondría daño a la reputación o buena imagen de las personas u organizaciones

(4) {1} pudiera causar molestias a un individuo
{1} pudiera causar el incumplimiento leve o técnico de una ley o regulación
{3} Probablemente cause la interrupción de actividades propias de la Organización
{2} Probablemente cause una pérdida menor de la confianza dentro de la Organización
{1} Pudiera causar una pérdida menor de la confianza dentro de la Organización

(5) {1} pudiera causar molestias a un individuo
{1} pudiera causar el incumplimiento leve o técnico de una ley o regulación
{1} pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
{0} supondría pérdidas económicas mínimas
{3} Probablemente cause la interrupción de actividades propias de la Organización

{1} Pudiera causar protestas puntuales
{3} Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
{1} pudiera impedir la operación efectiva de una parte de la Organización
{2} Probablemente cause una pérdida menor de la confianza dentro de la Organización
Nacional

(6) {2} pudiera quebrantar de forma leve leyes o regulaciones
{1} pudiera causar el incumplimiento leve o técnico de una ley o regulación
{1} pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
{0} supondría pérdidas económicas mínimas
{3} Probablemente cause la interrupción de actividades propias de la Organización
{1} Pudiera causar protestas puntuales
{3} Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
{1} pudiera impedir la operación efectiva de una parte de la Organización
{2} Probablemente cause una pérdida menor de la confianza dentro de la Organización
Nacional

(7) {4} probablemente afecte a un grupo de individuos
{0} supondría pérdidas económicas mínimas
{3} Probablemente cause la interrupción de actividades propias de la Organización
{3} Causa de protestas puntuales
{1} Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
{1} pudiera impedir la operación efectiva de una parte de la Organización
{2} Probablemente cause una pérdida menor de la confianza dentro de la Organización
{1} 1 día < RTO < 5 días
{1} Sin Clasificar

(8) {4} probablemente afecte a un grupo de individuos
{1} Pudiera causar la interrupción de actividades propias de la Organización

(9) {0} no supondría daño a la reputación o buena imagen de las personas u organizaciones

(10) {3} Probablemente cause la interrupción de actividades propias de la Organización

(11) {2} Probablemente cause una pérdida menor de la confianza dentro de la Organización

(12) {1} Pudiera causar la interrupción de actividades propias de la Organización
{1} pudiera impedir la operación efectiva de una parte de la Organización

(13) {3} Probablemente cause la interrupción de actividades propias de la Organización
{1} Pudiera causar la interrupción de actividades propias de la Organización
{1} Pudiera causar una pérdida menor de la confianza dentro de la Organización

(14) {3} Probablemente cause la interrupción de actividades propias de la Organización
{1} pudiera impedir la operación efectiva de una parte de la Organización
{2} Probablemente cause una pérdida menor de la confianza dentro de la Organización

(15) {1} Pudiera causar la interrupción de actividades propias de la Organización
{1} pudiera impedir la operación efectiva de una parte de la Organización
{1} Pudiera causar una pérdida menor de la confianza dentro de la Organización
{1} 1 día < RTO < 5 días

(16) {1} pudiera causar el incumplimiento leve o técnico de una ley o regulación
{1} pudiera impedir la operación efectiva de una parte de la Organización
{1} Pudiera causar una pérdida menor de la confianza dentro de la Organización

(17) {1} pudiera causar molestias a un individuo
{1} podría lesionar levemente a un individuo

(18) {1} Pudiera causar una pérdida menor de la confianza dentro de la Organización

(19) {1} Pudiera causar la interrupción de actividades propias de la Organización

(20) {1} pudiera causar molestias a un individuo

(21) {1} Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
{1} Pudiera causar una pérdida menor de la confianza dentro de la Organización

(22) {3} Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)

(23) {1} pudiera causar el incumplimiento leve o técnico de una ley o regulación
{3} Probablemente cause la interrupción de actividades propias de la Organización

(24) {1} Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

2.3 Valoración de los dominios

dominio de seguridad	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[DP]**
[base] Base	[4]	[4]	[4]	[4]	[4]	

3 Riesgo acumulado

Se presentan los principales riesgos en cada dominio de seguridad del sistema en las diferentes fases de trabajo.

amenaza
: presenta la amenaza dentro del catálogo de PILAR. Una amenaza aparece cuando algún activo del sistema está expuesto a ella

D – dimensión
: se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
: se muestra el máximo impacto causado por esta amenaza en algún activo del sistema

R – riesgo
: se muestra el máximo riesgo al que está expuesto el sistema por causa de esta amenaza

Fase: [potencial]
[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[3]	{4,7}
[A.5] Suplantación de la identidad	A	[4]	{4,4}

Fase: [current] situación actual
[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[3]	{4,7}
[A.5] Suplantación de la identidad	A	[4]	{4,4}

Fase: [PILAR] recomendación
[base] Base

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[0]	{1,1}
[A.5] Suplantación de la identidad	A	[0]	{0,95}

4 Riesgo repercutido

Se presentan los máximos riesgos a los que están expuestos los activos esenciales del sistema en cada fase de trabajo.

activo
: presenta el activo esencial que está en riesgo; es decir, sobre el que repercute indirectamente la amenaza

amenaza
presenta la amenaza dentro del catálogo de PILAR.

D – dimensión
se muestra la dimensión (o dimensiones) de seguridad a las que afecta la amenaza

I – impacto
se muestra el máximo impacto causado por esta amenaza sobre el activo esencial

R – riesgo
se muestra el máximo riesgo al que está expuesto el activo esencial por causa de esta amenaza

Fase: [potencial]
[base] Base

activo	amenaza	D	I	R
[I3] Expedientes	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I13] Prevención	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I14] Retribuciones	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I17] Registro	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I3] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I12] Personal	[A.5] Suplantación de la identidad	I	[4]	{4,4}
[I13] Prevención	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I14] Retribuciones	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I17] Registro	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I3] Expedientes	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I12] Personal	[A.15] Modificación de la información	I	[4]	{4,1}
[I13] Prevención	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I14] Retribuciones	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I17] Registro	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	[A.24] Denegación de servicio	D	[4]	{3,9}
[A1-S2] Soporte a las aulas multimedia.	[A.24] Denegación de servicio	D	[4]	{3,9}
[A1-S3] Gestión del licenciamiento	[A.24] Denegación de servicio	D	[4]	{3,9}

[A1-S4] Aula Virtual	[A.24] Denegación de servicio	D	[4]	{3,9}
[A2-S1] Supercomputación	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S1] Gestión académica	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S3] Contratación y presupuestos	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S7] Secretaria general	[A.24] Denegación de servicio	D	[4]	{3,9}
[A4-S2] Web institucional	[A.24] Denegación de servicio	D	[4]	{3,9}
[A4-S3] Sede electrónica	[A.24] Denegación de servicio	D	[4]	{3,9}
[I1] Información Aula Virtual	[A.5] Suplantación de la identidad	T	[3]	{3,8}
[I3] Expedientes	[A.19] Revelación de información	C	[3]	{3,8}
[I3] Expedientes	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I13] Prevención	[A.19] Revelación de información	C	[3]	{3,8}
[I13] Prevención	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I14] Retribuciones	[A.19] Revelación de información	C	[3]	{3,8}
[I14] Retribuciones	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I17] Registro	[A.19] Revelación de información	C	[3]	{3,8}
[I17] Registro	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}

Fase: [current] situación actual
[base] Base

activo	amenaza	D	I	R
[I3] Expedientes	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I13] Prevención	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I14] Retribuciones	[A.11] Acceso no autorizado	C, A	[3]	{4,7}
[I17] Registro	[A.11] Acceso no autorizado	C, A	[3]	{4,7}

[I3] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I12] Personal	[A.5] Suplantación de la identidad	I	[4]	{4,4}
[I13] Prevención	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I14] Retribuciones	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I17] Registro	[A.5] Suplantación de la identidad	I, C, A, T	[4]	{4,4}
[I3] Expedientes	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I12] Personal	[A.15] Modificación de la información	I	[4]	{4,1}
[I13] Prevención	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I14] Retribuciones	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[I17] Registro	[A.15] Modificación de la información	I, A, T	[4]	{4,1}
[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia	[A.24] Denegación de servicio	D	[4]	{3,9}
[A1-S2] Soporte a las aulas multimedia.	[A.24] Denegación de servicio	D	[4]	{3,9}
[A1-S3] Gestión del licenciamiento	[A.24] Denegación de servicio	D	[4]	{3,9}
[A1-S4] Aula Virtual	[A.24] Denegación de servicio	D	[4]	{3,9}
[A2-S1] Supercomputación	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S1] Gestión académica	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S3] Contratación y presupuestos	[A.24] Denegación de servicio	D	[4]	{3,9}
[A3-S7] Secretaria general	[A.24] Denegación de servicio	D	[4]	{3,9}
[A4-S2] Web institucional	[A.24] Denegación de servicio	D	[4]	{3,9}
[A4-S3] Sede electrónica	[A.24] Denegación de servicio	D	[4]	{3,9}
[I1] Información Aula Virtual	[A.5] Suplantación de la identidad	T	[3]	{3,8}
[I3] Expedientes	[A.19] Revelación de información	C	[3]	{3,8}
[I3] Expedientes	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I13] Prevención	[A.19] Revelación de	C	[3]	{3,8}

	información			
[I13] Prevención	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I14] Retribuciones	[A.19] Revelación de información	C	[3]	{3,8}
[I14] Retribuciones	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}
[I17] Registro	[A.19] Revelación de información	C	[3]	{3,8}
[I17] Registro	[A.13] Repudio (negación de actuaciones)	T	[4]	{3,8}

Fase: [PILAR] recomendación
[base] Base

activo	amenaza	D	I	R
[I3] Expedientes	[A.11] Acceso no autorizado	C, A	[0]	{1,1}
[I13] Prevención	[A.11] Acceso no autorizado	C, A	[0]	{1,1}
[I14] Retribuciones	[A.11] Acceso no autorizado	C, A	[0]	{1,1}
[I17] Registro	[A.11] Acceso no autorizado	C, A	[0]	{1,1}
[I3] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,95}
[I13] Prevención	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,95}
[I14] Retribuciones	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,95}
[I17] Registro	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,95}
[I3] Expedientes	[A.15] Modificación de la información	I	[0]	{0,94}
[I12] Personal	[A.15] Modificación de la información	I	[0]	{0,94}
[I12] Personal	[A.5] Suplantación de la identidad	I	[0]	{0,94}
[I13] Prevención	[A.15] Modificación de la información	I	[0]	{0,94}
[I14] Retribuciones	[A.15] Modificación de la información	I	[0]	{0,94}
[I17] Registro	[A.15] Modificación de la información	I	[0]	{0,94}
[A1-S1] Soporte a las aulas	[A.24] Denegación	D	[0]	{0,88}

informáticas de libre acceso y de docencia	de servicio			
[A1-S2] Soporte a las aulas multimedia.	[A.24] Denegación de servicio	D	[0]	{0,88}
[A1-S3] Gestión del licenciamiento	[A.24] Denegación de servicio	D	[0]	{0,88}
[A1-S4] Aula Virtual	[A.24] Denegación de servicio	D	[0]	{0,88}
[A2-S1] Supercomputación	[A.24] Denegación de servicio	D	[0]	{0,88}
[A3-S1] Gestión académica	[A.24] Denegación de servicio	D	[0]	{0,88}
[A3-S3] Contratación y presupuestos	[A.24] Denegación de servicio	D	[0]	{0,88}
[A3-S7] Secretaria general	[A.24] Denegación de servicio	D	[0]	{0,88}
[A4-S2] Web institucional	[A.24] Denegación de servicio	D	[0]	{0,88}
[A4-S3] Sede electrónica	[A.24] Denegación de servicio	D	[0]	{0,88}

5 Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Base

- Activos esenciales
  - [essential] Activos esenciales
    - [I1] Información Aula Virtual
    - [I2] Licencias
    - [I3] Expedientes
    - [I4] Información supercomputación
    - [I5] Asignaturas
    - [I6] Plan Docente
    - [I7] Expedientes administrativos
    - [I8] Investigación
    - [I9] Datos económicos
    - [I10] Contratación
    - [I11] Patrimonio e inventario
    - [I12] Personal
    - [I13] Prevención
    - [I14] Retribuciones
    - [I15] Actividades deportivas
    - [I16] Archivo
    - [I17] Registro
    - [I18] Documentación
    - [I19] Infraestructuras
    - [I20] Biblioteca
    - [I21] Almacén de datos
    - [I22] Atención al usuario (CAU)
    - [I23] Correo Electrónico
    - [I24] Material audiovisual y fotográfico
    - [I25] Directorio
    - [I26] Registros de acceso y navegación
    - [A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia
    - [A1-S2] Soporte a las aulas multimedia.
    - [A1-S3] Gestión del licenciamiento
    - [A1-S4] Aula Virtual
    - [A2-S1] Supercomputación
    - [A2-S2] Consultoría
    - [A3-S1] Gestión académica
    - [A3-S2] Gestión económica y tesorería
    - [A3-S3] Contratación y presupuestos
    - [A3-S4] Gestión de RR.HH.
    - [A3-S5] Extensión Universitaria
    - [A3-S6] Archivo
    - [A3-S7] Secretaria general
    - [A3-S8] Gestión de infraestructuras
    - [A3-S9] Servicio de bibliotecas
    - [A3-S10] Comunicación
    - [A3-S11] Calidad

        - [A3-S12] Análisis de datos
        - [A3-S13] Atención al usuario (CAU)
        - [A3-S14] Gestión de publicaciones
        - [A4-S1] Gestión del correo electrónico
        - [A4-S2] Web institucional
        - [A4-S3] Sede electrónica
        - [A4-S4] Intranet
        - [A4-S5] Portal del empleado
        - [A4-S6] Secretaria virtual
        - [A4-S7] Contenidos digitales
        - [A5-S1] Servicio integral Workplace
        - [A6-S1] Servicio de Telefonía fija, móvil y fax
        - [A6-S2] Servicio de red cableada e inalámbrica
        - [A7-S1] Servicios de directorio
- activos
    - [D] Datos / Información
        - [D.files] ficheros de datos
        - [D.e-files] ficheros cifrados
        - [D.backup] copias de respaldo
        - [D.conf] datos de configuración
        - [D.int] datos de gestión interna
        - [D.password] credenciales (ej. contraseñas)
        - [D.auth] datos de validación de credenciales
        - [D.acl] datos de control de acceso
        - [D.log] registro de actividad (log)
        - [D.voice] voz
        - [D.multimedia] multimedia
        - [D.source] código fuente
        - [D.exe] código ejecutable
        - [D.test] datos de prueba
    - [keys] Claves criptográficas
        - [keys.info] protección de la información
        - [keys.com] protección de las comunicaciones
        - [keys.disk] cifrado de soportes de información
        - [keys.x509] certificados de clave pública
    - [S] Servicios
        - [S.prov.anon] anónimo (sin requerir identificación)
        - [S.prov.pub] al público en general (sin relación contractual)
        - [S.prov.ext] a usuarios externos (bajo una relación contractual)
        - [S.prov.int] interno (usuarios y medios de la propia organización)
        - [S.prov.www] world wide web
        - [S.prov.email] correo electrónico
        - [S.prov.voip] voz sobre ip
        - [S.prov.file] almacenamiento de ficheros
        - [S.prov.print] servicio de impresión
        - [S.prov.backup] servicio de copias de respaldo (backup)
        - [S.prov.time] servicio de tiempos
        - [S.prov.edi] intercambio electrónico de datos
        - [S.prov.dir] servicio de directorio
        - [S.prov.dns] servidor de nombres de dominio

    - [S.prov.ipm] gestión de privilegios
- [SW] Aplicaciones (software)
    - [SW.prp] desarrollo propio (in house)
    - [SW.std.www] servidor de presentación
    - [SW.std.app] servidor de aplicaciones
    - [SW.std.email_server] servidor de correo electrónico
    - [SW.std.directory] servidor de directorio
    - [SW.std.file] servidor de ficheros
    - [SW.std.dbms] sistema de gestión de bases de datos
    - [SW.std.tm] monitor transaccional
    - [SW.std.os] sistema operativo
    - [SW.std.os.windows] windows
    - [SW.std.os.linux] linux
    - [SW.std.os.macosx] mac osx
    - [SW.std.hypervisor] hypervisor (gestor de la máquina virtual)
    - [SW.std.backup] servicio de backup
    - [SW.sec] herramientas de seguridad
    - [SW.sec.av] anti virus
    - [SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)
    - [SW.sec.traf] análisis de tráfico
- [HW] Equipamiento informático (hardware)
    - [HW.host] grandes equipos (host)
    - [HW.mid] equipos medios
    - [HW.pc] informática personal
    - [HW.peripheral] periféricos
    - [HW.peripheral.print] medios de impresión
- [COM] Redes de comunicaciones
    - [COM.wifi] WiFi
    - [COM.LAN] red local
    - [COM.VLAN] LAN virtual
    - [COM.Internet] Internet
    - [COM.vpn] canal cifrado (red privada virtual)
    - [COM.backup] comunicaciones de respaldo
- [Media] Soportes de información
    - [Media.electronic] electrónicos
- [AUX] Equipamiento auxiliar
    - [AUX.power] fuentes de alimentación
    - [AUX.ups] sai - sistemas de alimentación ininterrumpida
    - [AUX.gen] generadores eléctricos
    - [AUX.ac] equipos de climatización
    - [AUX.cabling] cableado de datos
    - [AUX.cabling.wire] cable eléctrico
    - [AUX.cabling.fiber] fibra óptica
- [L] Instalaciones
    - [L.building] edificio
    - [L.local] cuarto
- [P] Personal
    - [P.ue] usuarios externos
    - [P.ui] usuarios internos
    - [P.op] operadores

- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.sec] administradores de seguridad
- [P.dev] desarrolladores / programadores
- [P.sub] subcontratas
- [P.prov] proveedores

5.1 Descripción

Detalle de los activos identificados en el sistema de información.

dominio de seguridad: [base] Base

[I1] Información Aula Virtual

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

  Información sobre los alumnos, contenidos de asignaturas, debates, ejercicios, etc. Pertenecientes al Aula Virtual

[I2] Licencias

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

  Licencias software de los equipos corporativos

[I3] Expedientes

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Información sobre los expedientes académicos, títulos, exámenes, Tesis y estudiantes con necesidades educativas especiales

[I4] Información supercomputación

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Información sobre los datos manejados en proyectos de supercomputación

[I5] Asignaturas

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Contenido de las distintas asignaturas de las titulaciones.

[I6] Plan Docente

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Asignación de asignaturas a los docentes y horarios de docencia

[I7] Expedientes administrativos

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos pertenecientes a los expedientes administrativos

[I8] Investigación

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos de gestión de proyectos de investigación

[I9] Datos económicos

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos de gestión económica de la Universidad, presupuestos, ingresos y contabilidad

[I10] Contratación

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos relativos a los expedientes de contratación

[I11] Patrimonio e inventario

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Bienes muebles e inmuebles de la Universidad e inventario de los mismos

[I12] Personal

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

  Datos del personal de la Universidad, selección, acceso, expedientes, relación de Puestos de Trabajo, Control Horario, Valoración del Desempeño y formación

[I13] Prevención

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

  Datos de los procesos de prevención, incluyendo procesos de revisión médica de los recursos humanos de la Universidad

[I14] Retribuciones

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

  Retribuciones del personal de la Universidad

[I15] Actividades deportivas

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos gestionados por el Servicio de Deportes

[I16] Archivo

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos del Archivo universitario en diferentes soportes como documentos, fichas, DVD, negativos y positivos fotográficos, cuadernos, películas e impresos.

[I17] Registro

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos del Registro universitario, incluyendo procesos de entrada/salida, en modalidad presencial y telemática

[I18] Documentación

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Datos de gestión documental institucional, convenios, normativa universitaria, procesos electorales, censo y publicaciones

[I19] Infraestructuras

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Datos de los espacios universitarios, incluyendo procesos de reserva de los mismos, control de acceso a edificios e instalaciones

[I20] Biblioteca

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Aplicaciones para la gestión de los procesos soportados por la Biblioteca universitaria, repositorio institucional de la Universidad y catálogo de Biblioteca.

[I21] Almacén de datos

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Análisis de datos, e información institucional, como el Data warehouse.

[I22] Atención al usuario (CAU)

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Datos de peticiones e incidencias relacionadas con los servicios universitarios

[I23] Correo Electrónico

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales

- [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Datos correo electrónico (mensajes, listas…) destinado al PAS, PDI, estudiantes universitarios, preuniversitarios y egresados.

[I24] Material audiovisual y fotográfico

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Imágenes, voz, video, grabaciones de video-vigilancia.

[I25] Directorio

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Información de contacto sobre los usuarios de la Universidad.

[I26] Registros de acceso y navegación

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.info] información

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Registros de acceso a los sistemas, registros de navegación interna/Internet, etc.

[A1-S1] Soporte a las aulas informáticas de libre acceso y de docencia

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales

- [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Soporte a las aulas informáticas de libre acceso y de docencia

[A1-S2] Soporte a las aulas multimedia.

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

[A1-S3] Gestión del licenciamiento

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Gestión del licenciamiento

[A1-S4] Aula Virtual

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Aula Virtual

[A2-S1] Supercomputación

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Supercomputación

[A2-S2] Consultoría
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Consultoría

[A3-S1] Gestión académica
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Gestión académica

[A3-S2] Gestión económica y tesorería
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Gestión económica y tesorería

[A3-S3] Contratación y presupuestos
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Contratación y presupuestos

[A3-S4] Gestión de RR.HH.

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Gestión de RR.HH.

[A3-S5] Extensión Universitaria

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Extensión Universitaria

[A3-S6] Archivo

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Archivo

[A3-S7] Secretaria general

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Secretaria general

[A3-S8] Gestión de infraestructuras

Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Gestión de infraestructuras

[A3-S9] Servicio de bibliotecas
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Servicio de bibliotecas

[A3-S10] Comunicación
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Comunicación

[A3-S11] Calidad
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Calidad

[A3-S12] Análisis de datos
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Análisis de datos

[A3-S13] Atención al usuario (CAU)

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Atención al usuario (CAU)

[A3-S14] Gestión de publicaciones

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Gestión de publicaciones

[A4-S1] Gestión del correo electrónico

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Gestión del correo electrónico

[A4-S2] Web institucional

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Web institucional

[A4-S3] Sede electrónica

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Sede electrónica

[A4-S4] Intranet

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Intranet

[A4-S5] Portal del empleado

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Portal del empleado

[A4-S6] Secretaria virtual

Dominio de seguridad

[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Secretaria virtual

[A4-S7] Contenidos digitales
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Contenidos digitales

[A5-S1] Servicio integral Workplace
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Servicio integral Workplace

[A6-S1] Servicio de Telefonía fija, móvil y fax
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos
- Responsable del Sistema: Francisco Jose Muñoz Torrijos
  Servicio de Telefonía fija, móvil y fax

[A6-S2] Servicio de red cableada e inalámbrica
Dominio de seguridad
[base] Base

Clases de activos
- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Servicio de red cableada e inalámbrica

[A7-S1] Servicios de directorio

Dominio de seguridad

[base] Base

Clases de activos

- [essential] Activos esenciales
  - [essential.service] servicio

Datos

- Responsable del Sistema: Francisco Jose Muñoz Torrijos

Servicios de directorio

[D.files] ficheros de datos

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.files] ficheros de datos

[D.e-files] ficheros cifrados

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.e-files] ficheros cifrados

[D.backup] copias de respaldo

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.backup] copias de respaldo

[D.conf] datos de configuración

Dominio de seguridad

[base] Base

Clases de activos

- [D] Datos / Información
  - [D.conf] datos de configuración

[D.int] datos de gestión interna

Dominio de seguridad

[base] Base

Clases de activos
- [D] Datos / Información
  - [D.int] datos de gestión interna

[D.password] credenciales (ej. contraseñas)
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.password] credenciales (ej. contraseñas)

[D.auth] datos de validación de credenciales
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.auth] datos de validación de credenciales

[D.acl] datos de control de acceso
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.acl] datos de control de acceso

[D.log] registro de actividad (log)
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.log] registro de actividad (log)

[D.voice] voz
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.voice] voz

[D.multimedia] multimedia
Dominio de seguridad
[base] Base

Clases de activos

- [D] Datos / Información
  - [D.multimedia] multimedia

[D.source] código fuente
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.source] código fuente

[D.exe] código ejecutable
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.exe] código ejecutable

[D.test] datos de prueba
Dominio de seguridad
[base] Base

Clases de activos
- [D] Datos / Información
  - [D.test] datos de prueba

[keys.info] protección de la información
Dominio de seguridad
[base] Base

Clases de activos
- [keys] Claves criptográficas
  - [keys.info] protección de la información

[keys.com] protección de las comunicaciones
Dominio de seguridad
[base] Base

Clases de activos
- [keys] Claves criptográficas
  - [keys.com] protección de las comunicaciones

[keys.disk] cifrado de soportes de información
Dominio de seguridad
[base] Base

Clases de activos
- [keys] Claves criptográficas
  - [keys.disk] cifrado de soportes de información

[keys.x509] certificados de clave pública

Dominio de seguridad

[base] Base

Clases de activos

- [keys] Claves criptográficas
  - [keys.x509] certificados de clave pública

[S.prov.anon] anónimo (sin requerir identificación)

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.anon] anónimo (sin requerir identificación)

[S.prov.pub] al público en general (sin relación contractual)

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.pub] al público en general (sin relación contractual)

[S.prov.ext] a usuarios externos (bajo una relación contractual)

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.ext] a usuarios externos (bajo una relación contractual)

[S.prov.int] interno (usuarios y medios de la propia organización)

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.int] interno (usuarios y medios de la propia organización)

[S.prov.www] world wide web

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.www] world wide web

[S.prov.email] correo electrónico

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.email] correo electrónico

[S.prov.voip] voz sobre ip

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.voip] voz sobre ip

[S.prov.file] almacenamiento de ficheros

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.file] almacenamiento de ficheros

[S.prov.print] servicio de impresión

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.print] servicio de impresión

[S.prov.backup] servicio de copias de respaldo (backup)

Dominio de seguridad

[base] Base

Clases de activos

- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.backup] servicio de copias de respaldo (backup)

[S.prov.time] servicio de tiempos

Dominio de seguridad
[base] Base

Clases de activos
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.time] servicio de tiempos

[S.prov.edi] intercambio electrónico de datos
Dominio de seguridad
[base] Base

Clases de activos
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.edi] intercambio electrónico de datos

[S.prov.dir] servicio de directorio
Dominio de seguridad
[base] Base

Clases de activos
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.dir] servicio de directorio

[S.prov.dns] servidor de nombres de dominio
Dominio de seguridad
[base] Base

Clases de activos
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.dns] servidor de nombres de dominio

[S.prov.ipm] gestión de privilegios
Dominio de seguridad
[base] Base

Clases de activos
- [S] Servicios
  - [S.prov] proporcionado por nosotros
  - [S.prov.ipm] gestión de privilegios

[SW.prp] desarrollo propio (in house)
Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)

- [SW.prp] desarrollo propio (in house)

[SW.std.www] servidor de presentación

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.www] servidor de presentación

[SW.std.app] servidor de aplicaciones

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.app] servidor de aplicaciones

[SW.std.email_server] servidor de correo electrónico

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.email_server] servidor de correo electrónico

[SW.std.directory] servidor de directorio

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.directory] servidor de directorio

[SW.std.file] servidor de ficheros

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.file] servidor de ficheros

[SW.std.dbms] sistema de gestión de bases de datos

Dominio de seguridad

[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.dbms] sistema de gestión de bases de datos

[SW.std.tm] monitor transaccional

Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.tm] monitor transaccional

[SW.std.os] sistema operativo

Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo

[SW.std.os.windows] windows

Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo
    - [SW.std.os.windows] windows

[SW.std.os.linux] linux

Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.os] sistema operativo
    - [SW.std.os.linux] linux

[SW.std.os.macosx] mac osx

Dominio de seguridad
[base] Base

Clases de activos
- [SW] Aplicaciones (software)

- [SW.std] estándar (off the shelf)
- [SW.std.os] sistema operativo
  - [SW.std.os.macosx] mac osx

[SW.std.hypervisor] hypervisor (gestor de la máquina virtual)

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.hypervisor] hypervisor (gestor de la máquina virtual)

[SW.std.backup] servicio de backup

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.std] estándar (off the shelf)
  - [SW.std.backup] servicio de backup

[SW.sec] herramientas de seguridad

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.sec] herramientas de seguridad

[SW.sec.av] anti virus

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.sec] herramientas de seguridad
  - [SW.sec.av] anti virus

[SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)

Dominio de seguridad

[base] Base

Clases de activos

- [SW] Aplicaciones (software)
  - [SW.sec] herramientas de seguridad
  - [SW.sec.ids] IDS / IPS (deteción / prevención de intrusion)

[SW.sec.traf] análisis de tráfico

Dominio de seguridad

[base] Base

Clases de activos
- [SW] Aplicaciones (software)
  - [SW.sec] herramientas de seguridad
  - [SW.sec.traf] análisis de tráfico

[HW.host] grandes equipos (host)
Dominio de seguridad
[base] Base

Clases de activos
- [HW] Equipamiento informático (hardware)
  - [HW.host] grandes equipos (host)

[HW.mid] equipos medios
Dominio de seguridad
[base] Base

Clases de activos
- [HW] Equipamiento informático (hardware)
  - [HW.mid] equipos medios

[HW.pc] informática personal
Dominio de seguridad
[base] Base

Clases de activos
- [HW] Equipamiento informático (hardware)
  - [HW.pc] informática personal

[HW.peripheral] periféricos
Dominio de seguridad
[base] Base

Clases de activos
- [HW] Equipamiento informático (hardware)
  - [HW.peripheral] periféricos

[HW.peripheral.print] medios de impresión
Dominio de seguridad
[base] Base

Clases de activos
- [HW] Equipamiento informático (hardware)
  - [HW.peripheral] periféricos
  - [HW.peripheral.print] medios de impresión

[COM.wifi] WiFi
Dominio de seguridad

[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.wifi] WiFi

[COM.LAN] red local
Dominio de seguridad
[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.LAN] red local

[COM.VLAN] LAN virtual
Dominio de seguridad
[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.VLAN] LAN virtual

[COM.Internet] Internet
Dominio de seguridad
[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.Internet] Internet

[COM.vpn] canal cifrado (red privada virtual)
Dominio de seguridad
[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.vpn] canal cifrado (red privada virtual)

[COM.backup] comunicaciones de respaldo
Dominio de seguridad
[base] Base

Clases de activos
- [COM] Redes de comunicaciones
  - [COM.backup] comunicaciones de respaldo

[Media.electronic] electrónicos
Dominio de seguridad
[base] Base

Clases de activos
- [Media] Soportes de información
  - [Media.electronic] electrónicos

[AUX.power] fuentes de alimentación

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar
  - [AUX.power] fuentes de alimentación

[AUX.ups] sai - sistemas de alimentación ininterrumpida

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar
  - [AUX.ups] sai - sistemas de alimentación ininterrumpida

[AUX.gen] generadores eléctricos

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar
  - [AUX.gen] generadores eléctricos

[AUX.ac] equipos de climatización

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar
  - [AUX.ac] equipos de climatización

[AUX.cabling] cableado de datos

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar
  - [AUX.cabling] cableado de datos

[AUX.cabling.wire] cable eléctrico

Dominio de seguridad
[base] Base

Clases de activos
- [AUX] Equipamiento auxiliar

- [AUX.cabling] cableado de datos
- [AUX.cabling.wire] cable eléctrico

[AUX.cabling.fiber] fibra óptica

Dominio de seguridad

[base] Base

Clases de activos

- [AUX] Equipamiento auxiliar
  - [AUX.cabling] cableado de datos
  - [AUX.cabling.fiber] fibra óptica

[L.building] edificio

Dominio de seguridad

[base] Base

Clases de activos

- [L] Instalaciones
  - [L.building] edificio

[L.local] cuarto

Dominio de seguridad

[base] Base

Clases de activos

- [L] Instalaciones
  - [L.local] cuarto

[P.ue] usuarios externos

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.ue] usuarios externos

[P.ui] usuarios internos

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.ui] usuarios internos

[P.op] operadores

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal

- [P.op] operadores

[P.adm] administradores de sistemas

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.adm] administradores de sistemas

[P.com] administradores de comunicaciones

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.com] administradores de comunicaciones

[P.dba] administradores de BBDD

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.dba] administradores de BBDD

[P.sec] administradores de seguridad

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.sec] administradores de seguridad

[P.dev] desarrolladores / programadores

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.dev] desarrolladores / programadores

[P.sub] subcontratas

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.sub] subcontratas

[P.prov] proveedores

Dominio de seguridad

[base] Base

Clases de activos

- [P] Personal
  - [P.prov] proveedores