Elaboración de un Plan de adecuación al Esquema Nacional de Seguridad

Nombre Estudiante: Rubén Lacruz Sanz
Plan de Estudios del Estudiante: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Nombre Consultor: Ana Maria Chulia Cebolla

Fecha entrega: 5 de enero de 2018

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Elaboración de un Plan de adecuación al Esquema Nacional de Seguridad
Nombre del autor:	Rubén Lacruz Sanz
Nombre del consultor:	Ana Maria Chulia Cebolla
Fecha de entrega (mm/aaaa):	01/2018
Área del Trabajo Final:	TFM ad-hoc
Titulación:	Master Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Resumen del Trabajo (máximo 250 palabras):

La Seguridad de la Información es ya hoy una realidad y algo que todas las organizaciones deben tener integrado en todos los niveles de su estructura, y principalmente en su dirección, si no quieren quedarse atrás en las medidas de actuación, dentro del hipersector TIC.

Cualquier empresa o institución debe contar ya con los profesionales y medios adecuados que le permitan dirigir y gestionar con éxito, la seguridad de sus recursos, tanto físicos como lógicos.

Para la administración pública española este proceso, de obligado cumplimiento, implica la implantación del Esquema Nacional de Seguridad (ENS)

El ENS ayudará a que los ciudadanos puedan desarrollar, a través de medios digitales, gestiones relacionadas con la eAdministración con mayor seguridad y confianza en todos los procesos relacionados con sistemas, datos y comunicaciones electrónicas. Lo que sin duda supone un impulso al desarrollo de la sociedad de la información.

El presente trabajo describe el Plan de adecuación al ENS en un ayuntamiento. Con el objeto de realizar todo el trabajo se ha estructurado en seis fases: situación inicial, análisis diferencial del ENS, análisis de riesgos, definición de Plan de Adecuación al ENS, Adecuación al ENS y auditoría de conformidad.

Abstract (in English, 250 words or less):

Information Security is now a reality and something that all organizations must have integrated at all levels of its structure, and mainly in its direction, if they do not want to be left behind in the action measures, within the ICT sector.

Any company or institution must already have the appropriate professionals and resources that allow it to manage and successfully manage the security of its resources, both physical and logical.

For the Spanish public administration, this process, which is mandatory, implies the implantation of the National Security Scheme (ENS)

The ENS will help citizens to develop, through digital means, eAdministration related procedures with greater security and confidence in all processes related to systems, data and electronic communications. What undoubtedly supposes an impulse to the development of the society of the information.

The present work describes the Plan of adaptation to the ENS in a town hall. In order to carry out all the work, it has been structured in six phases: initial situation, differential analysis of the ENS, risk analysis, definition of the Adaptation Plan to the ENS, adaptation to the ENS and compliance audit.

Palabras clave (entre 4 y 8):

Esquema Nacional de Seguridad, Plan de Adecuación, Metodología MAGERIT, PILAR.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

La necesidad a cubrir en este proyecto es la obligada implantación en una administración pública del Esquema Nacional de Seguridad (ENS). Este establece un marco de seguridad para los sistemas de información que sustentan la aplicación de LAESCP (Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos). La LAESCP nace con el propósito de que el ciudadano pueda llevar a cabo sus trámites administrativos con las Administraciones Públicas vía web.

El Plan de adecuación al Esquema Nacional de Seguridad es un aspecto clave en cualquier organización de la administración pública española o que ofrezca sus servicios a esta misma.

El principal objetivo es sentar las bases del proceso de mejora continua en materia de seguridad de la Información, permitiendo a las organizaciones conocer el estado de la misma y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Se trata de un tema que frecuentemente no preocupa a las altos comités de dirección de las organizaciones pero en el momento que descubren que en su empresa ha habido una fuga de información o han sufrido una denegación de servicio de sus aplicaciones corporativas y por ello una pérdida de dinero o reputación, comienzan a valorar la importancia de disponer de una implementación de seguridad.

Para que no se trate de acciones reactivas y puntuales, es decir, a posterior de la incidencia ocurrida, se deben de implantar unas medidas de seguridad que permitan reducir los riesgos a los que está expuesta una organización y dedicar los recursos necesarios a prevenir los posibles ataques o incidencias que puede sufrir una entidad.

1.2 Objetivos del Trabajo

El presente Trabajo Final de Máster tiene como objetivo principal la adecuación de una Administración Pública local al Esquema Nacional de Seguridad estableciendo un Plan de adecuación. Para ellos es necesario conocer las diferentes etapas necesarias.

En este caso se realiza en un ayuntamiento, un organismo de la administración pública española que tiene su obligada implantación.

Como objetivos secundarios destacaríamos el conocer el concepto de política de seguridad, la estructura de un procedimiento del sistema de gestión documental, las diferentes metodologías para desarrollar un análisis de riesgos y también estudiar los posibles proyectos que se pueden llevar a cabo para reducir las amenazas a las que está expuesta una organización.

1.3 Enfoque y método seguido

El Esquema Nacional de Seguridad es un marco normativo reconocido a nivel nacional y sobre el que se apoyan las organizaciones certificadoras para determinar si una organización cumple con los requisitos necesarios que debe tener si sus servicios están relacionados con las administraciones públicas.

Por ello, el marco normativo ha servido como guía para realizar el proyecto. No obstante, la norma citada no especifica que metodología se ha de seguir para desarrollar el análisis de riesgos.

Para elaborar el análisis de riesgos se ha escogido la metodología MAGERIT por su reconocimiento a nivel nacional y por ser una de las guías más aceptadas y utilizadas en el ámbito del análisis de riesgos. La herramienta utilizada para este análisis de riesgos ha sido PILAR.

1.4 Introducción del Esquema Nacional de Seguridad

La Seguridad de la Información es ya hoy una realidad y algo que todas las organizaciones deben tener integrado en todos los niveles de su estructura, y principalmente en su dirección, si no quieren quedarse atrás en las medidas de actuación, dentro del sector TIC.

Cualquier empresa o institución debe contar ya con los profesionales y medios adecuados que le permitan dirigir y gestionar con éxito, la seguridad de sus recursos, tanto físicos como lógicos.

Para la administración pública española este proceso, de obligado cumplimiento, implica la adecuación al Esquema Nacional de Seguridad (ENS)

El ENS ayudará a que los ciudadanos puedan desarrollar, a través de medios digitales, gestiones relacionadas con la e-Administración con mayor seguridad y confianza en todos los procesos relacionados con sistemas, datos y comunicaciones electrónicas.

Lo que sin duda supone un impulso al desarrollo de la sociedad de la información.

1.5 Planificación del trabajo

El trabajo se ha estructurado en seis fases, las cuales están establecidas en un margen de tiempo. En la siguiente tabla se puede observar las tareas a realizar en cada fase y el tiempo necesario que se debe dedicar.

Los días necesarios indicados son a tiempo completo, es decir, 8 horas por día establecido.

Fase 1: Situación inicial: Contextualización, objetivos y análisis diferencial
Días necesarios: **5 días** Introducción al Proyecto. Enfoque y selección de la organización que será objeto de estudio. Delimitar el alcance del Esquema Nacional y analizar tanto los servicios como la información.

Fase 2: Análisis diferencial del ENS
Días necesarios: **5 días** Habrá que realizar un análisis diferencial con el fin de determinar qué controles, de los existentes en el ENS ya se encuentran implantados en la organización.

Fase 3: Análisis de riesgos
Días necesarios: **14 días** Elaboración de una metodología de análisis de riesgos mediante MAGERIT: Identificación y valoración de activos, amenazas, vulnerabilidades, cálculo del riesgo, nivel de riesgo aceptable y riesgo residual.

Fase 4: Definición de Plan de adecuación al ENS
Días necesarios: **5 días** Preparación de un Plan de adecuación con las tareas a realizar y los plazos de ejecución para la completa aplicación de lo exigido por el ENS.

Fase 5: Adecuación al ENS
Días necesarios: **15 días** Llevar a cabo todas las tareas para la implantación del ENS en la organización.

Fase 6: Auditoría de conformidad
Días necesarios: **5 días** Esta última fase es realizada por un auditor externo debidamente cualificado que es el que verifica el cumplimiento del ENS en la organización.

2. Contexto del ENS

2.1 Origen

En junio del año 2007 se aprobó la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAESCP) con el objetivo de poder hacer los trámites administrativos por internet. Define el concepto de sede electrónica, que es la dirección electrónica a través de la cual los ciudadanos se conectan para realizar sus trámites administrativos.

Esta finalidad establecida por la Ley 11/2007 debe alcanzarse junto con el requisito de crear las condiciones de confianza en el uso de los medios electrónicos, y por ello las Administraciones Públicas y entidades privadas que presten servicios electrónicos a las mismas deben establecer las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial de los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos. De este modo, se reconoce expresamente que la necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

En este contexto, se entiende por seguridad la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas, que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, o a través de los que se realiza el acceso.

¿Por qué? Porque es de sentido común y de una previsión encomiable, prescribir que un servicio público que va a utilizar masivamente las Tecnologías de la Información y la Comunicación (TICs) tenga que ser seguro para los ciudadanos y compatible tanto con las tecnología que ellos usan como con las que usan las administraciones.

De la misma forma, esta Ley establece seguridad como un derecho de los ciudadanos y una obligación para las AAPP, de forma que se contempla el derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones públicas. Junto con esta figura, esta Ley establece que dichos requisitos de seguridad estén presentes en el tratamiento de la sede electrónica, de las transmisiones de datos entre administraciones, de los registros electrónicos, de las comunicaciones electrónicas, del archivo electrónico de documentos y del procedimiento por medios electrónicos.

El artículo 42 de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos establece la creación del Esquema Nacional de Seguridad (ENS), cuyo objeto es establecer una política de seguridad para la utilización de medios electrónicos en el ámbito de la Administración Pública y que está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Esto se ha materializado 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.

El ENS se ha elaborado 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; así como a la regulación de diferentes Instrumentos y Servicios de la Administración, a las Directrices y Guías de la OCDE y a la normalización en la materia.

Pero esto no es todo ya que también han realizado el contenido del Esquema Nacional de Seguridad con documentos de la Administración en materia de seguridad de tecnologías de la información, tales como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades, las Guías CCN-STIC de Seguridad de los Sistemas de Información y las Comunicaciones.

Junto con lo ya mencionado, la redacción del Esquema Nacional de Seguridad ha tenido presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/EC del Consejo de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos; también se han tenido presentes documentos previos de la Administración en materia de seguridad de los medios electrónicos, informáticos y telemáticos.

Es de importante mención que el artículo 29 del Esquema Nacional de Seguridad indica que: “Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.” De este modo, aunque no se trata de normas imperativas, se aconseja observar las recomendaciones establecidas por las Guías-STIC (ver anexo) a modo de metodologías para el adecuado cumplimiento.

Por lo tanto, el Esquema Nacional de Seguridad establece todas las medidas de seguridad que deben aplicar las Administraciones Públicas en el ámbito de lo dispuesto en la Ley 11/2007, de 22 de junio, así como los plazos en los que las Administraciones Públicas deben adecuar los sistemas existentes al Real Decreto 3/2010, de 8 de enero, siendo necesaria su adecuación antes de 12 meses desde su entrada en vigor, salvo que existan circunstancias que impidan la plena adecuación al ENS.

El objeto de este trabajo es transmitir conocimientos acerca de la seguridad de la información tal y como se entiende en el Esquema Nacional de Seguridad así como proporcionar unas pautas que ayuden en la tarea de la adecuación de una Administración Pública local al Esquema Nacional de Seguridad.

2.2 Principios básicos

El principal objetivo de la seguridad de la información es asegurar que una organización podrá cumplir sus objetivos utilizando sistemas de información. Tal y como estipula el Esquema Nacional de Seguridad, en las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

- Seguridad integral.
- Gestión de riesgos.
- Prevención, reacción y recuperación.
- Líneas de defensa.
- Reevaluación periódica.
- Función diferenciada.

2.2.1 Seguridad integral

Para su correcta efectividad, la gestión de la seguridad debe ser un proceso integral, es decir, que hay que considerar todos los elementos técnicos, los elementos humanos, los materiales y los organizativos, relacionados con el sistema. En el Esquema Nacional de Seguridad no se admiten actuaciones puntuales ni coyunturales.

La formación de todo el personal que tenga algún tipo de responsabilidad en los servicios electrónicos que se prestan es una parte fundamental en la consecución de una gestión integral de la seguridad.

No hay que olvidar que los sistemas son gestionados y operados por personas. Con esto se quiere llegar a la conclusión de que a pesar de tener una implantación de todas las medidas técnicas aplicables, es imposible evitar un error humano o un ataque. La medida preventiva que más efecto tiene en estos casos es la concienciación y la formación.

2.2.2 Gestión de riesgos

Un programa de seguridad tiene cierto sentido en el momento en el que responde a las necesidades de reducción de riesgos de la organización.

La herramienta conocida para realizarlo es el análisis de riesgos y la gestión de riesgos. El análisis de riesgos detectará los problemas de seguridad y los categorizará mientras que la gestión reduce los riesgos a un nivel considerado aceptable mediante la implantación de medidas de seguridad. Como las entidades están en un continuo cambio, por muy pequeño que sea, el análisis de riesgos debe mantenerse actualizado continuamente.

2.2.3 Prevención, reacción y recuperación

No todas las medidas de seguridad del Esquema Nacional de Seguridad están enfocadas a los mismos objetivos. Se pueden diferenciar medidas de prevención, de reacción y de recuperación.

Las medidas de prevención tienen como finalidad evitar en la medida de lo posible que se produzcan eventos o incidentes.

Las medidas de detección (la implantación de un antivirus por ejemplo) sirven para identificar eventos potencialmente peligrosos. Deben existir medidas de reacción (eliminación del virus detectado) que atajen el evento, minimizando de esta forma los daños que hayan podido ocurrir.

Las medidas de recuperación (entre las que se encuentra la realización de copias de seguridad) son las que permiten restablecer la información o los servicios que hayan podido resultar dañados por un incidente de seguridad. Esta recuperación puede ser por completo o de forma parcial pero siempre será mejor una completa recuperación.

La utilización de los tres tipos de medidas nos permitirá un enfoque integro de la seguridad tal y como exige el ENS, evitando incidencias y reduciendo el impacto de aquellas que puedan ocurrir en un futuro.

La necesidad de conservar los datos en soporte electrónico y mantener disponibles los servicios que los utilizan durante todo el ciclo de vida útil son aspectos a considerar. Esta acción se hará habitualmente mediante procedimientos orientados a preservar el patrimonio digital.

2.2.4 Líneas de defensa

El sistema de seguridad debe contener diversas capas de protección para evitar que un incidente sea capaz de desarrollar todo su potencial en caso de que ocurra y pueda provocar una cantidad alta de daños. Las diversas capas pueden estar constituidas por medidas organizativas, física y lógicas. Para ello es necesario que encuentre distintos obstáculos que reduzcan su impacto total en forma de líneas de defensa.

Si por cualquier motivo llegara a ocurrir un incidente, independientemente de la gravedad, las capas de medidas de seguridad deben permitir:

- Reducir el alcance o la amplitud del impacto, evitando que se difunda
- Ganar tiempo para reaccionar, conteniendo el incidente.
- Disminuir lo máximo posible el impacto que puede tener el incidente sobre el sistema.

2.2.5 Reevaluación periòdica

De la misma forma que la evaluación de riesgos debe estar actualizada para que cumpla eficazmente con su función de detectar peligros potenciales para el sistema, habría que hacer lo mismo con las medidas de seguridad mediante una revisión. La revisión de las medidas de seguridad sirve para verificar que siguen siendo las adecuadas a los riesgos detectados y que mantienen su eficacia protegiendo el sistema contra ellos.

Mediante esta revisión se puede llegar a la conclusión de que hay que añadir más controles, mejorar los existentes o incluso reorganizar por completo el conjunto de controles aplicados. Esta revisión debe ser continua y la organización debe de conocer su importancia.

2.2.6 Función diferenciada

En cualquier marco de trabajo de seguridad es imprescindible mantener una separación de responsabilidades que evite conflictos de interés que puedan ir en detrimento de la seguridad. El Esquema Nacional de Seguridad estipula que las funciones de responsable de la información, responsable del servicio y responsable de la seguridad deben estar separadas.

El responsable de la información es quien conoce el uso que se le debe dar a dicha información por lo que es la persona más apropiada para definir los requisitos de seguridad de la información tratada.

El responsable del servicio es quien conoce la problemática de dicho servicio y las condiciones en la que se puede y debe prestar, por lo que es el indicado para determinar los requisitos de seguridad de los servicios prestados.

Por último, el responsable de seguridad es quien está al tanto de la visión general de los sistemas, datos y riesgos a los que están expuestos, por lo que es la personal que puede tomar con más conocimiento de causa las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2.3 Ámbito de aplicación

El Esquema Nacional de Seguridad (ENS), es de obligado cumplimiento para el conjunto de la administración española, entendiendo por tal la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.

Esto incluye, además de ministerios, consejerías autonómicas, corporaciones municipales, otras entidades tales como:

- Las Universidades, en cuanto a organismos autónomos de la administración.
- Autoridades Portuarias y aeroportuarias.
- A las entidades públicas tipo Institutos de Desarrollo Económico, Servicios de Salud, etc.

La Administración de Justicia no está obligada por la Ley 11/2007, ni por lo tanto por el ENS. Sin embargo cuentan con un programa de actuación, denominado Esquema Judicial de Interoperabilidad y Seguridad (EJIS), suscrito por las Instituciones con responsabilidades en la Administración de Justicia (Ministerio de Justicia, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Comunidades Autónomas con competencias transferidas). El EJIS es un marco de colaboración para colegiar esfuerzos y cuyos objetivos fundamentales son la prestación de los servicios de Administración de Justicia bajo el paradigma de la interoperabilidad, accesibilidad, reusabilidad y seguridad.

Esta norma aplica a todos los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de medios electrónicos.

Están excluidos los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

Tampoco aplica a las administraciones en las actividades que desarrollen en régimen de derecho privado.

Se daban doce meses de plazo tras la entrada en vigor del Esquema Nacional de Seguridad para aplicarlo en los servicios que se prestaban en ese momento. Cuando no es posible hacerlo por cualquier circunstancia, hay que preparar un plan de adecuación, con las tareas a realizar para la completa aplicación de lo exigido por el ENS a lo largo de un plazo que no puede ser superior a 48 meses desde la entrada en

vigor del mismo. Actualmente nos encontramos con la problemática de que muchas AAPP no han cumplido estos plazos.

3. Fase 1: Situación inicial

3.1 Introducción

El incremento exponencial del uso de las nuevas tecnologías en las organizaciones, y la cada vez mayor dependencia de los sistemas de información, hacen que los procesos de negocio de una empresa dependan en gran medida de la disponibilidad de sus sistemas de información, y de la integridad y confidencialidad de los datos que éstos gestionan. Así, se definen los cinco pilares sobre los que se basa la seguridad de los sistemas de información:

- **Disponibilidad**: debemos tener garantías de que la información va a estar disponible en el momento en que se necesita.
- **Integridad**: características consistente en que el activo de información no ha sido alterado sin autorización.
- **Confidencialidad**: debemos tener garantías de que sólo las personas autorizadas disponen de acceso a la información. Esta información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Trazabilidad**: característica consistente en que una acción pueda ser imputada exclusivamente a una entidad.
- **Autenticidad**: característica consistente en que una entidad garantiza la fuente de la que proceden los datos.

Con idea de incrementar la eficacia de la seguridad, las organizaciones deben valorar la seguridad de sus sistemas de información desde un enfoque global, que tenga en cuenta no sólo aspectos técnicos, sino también físicos, organizativos e incluso legales. El conocimiento del estado de la seguridad de la información bajo este prisma global como paso previo a iniciativas específicas, permite a las organizaciones conocer su estado inicial en materia de seguridad, paso imprescindible para ordenar, con conocimiento de causa, las acciones futuras en relación a esta materia.

Una vez alcanzados los niveles objetivo en seguridad de la información, hay que tener presente que la seguridad es un proceso continuo, no un proyecto o un producto, un proceso continuado en el tiempo que como tal, necesita de una gestión.

En este sentido, la implantación del Esquema Nacional de Seguridad introduce el concepto de mejora continua (entre otros), garantizando tanto el mantenimiento en el tiempo de los niveles de seguridad establecidos en una organización determinada como el incremento paulatino de los mismos.

3.2 Caso de estudio

El Ayuntamiento de Invernalia lleva varios años con la intención de modernizar el Municipio, y el equipo que gestiona el consistorio siempre ha tenido claro que las Tecnologías de la Información y la Comunicación eran las herramientas para conseguirlo.

Existe un grupo de Informática, formado por un responsable de Sistemas, Raúl y un técnico, Maite. Diversas tareas están subcontratadas. El grupo cuenta con una pequeña oficina en el Ayuntamiento, donde trabajan Raúl y Maite, así como un cuarto en el sótano en el que han ubicado el CPD.

Hace dos años lanzaron la página Web del Ayuntamiento. Esta primera página era informativa, pero ya tenía un Buzón del Ciudadano con una dirección de correo electrónico para que los ciudadanos expresaran sus quejas, sugerencias e incluso llegó alguna que otra felicitación.

Hace un año se pusieron en marcha los dos primeros servicios, peticiones de licencias de obra y certificados de empadronamiento.

Para ello se compró un nuevo servidor que albergara inicialmente estos dos servicios y tuviera capacidad para los que vinieran más adelante.

Las aplicaciones utilizadas son desarrollos a medida:

- InvernaliaGestión, para la gestión de expedientes municipales, entre ellos la concesión de licencias de obra.
- InvernaliaPadrón, para la gestión del padrón municipal (altas, bajas y modificaciones).

El mapa de red quedaría de la siguiente forma.

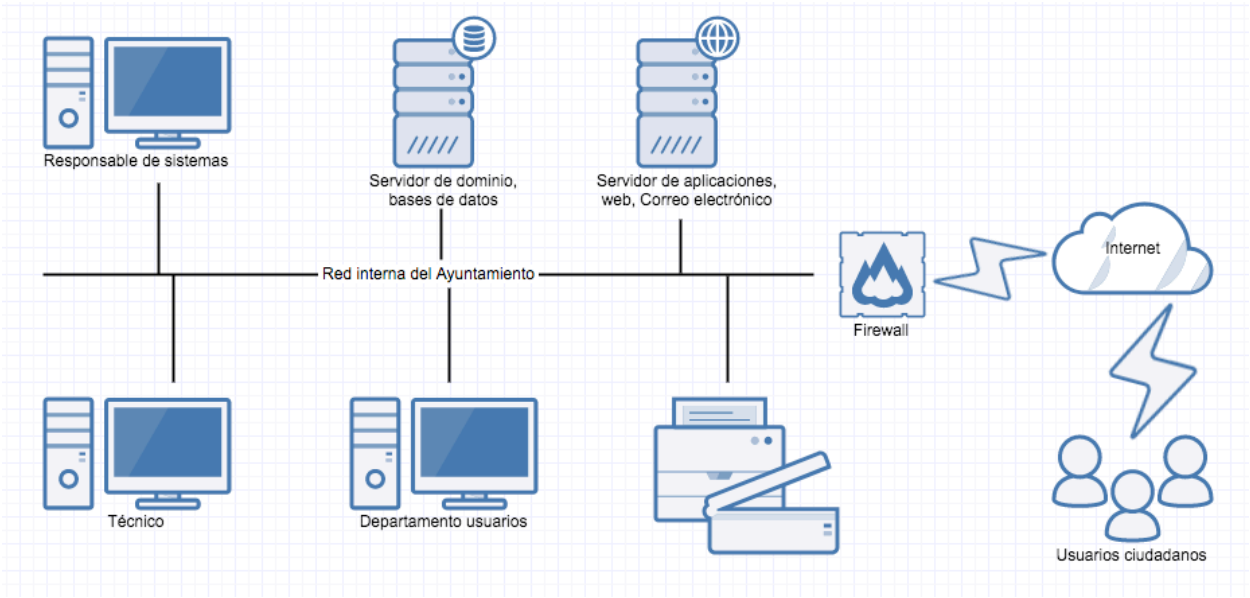


Ilustración 1: Mapa de red

Creo necesario advertir que por motivos didácticos/ilustrativos el caso de estudio se refiere a un modelo sencillo, sin tener en cuenta la complejidad del tratamiento de la información que realizan hoy en día los Ayuntamientos, puesto que están encargados de gestionar numerosos servicios, algunos de ellos serían categorizados como categorías especiales de datos en el RGPD (por ejemplo, los servicios sociales que prestan).

3.3 Alcance del Esquema Nacional de Seguridad

El alcance de los trabajos realizados ha comprendido la realización de un Plan de Adecuación respecto al 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 reflejado en el presente informe.

El trabajo ha cubierto todos los departamentos y personal de la Entidad en el ámbito de los servicios prestados de la Administración Electrónica por parte del Ayuntamiento a los ciudadanos, y se ha circunscrito a las instalaciones de la sede central del Ayuntamiento.

3.4 Análisis de servicio / información

El Ayuntamiento de Invernalia a raíz de los cambios producidos recientemente ofrece tres tipos de servicios que serán en los que habrá que implementar el Esquema Nacional de Seguridad.

El primer servicio es el del portal web donde ofrece información a los ciudadanos pero también contiene una dirección de correo electrónico. Esta dirección de correo electrónico básicamente se utiliza para quejas, sugerencias o cualquier otro aspecto que se quiera comentar.

El segundo servicio hace referencia a la gestión de expedientes en lo que respecta a peticiones de licencias de obra. Este servicio se lleva a cabo mediante una aplicación llamada InvernaliaGestión.

El tercer servicio tiene relación con la otra aplicación denominada InvernaliaPadrón, donde se lleva la gestión del padrón municipal de los ciudadanos. Estamos hablando de altas, bajas o modificaciones.

Evidentemente estos servicios generan una información importante para el ayuntamiento que también hay que proteger. Estamos hablando de la información web, los expedientes, las licencias de obra y los datos del padrón.

3.5 Categorización de sistemas

El sistema se ha categorizado valorando los parámetros de confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad, según los criterios definidos. La escala utilizada para cada valor es la establecida en la guía CCN-STIC-803 del ENS.

Confidencialidad

Valor	Escala
Alto	Porque la información debe conocerla un número muy reducido de personas. Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría un grave daño, de difícil o imposible reparación. Porque su revelación supondría el incumplimiento grave de una norma. Porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas masivas (alteración seria del orden público).
Medio	Porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita. Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría un daño importante aunque subsanable. Porque su revelación supondría el incumplimiento material o formal de una norma. Porque su revelación causaría pérdidas económicas importantes. Porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas públicas (alteración del orden público).
Bajo	Porque la información no deben conocerla personas ajenas a la organización. Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque su revelación causaría algún perjuicio. Porque su revelación supondría el incumplimiento leve de una norma. Porque su revelación supondría pérdidas económicas apreciables. Porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en múltiples protestas individuales.
Sin Valorar	Información de carácter público, accesible por cualquier persona.

Integridad	
Valor	**Escala**
Alto	Por disposición legal o administrativa: ley, decreto, orden,… Porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación. Porque su manipulación o modificación no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque su manipulación o modificación no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en protestas masivas (alteración seria del orden público).
Medio	Por disposición legal o administrativa: ley, decreto, orden,… Porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable. Porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma. Porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes. Porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público).
Bajo	Por disposición legal o administrativa: ley, decreto, orden,… Porque su manipulación o modificación no autorizada causaría algún perjuicio. Porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma. Porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables. Porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales.

Autenticidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden,… Porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación. Porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas. Porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración seria del orden público).
Medio	Por disposición legal o administrativa: ley, decreto, orden,… Porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable. Porque la falsedad en su origen o en su destinatario supondría el incumplimiento material o formal de una norma. Porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes. Porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público).
Bajo	Por disposición legal o administrativa: ley, decreto, orden,… Porque la falsedad en su origen o en su destinatario causaría algún perjuicio. Porque la falsedad en su origen o en su destinatario supondría el incumplimiento leve de una norma. Porque la falsedad en su origen o en su destinatario supondría pérdidas económicas apreciables. Porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales.
Sin Valorar	Cuando el origen es irrelevante o ampliamente conocido por otros medios. Cuando el destinatario es irrelevante, por ejemplo por tratarse de información de difusión anónima.

Trazabilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden,… Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error grave. Porque la incapacidad para rastrear un acceso a la información impediría la capacidad para perseguir delitos. Porque la incapacidad para rastrear un acceso a la información facilitaría enormemente la comisión de delitos graves.
Medio	Por disposición legal o administrativa: ley, decreto, orden,… Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad de subsanar un error grave. Porque la incapacidad para rastrear un acceso a la información impediría la capacidad de subsanar un error importante. Porque la incapacidad para rastrear un acceso a la información dificultaría gravemente la capacidad para perseguir delitos. Porque la incapacidad para rastrear un acceso a la información facilitaría la comisión de delitos.
Bajo	Por disposición legal o administrativa: ley, decreto, orden,… Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores. Porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad para perseguir delitos.
Sin Valorar	Cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios. Cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios

Disponibilidad

Valor	Escala
Alto	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible reparación. Porque la indisponibilidad de la información supondría el incumplimiento grave de una norma. Porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones. Porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público). Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es inferior a 4 horas.
Medio	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría un daño importante aunque subsanable. Porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma. Porque la indisponibilidad de la información causaría un daño reputacional importante con los ciudadanos o con otras organizaciones. Porque su revelación podría desembocar en protestas públicas (alteración del orden público). Cuando el RTO (tiempo máximo que el servicio puede permanecer interrumpido) es de entre 4 y 24 horas (un día).
Bajo	Por disposición legal o administrativa: ley, decreto, orden, reglamento,… Porque la indisponibilidad de la información causaría algún perjuicio. Porque la indisponibilidad de la información supondría el incumplimiento leve de una norma. Porque la indisponibilidad de la información supondría pérdidas económicas apreciables. Porque la indisponibilidad de la información causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones. Porque la indisponibilidad de la información podría desembocar en múltiples protestas individuales. Cuando el RTO se sitúa entre 1 y 5 días (una semana).
Sin Valorar	Cuando la información es prescindible por tiempo indefinido. Cuando el RTO es superior a 5 días laborables (una semana).

Se detallan a continuación las valoraciones de cada uno de los activos esenciales, que son los correspondientes a los Servicios (de administración electrónica) e Información.

Como establece el Esquema Nacional de Seguridad, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio. Consecuentemente, la categoría del Sistema viene dada por el valor máximo en cada parámetro.

ID	Activo	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	Servicios					
S1	Portal Web	M	B	Sin valorar	B	B
S2	Gestión de expedientes	B	M	M	M	M
S3	Padrón	B	M	M	M	M
	Información					
I1	Información web	M	B	B	B	B
I2	Expedientes	M	M	M	M	M
I3	Licencias	B	M	B	M	M
I4	Datos del padrón	B	M	M	M	M
	Sistema	M	M	M	M	M

La categoría del Sistema es Media, por lo que a estos activos se les aplicará como mínimo aquellas medidas de seguridad estipuladas para este nivel en el Anexo II, Medidas de Seguridad, del ENS.

3.6 Valoración de los activos

También es necesaria una valoración de los activos que no pertenecen ni a servicios ni a información pero que tienen una dependencia de estos. La valoración de los activos que pertenecen a hardware, a software, al personal o a las instalaciones, es la heredada de los activos de tipo servicio e información. La siguiente tabla indica la valoración de los activos teniendo en cuenta las dependencias significativas.

ID	Activo	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	Hardware					
HW01	Servidor Web	M	M	M	M	M
HW02	Servidor e-administración	M	M	M	M	M
HW03	Red Lan	M	M	M	M	M
HW04	Periféricos	M	M	M	M	M
HW05	Equipos de usuario	M	M	M	M	M
HW06	Red DMZ	M	M	M	M	M
	Software					
SW01	Aplicación Web	M	M	M	M	M
SW02	InvernaliaGestión	M	M	M	M	M
SW03	InvernaliaPadron	M	M	M	M	M

ID	Activo	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
	Personal					
P01	Personal del Ayuntamiento	M	M	M	M	M
P02	Personal subcontratado	M	M	M	M	M
	Instalaciones					
IN01	CPD	M	M	M	M	M
IN02	Oficinas del Ayuntamiento	M	M	M	M	M

4. Fase 2: Análisis diferencial ENS

4.1 Introducción

A pesar de dejar bien establecido el alcance, uno de los pasos más importantes antes de iniciar la implantación del Esquema Nacional de Seguridad en una organización, es conocer el estado inicial de la misma según los requerimientos descritos en el anexo II.

El análisis diferencial nos permite obtener el nivel en el que se encuentra una organización en torno a la seguridad de la información y de esta forma se obtiene una definición más precisa del alcance. Es el mejor método de conocer el estado actual de la organización porque se hace un análisis individual de cada medida de seguridad. Con el análisis diferencial se conocen las diferencias entre el modelo de seguridad actual de la organización y el propuesto por el ENS.

En la organización que nos ocupa, se podría decir que el nivel de implantación del Esquema Nacional de seguridad es inmaduro en varios aspectos.

4.2 Análisis diferencial

Medida de seguridad		Aplicación	Descripción	Nivel
Marco Organizativo	org			
Política de seguridad	org.1	M	Política de seguridad aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11.	L2
Normativa de seguridad	org.2	M	Se dispone de una serie de documentos que describen: -Uso correcto de equipos, servicios e instalaciones. -Lo considerado como uso indebido. -La responsabilidad del personal con respecto al cumplimento o violación de las normas:	L2
Procedimientos de seguridad	org.3	M	Serie de documentos que detallen: -Cómo llevar a cabo las tareas habituales. -Quien debe hacer cada tarea. -Como reportar comportamientos anómalos	L1
Proceso de autorización	org.4	M	Proceso formal de autorizaciones que cubre lo siguiente: -Utilización de instalaciones. -Entrada de equipos en producción. -Entrada de aplicaciones en producción. -Establecimiento de enlaces de	L1

Medida de seguridad		Aplicación	Descripción	Nivel
			comunicaciones con otros sistemas. -Utilización de medios de comunicación, habituales y alternativos. -Utilización de equipos móviles y servicios de terceros.	
Marco operacional	op			
Planificación	op.pl			
Análisis de riesgos	op.pl.1	M	Análisis semi-formal con lenguaje específico con un catálogo básico de amenazas y una semántica definida.	L3
Arquitectura de seguridad	op.pl.2	M	Será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos: -Documentación de las instalaciones. -Documentación del sistema. -Esquema de líneas de defensa. -Sistema de identificación y autenticación de usuarios. -Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.	L3
Adquisición de nuevos componentes	op.pl.3	M	Proceso formal para planificar la adquisición de nuevos	L4

Medida de seguridad		Aplicación	Descripción	Nivel
			componentes del sistema. Este proceso atiende las conclusiones del análisis de riesgos, es acorde a la arquitectura de seguridad escogida y contempla las necesidades técnicas, de formación y de financiación.	
Dimensionamiento/Gestión de capacidades	op.pl.4	M	Se realiza un estudio que cubra las necesidades de procesamiento, las necesidades de almacenamiento de información, las necesidades de comunicación y las necesidades de personal.	L2
Componentes certificados	op.pl.5	n.a.		
Control de acceso	op.acc			
Identificación	op.acc.1	M	En la identificación de los usuarios se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación. Cuando el usuario tenga diferentes roles recibirá identificadores singulares para cada uno de los casos de forma que siempre queden delimitados privilegios y registros de actividad. Cada entidad contará con un identificador singular.	L4

Medida de seguridad		Aplicación	Descripción	Nivel
Requisitos de acceso	op.acc.2	M	Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo las entidades que disfruten de derechos de acceso suficientes. Se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.	L3
Segregación de funciones y tareas	op.acc.3	M	El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar al menos las siguientes funciones.	L1
Proceso de gestión de derechos de acceso	op.acc.4	M	Los derechos de acceso de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. Los usuarios solo podrán acceder al conocimiento de aquella información requerida.	L4
Mecanismo de autenticación	op.acc.5	M	Se exige el uso de al menos dos factores de autenticación. Se establecerán exigencias rigurosas de calidad y renovación en el caso de utilizarse un factor de autenticación sabido.	L3

Medida de seguridad		Aplicación	Descripción	Nivel
Acceso local (local login)	op.acc.6	M	En el acceso local se informará al usuario del último acceso efectuado con su identidad, el número de intentos permitidos será limitado, se registrará cualquier intento de acceso y el sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.	L5
Acceso remoto (remote login)	op.acc.7	M	Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades y se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.	L5
Explotación	op.exp			
Inventario de activos	op.exp.1	M	Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable.	L5
Configuración de seguridad	op.exp.2	M	Se configurarán los equipos previamente a su entrada en operación, de forma que: -Se retiren cuentas y contraseñas estándar. -Se aplicará la regla de <<mínima	L4

Medida de seguridad		Aplicación	Descripción	Nivel
			funcionalidad>>: -Se aplicará la regla de <<seguridad por defecto>>	
Gestión de la configuración	op.exp.3	M	Se gestionará de forma continua la configuración de los componentes del sistema de forma que: -Se mantenga en todo momento la regla de “funcionalidad mínima” y de “seguridad por defecto”. -El sistema se adapte a las nuevas necesidades, previamente autorizadas. -El sistema reaccione a vulnerabilidades reportadas. -El sistema reaccione a incidentes.	L4
Mantenimiento	op.exp.4	M	Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas. Se efectuará un seguimiento continuo de los anuncios de defectos.	L3
Gestión de cambios	op.exp.5	M	Se mantendrá un control continuo de cambios realizados por el fabricante o proveedor para determinar su conveniencia para ser incorporados. Antes de poner en producción una nueva versión se probará en un equipo que no esté en producción. Mediante análisis de riesgos se determinará si los	L2

Medida de seguridad		Aplicación	Descripción	Nivel
			cambios son relevantes.	
Protección frente a código dañino	op.exp.6	M	Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.	L3
Gestión de incidentes	op.exp.7	M	Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema	L2
Registro de la actividad de los usuarios	op.exp.8	M	Se registrarán las actividades de los usuarios en el sistema de forma que el registro indique quien realiza la actividad, cuando lo hace y sobre qué información. Se revisarán informalmente los registros de actividad buscando patrones anormales.	L4
Registro de la gestión de incidentes	op.exp.9	M	Se registrarán todas las actuaciones relacionadas con la gestión de incidentes. Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente. Se revisará la determinación de los eventos auditables. Se registrará aquella evidencia que pueda sustentar una demanda judicial o hacer frente a ella.	L2

Medida de seguridad		Aplicación	Descripción	Nivel
Protección de los registros de actividad	op.exp.10	n.a.		
Protección de claves criptográficas	op.exp.11	M	Las claves criptográficas se protegerán durante todo su ciclo de vida. Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5]. Se emplearán algoritmos acreditados por el CCN.	L3
Servicios externos	op.ext			
Contratación y acuerdos de nivel de servicio	op.ext.1	M	Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.	L4
Gestión diaria	op.ext.2	M	Para la gestión diaria del sistema, se establecerán los siguientes puntos: -Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen. -El mecanismo y los procedimientos de coordinación para llevar	L2

Medida de seguridad		Aplicación	Descripción	Nivel
			a cabo las tareas de mantenimiento de los sistemas afectados.	
Medios alternativos	op.ext.9	n.a.		
Continuidad del servicio	op.cont			
Análisis de impacto	op.cont.1	M	Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.	L3
Plan de continuidad	op.cont.2	n.a.		
Pruebas periódicas	op.cont.3	n.a.		
Monitorización del sistema	op.mon			
Detección de intrusión	op.mon.1	M	Se dispondrá de herramientas de detección o de prevención de intrusión.	L2
Sistema de métricas	op.mon.2	M	Se dispondrá de herramientas de detección o de prevención de intrusión.	L2
Medidas de protección	mp			
Protección de las instalaciones e infraestructuras	mp.if			
Áreas separadas y con control de acceso	mp.if.1	M	El equipamiento se instalará en áreas separadas específicas para su función. Se controlarán los accesos a las áreas indicadas de	L4

Medida de seguridad		Aplicación	Descripción	Nivel
			forma que sólo se pueda acceder por las entradas previstas y vigiladas.	
Identificación de las personas	mp.if.2	M	El mecanismo de control de acceso se atendrá a lo que se dispone a continuación: -Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.	L5
Acondicionamiento de los locales	mp.if.3	M	Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, teniendo en cuenta la temperatura, humedad, las amenazas detectadas en el análisis de riesgos y la protección del cableado.	L4
Energía eléctrica	mp.if.4	M	Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.	L5
Protección frente a incendios	mp.if.5	M	Los locales donde se ubiquen los sistemas de	L5

Medida de seguridad		Aplicación	Descripción	Nivel
			información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.	
Protección frente a inundaciones	mp.if.6	M	Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.	L4
Registro de entrada y salida de equipamiento	mp.if.7	M	Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.	L3
Instalaciones alternativas	mp.if.9	n.a.		
Gestión del personal	mp.per			
Caracterización del puesto de trabajo	mp.per.1	M	En cada puesto de trabajo se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto.	L3

Medida de seguridad		Aplicación	Descripción	Nivel
Deberes y obligaciones	mp.per.2	M	Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.	L3
Concienciación	mp.per.3	M	Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel	L1
Formación	mp.per.4	M	Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a configuración de sistemas, detección y reacción de incidentes y gestión de la información en cualquier soporte en el que se encuentre.	L1
Personal alternativo	mp.per.9	n.a.		
Protección de los equipos	mp.eq			
Puesto de trabajo despejado	mp.eq.1	M	Se exigirá que los puestos de trabajo permanezcan despejados y que el material requerido esté guardado en un lugar cerrado cuando no se utilice.	L2
Bloqueo de puesto de trabajo	mp.eq.2	M	El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en	L5

Medida de seguridad		Aplicación	Descripción	Nivel
			curso.	
Protección de equipos portátiles	mp.eq.3	M	Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.	L3
Medios alternativos	mp.eq.9	M	Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.	L2
Protección de las comunicaciones	mp.com			
Perímetro seguro	mp.com.1	M	Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que solo dejará transitar los flujos previamente autorizados.	L4
Protección de la confidencialidad	mp.com.2	M	Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. Se emplearán algoritmos	L3

Medida de seguridad		Aplicación	Descripción	Nivel
			acreditados por el CCN.	
Protección de la autenticidad y de la integridad	mp.com.3	M	Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad. Se emplearán algoritmos acreditados por el CCN. Se aceptará cualquier mecanismo de autenticación de los previstos en la normativa de aplicación.	L3
Segregación de redes	mp.com.4	n.a.		
Medios alternativos	mp.com.9	n.a.		
Protección de los soportes de información	mp.si			
Etiquetado	mp.si.1	M	Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.	L2
Criptografía	mp.si.2	M	Se aplicarán mecanismos criptográficos a todos los dispositivos móviles de forma que garanticen la confidencialidad y la integridad de la información contenida.	L1
Custodia	mp.si.3	M	Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización.	L3

Medida de seguridad		Aplicación	Descripción	Nivel
Transporte	mp.si.4	M	El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados.	L4
Borrado y destrucción	mp.si.5	M	La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.	L5
Protección de las aplicaciones informáticas	mp.sw			
Desarrollo	mp.sw.1	M	El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción. Se aplicará una metodología de desarrollo reconocida.	L1
Aceptación y puesta en servicio	mp.sw.2	M	Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se realizará un análisis de vulnerabilidades y pruebas de penetración previas a la entrada en servicio.	L1
Protección de la información	mp.info			
Datos de carácter personal	mp.info.1	M	Cuando el sistema trate datos de carácter personal, se estará a lo dispuesto en la Ley	L4

Medida de seguridad		Aplicación	Descripción	Nivel
			Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto.	
Calificación de la información	mp.info.2	M	Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere.	L4
Cifrado	mp.info.3	n.a.		
Firma electrónica	mp.info.4	M	Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio. -Se emplearán algoritmos y parámetros acreditados por el CNN. -Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella soporte.	L4
Sellos de tiempo	mp.info.5	n.a.		
Limpieza de documentos	mp.info.6	M	En el proceso de limpieza de documentos, se retirará	L2

Medida de seguridad		Aplicación	Descripción	Nivel
			de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.	
Copias de seguridad (backup)	mp.info.9	M	Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada. Estas copias deberán abarcar: -Información de trabajo de la organización. -Aplicaciones en explotación, incluyendo los sistemas operativos. -Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga. -Claves utilizadas para preservar la confidencialidad de la información.	L4
Protección de los servicios	mp.s			
Protección del correo electrónico	mp.s.1	M	El correo electrónico se protegerá frente a las amenazas que le son propias. -La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos. -Se protegerá la información de encaminamiento de mensajes y	L5

Medida de seguridad		Aplicación	Descripción	Nivel
			establecimiento de conexiones. -Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico. -Se establecerán normas de uso del correo electrónico por parte del personal determinado.	
Protección de servicios y aplicaciones web	mp.s.2	M	Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias. Se emplearán “certificados de autenticación de sitio web” acordes a la normativa europea en la materia.	L3
Protección frente a la denegación de servicio	mp.s.8	M	Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service).	L3
Medios alternativos	mp.s.9	n.a.		

5. Fase 3: Análisis de riesgos

5.1 Introducción

Para realizar un análisis de Riesgos se debe partir de un inventario de los activos involucrados en la prestación de los servicios de administración electrónica. Habitualmente se consideran los siguientes tipos de activos:

- Hardware, equipos necesarios para la prestación de los servicios identificados.

- Software, aplicaciones utilizadas en la prestación de los servicios identificados.

- Personal, personal involucrado en la prestación de los servicios identificados.

- Instalaciones, ubicaciones, edificios u oficinas utilizadas durante la prestación de los servicios identificados.

Estos activos reciben la valoración de los servicios e información que dependen de ellos.

Tras la valoración, deben considerarse:

- las amenazas que pueden afectar a esos activos.
- la frecuencia de ocurrencia de esas amenazas.

Con estos datos, se obtendrá un informe de las diferentes amenazas, vulnerabilidades e impactos que podrían producirse en los sistemas de información de la entidad. Es decir, se consigue una valoración del riesgo inicial, es decir del riesgo latente de los activos si no estuvieran protegidos.

La siguiente tarea del análisis de riesgos será la valoración de la madurez de las medidas de seguridad que se hayan implantadas actualmente para proteger los activos. Hay cinco niveles:

Nivel	Significado	Descripción
n.a.	No es aplicable	
L0	Inexistente	En el nivel L0 de madurez no hay nada.
L1	Inicial / ad hoc	Las medidas de seguridad existen, pero no se gestionan. El éxito depende de buena suerte. En este caso, las entidades exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel L1 depende de tener personal de la alta calidad.
L2	Reproducible, pero intuitivo	La eficacia de las medidas de seguridad depende de la buena suerte y de la buena voluntad de las personas. Los éxitos son repetibles, pero no hay plan para los incidentes más allá de la reacción a los hechos. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
L3	Proceso definido	Se despliegan y se gestionan las medidas de seguridad. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es consecuencia del trabajo consciente y riguroso.
L4	Gestionado y medible	Usando medidas de campo, la dirección puede controlar empíricamente la eficacia y la efectividad de las medidas de seguridad. En particular, la dirección puede fijar metas cuantitativas de la calidad. En el nivel L4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza es cuantitativa, 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 de los procesos 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.

5.2 Metodología MAGERIT

La metodología Magerit, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del “Ministerio de Administraciones Públicas”, cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada.

En primer lugar, el análisis de riesgos permite conocer el sistema: sus activos, su valor, y las amenazas a las que está expuesto. Tras este análisis, el tratamiento de riesgos se centra en seleccionar medidas de seguridad para conjurar las amenazas. Por último, la gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

Para el Análisis de riesgos se identifican los Activos de la entidad. Estos activos están expuestos a una serie de Amenazas que, cuando ocurren, degradan el valor del activo, causando un cierto Impacto.

La metodología propone una serie de Amenazas que afectan directa o indirectamente al Activo según su tipo. Si estimamos la probabilidad de la amenaza, podemos concluir el Riesgo en el sistema, o la pérdida a la cual está expuesto.

La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza. Para la gestión de riesgos se seleccionan las salvaguardas para hacer frente a las amenazas, así como el nivel al que están aplicadas o el nivel objetivo que se pretende alcanzar.

Las salvaguardas mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores residuales, que deberán ser asumidos por la Entidad o mitigados de nuevo hasta un nivel aceptable.

5.3 Análisis de riesgos con la aplicación PILAR

La herramienta PILAR soporta el análisis y el tratamiento de riesgos de un sistema de información siguiendo la metodología Magerit v3. Esta herramienta está desarrollada y financiada de forma parcial por el CCN (Centro Criptológico Nacional). Existen diversas versiones de la herramienta Pilar:

- Pilar: versión integra
- Pilar basic: versión más sencilla para Pymes y Administración local.
- µPilar: versión de Pilar reducida, se utiliza para realizar un análisis de riesgos de forma rápida.

Todas las versiones están disponibles online (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html) tanto para Windows, Mac como Unix. Todas las versiones están disponibles tanto para la ISO 27000 como para el ENS.

Una vez identificados los activos que pertenecen a los servicios y a la información e dichos servicios se debe evaluar mediante la tabla indicada en la metodología del análisis de riesgos.

Para los servicios se valora la disponibilidad, la autenticidad y la trazabilidad. En cambio, en los datos empleados para que se lleven a cabo los servicios, se valora la integridad y la confidencialidad de los mismos.

Activos esenciales

dimensión	[D]	[I]	[C]	[A]	[T]	[V]
[1234] Proyecto	[M]	[M]	[M]	[M]	[M]	
Activos esenciales						
S [S1] Portal Web	[M]			[B]	[B]	
S [S2] Gestión de expedientes	[B]			[M]	[M]	
S [S3] Padrón	[B]			[M]	[M]	
I [I1] Información web		[B]	[B]	[B]	[B]	
I [I2] Expedientes		[M]	[M]	[M]	[M]	
I [I3] Licencias		[M]	[B]	[M]	[M]	
I [I4] Datos del padrón		[M]	[M]	[M]	[M]	

Ilustración 2 Valoración de los servicios e información

Para el presente análisis de riesgos se ha utilizado la versión de µPilar y se ha obtenido el riesgo potencial y el riesgo actual. El primero hace referencia al riesgo que habría sin aplicar medidas de seguridad, y el segundo, con las medidas de seguridad en el nivel actual.

Análisis de riesgos potencial:

riesgos

potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	{4,2}	{4,2}	{4,6}	{4,2}	{4,5}	
[S1] Portal Web	{4,2}			{2,5}	{2,7}	
[D] disponibilidad	{4,2}					
[A] autenticidad de los usuarios y de la información				{2,5}		
[T] trazabilidad del servicio y de los datos					{2,7}	
[S2] Gestión de expedientes	{2,4}			{4,2}	{4,5}	
[D] disponibilidad	{2,4}					
[A] autenticidad de los usuarios y de la información				{4,2}		
[T] trazabilidad del servicio y de los datos					{4,5}	
[S3] Padrón	{2,4}			{4,2}	{4,5}	
[D] disponibilidad	{2,4}					
[A] autenticidad de los usuarios y de la información				{4,2}		
[T] trazabilidad del servicio y de los datos					{4,5}	
[I1] Información web		{2,5}	{2,8}	{2,5}	{2,7}	
[I] integridad de los datos		{2,5}				
[C] confidencialidad de los datos			{2,8}			
[A] autenticidad de los usuarios y de la información				{2,5}		
[T] trazabilidad del servicio y de los datos					{2,7}	
[I2] Expedientes		{4,2}	{4,6}	{4,2}	{4,5}	
[I] integridad de los datos		{4,2}				
[C] confidencialidad de los datos			{4,6}			
[A] autenticidad de los usuarios y de la información				{4,2}		
[T] trazabilidad del servicio y de los datos					{4,5}	
[I3] Licencias		{4,2}	{2,8}	{4,2}	{4,5}	
[I] integridad de los datos		{4,2}				
[C] confidencialidad de los datos			{2,8}			
[A] autenticidad de los usuarios y de la información				{4,2}		
[T] trazabilidad del servicio y de los datos					{4,5}	
[I4] Datos del padrón		{4,2}	{4,6}	{4,2}	{4,5}	
[I] integridad de los datos		{4,2}				
[C] confidencialidad de los datos			{4,6}			
[A] autenticidad de los usuarios y de la información				{4,2}		
[T] trazabilidad del servicio y de los datos					{4,5}	

Ilustración 3: Análisis de riesgos potencial

Análisis de riesgos actual:

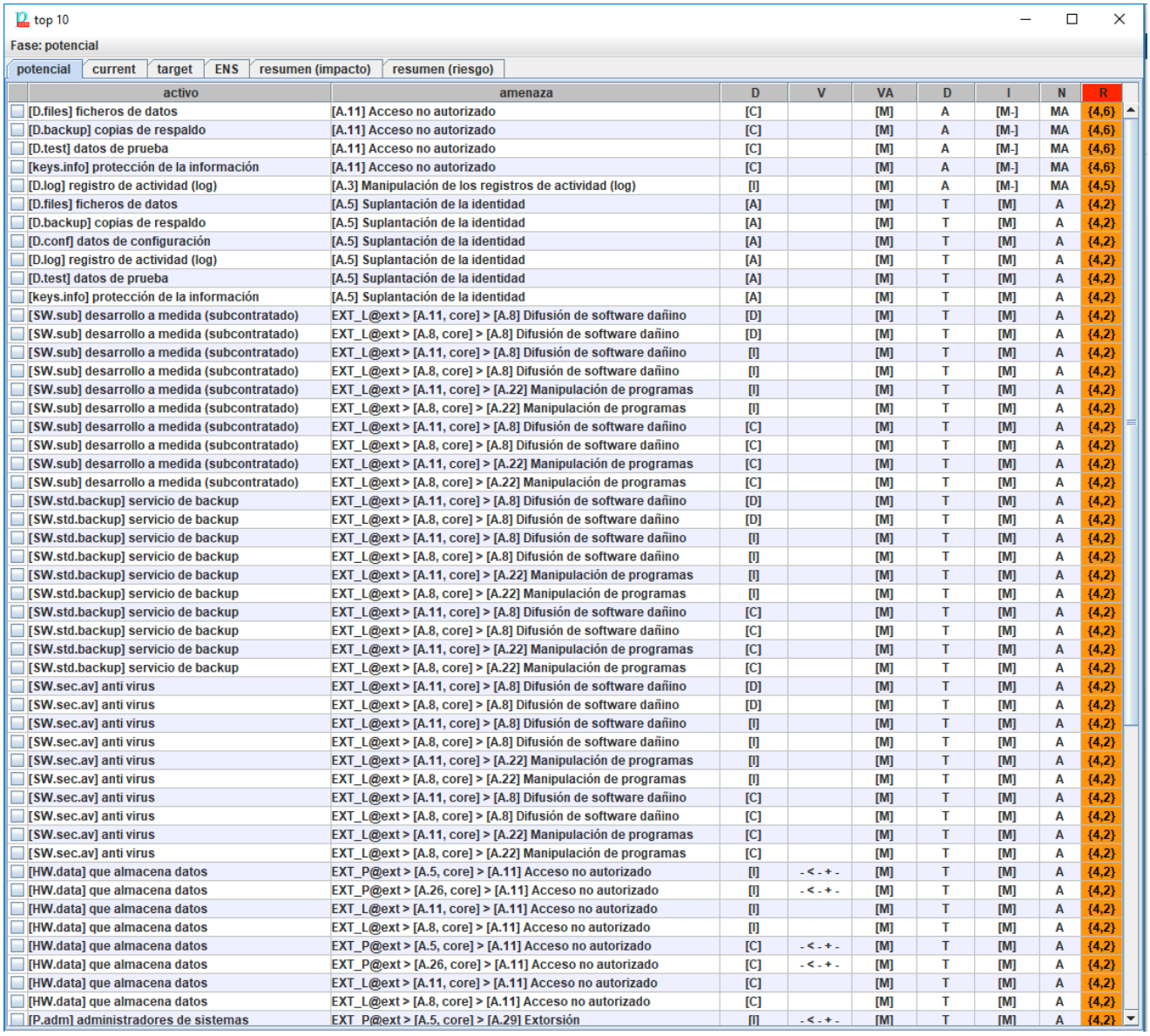
riesgos

potencial | current | target | ENS

activo	[D]	[I]	[C]	[A]	[T]	[V]
ACTIVOS	{2,9}	{3,0}	{3,3}	{3,0}	{3,0}	
[S1] Portal Web	{2,9}			{1,2}	{1,2}	
[D] disponibilidad	{2,9}					
[A] autenticidad de los usuarios y de la información				{1,2}		
[T] trazabilidad del servicio y de los datos					{1,2}	
[S2] Gestión de expedientes	{1,1}			{3,0}	{3,0}	
[D] disponibilidad	{1,1}					
[A] autenticidad de los usuarios y de la información				{3,0}		
[T] trazabilidad del servicio y de los datos					{3,0}	
[S3] Padrón	{1,1}			{3,0}	{3,0}	
[D] disponibilidad	{1,1}					
[A] autenticidad de los usuarios y de la información				{3,0}		
[T] trazabilidad del servicio y de los datos					{3,0}	
[I1] Información web		{1,3}	{1,5}	{1,2}	{1,2}	
[I] integridad de los datos		{1,3}				
[C] confidencialidad de los datos			{1,5}			
[A] autenticidad de los usuarios y de la información				{1,2}		
[T] trazabilidad del servicio y de los datos					{1,2}	
[I2] Expedientes		{3,0}	{3,3}	{3,0}	{3,0}	
[I] integridad de los datos		{3,0}				
[C] confidencialidad de los datos			{3,3}			
[A] autenticidad de los usuarios y de la información				{3,0}		
[T] trazabilidad del servicio y de los datos					{3,0}	
[I3] Licencias		{3,0}	{1,5}	{3,0}	{3,0}	
[I] integridad de los datos		{3,0}				
[C] confidencialidad de los datos			{1,5}			
[A] autenticidad de los usuarios y de la información				{3,0}		
[T] trazabilidad del servicio y de los datos					{3,0}	
[I4] Datos del padrón		{3,0}	{3,3}	{3,0}	{3,0}	
[I] integridad de los datos		{3,0}				
[C] confidencialidad de los datos			{3,3}			
[A] autenticidad de los usuarios y de la información				{3,0}		
[T] trazabilidad del servicio y de los datos					{3,0}	

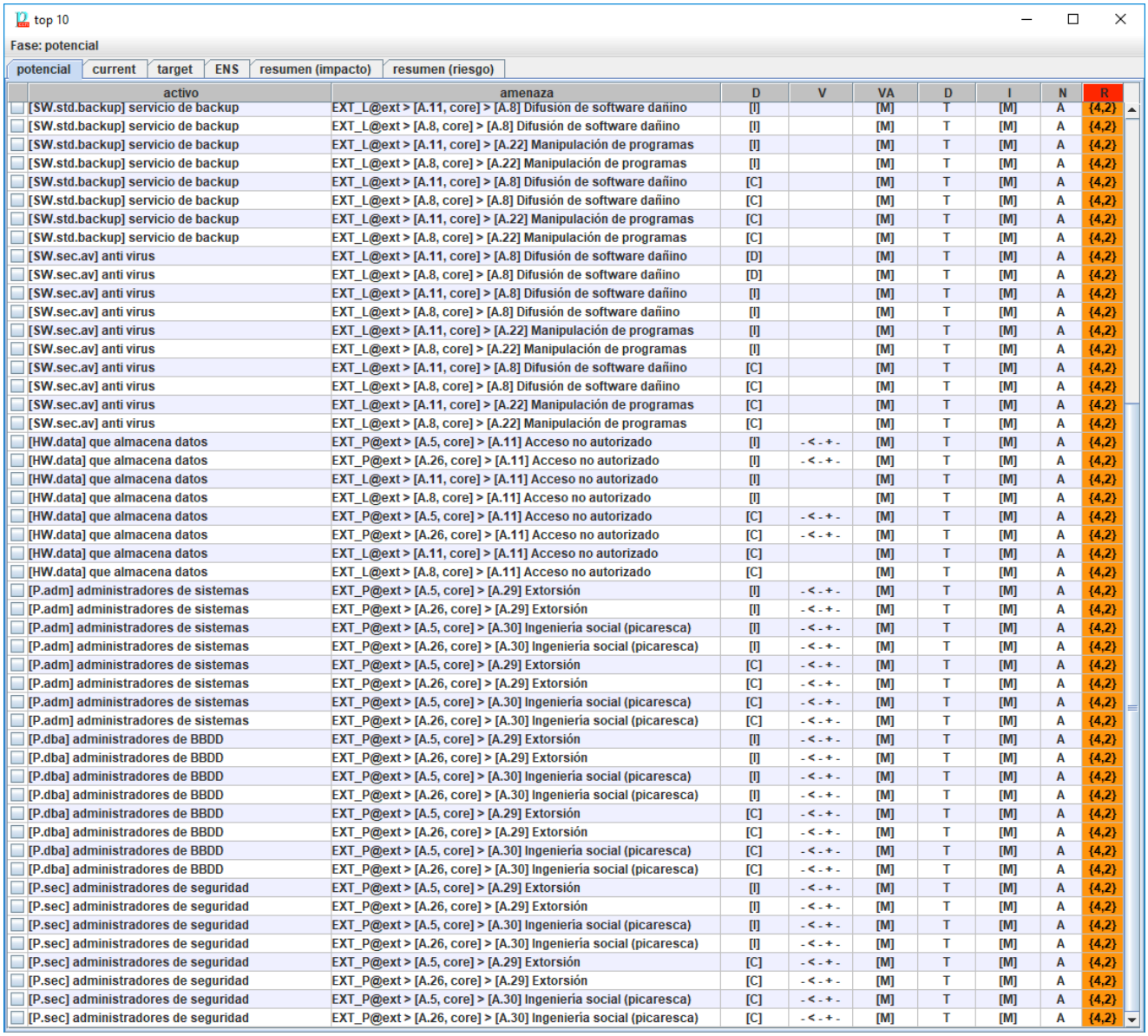
Ilustración 4: Análisis de riesgos actual

Una vez realizada la valoración de los activos pertenecientes a los servicios y a la información, PILAR se encarga de calcular los valores de riesgo del resto de activos de la organización. Las siguientes ilustraciones muestran el listado de activos con el riesgo potencial y con el riesgo actual más alto. Habría que aplicar medidas para que el riesgo más alto de estos activos disminuya en la medida de lo posible.



activo	amenaza	D	V	VA	D	I	N	R
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]		[M]	A	[M-]	MA	{4,6}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]		[M]	A	[M-]	MA	{4,6}
[D.test] datos de prueba	[A.11] Acceso no autorizado	[C]		[M]	A	[M-]	MA	{4,6}
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]		[M]	A	[M-]	MA	{4,6}
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de actividad (log)	[I]		[M]	A	[M-]	MA	{4,5}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[D.test] datos de prueba	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.sub] desarrollo a medida (subcontratado)	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acceso no autorizado	[I]	-<-+-	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acceso no autorizado	[I]	-<-+-	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acceso no autorizado	[I]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acceso no autorizado	[I]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acceso no autorizado	[C]	-<-+-	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acceso no autorizado	[C]	-<-+-	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acceso no autorizado	[C]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acceso no autorizado	[C]		[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[I]	-<-+-	[M]	T	[M]	A	{4,2}

Ilustración 5: Listado de activos con el riesgo potencial y con el riesgo actual más alto.



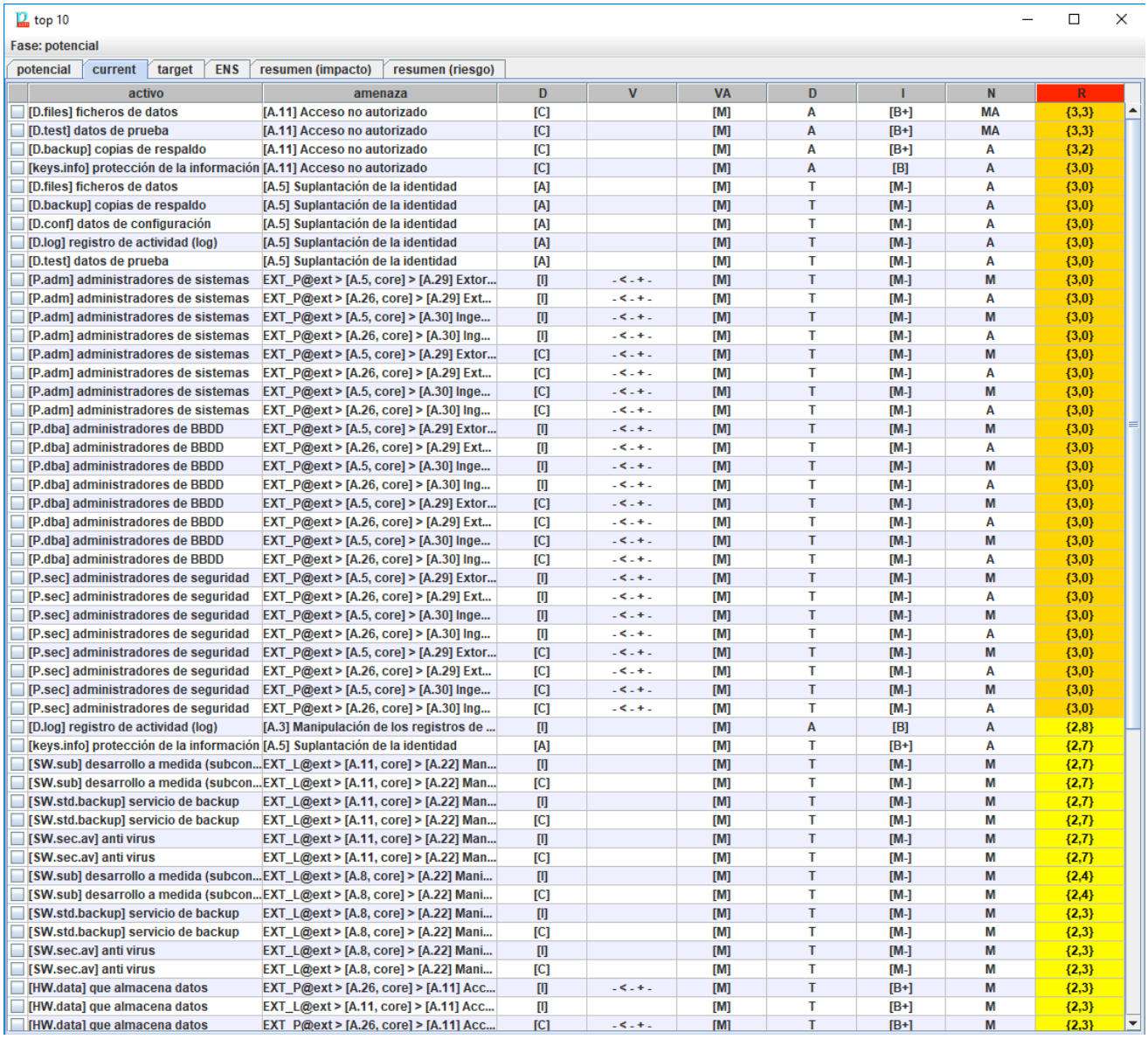
top 10

Fase: potencial

potencial | current | target | ENS | resumen (impacto) | resumen (riesgo)

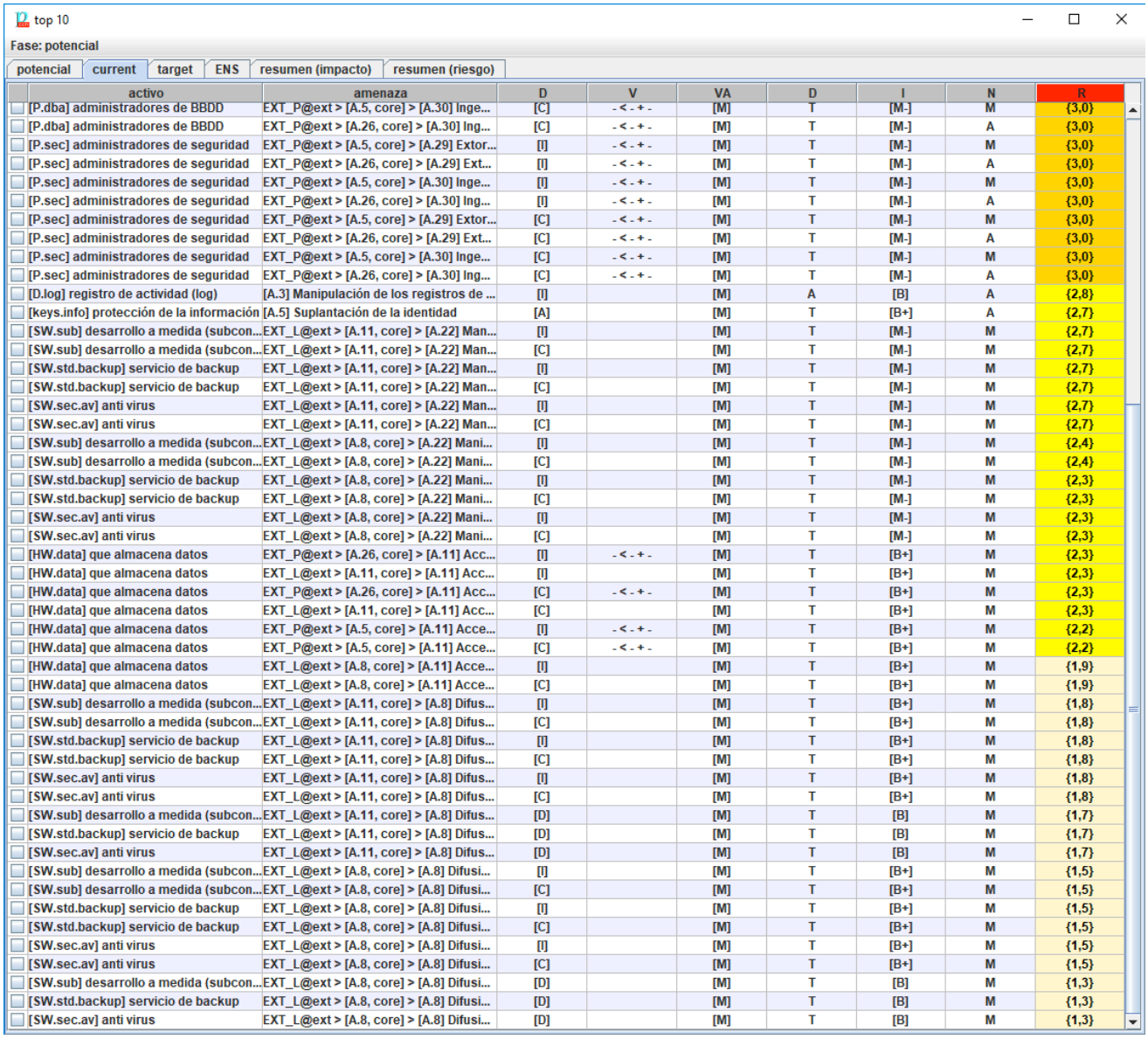
activo	amenaza	D	V	VA	D	I	N	R
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[D]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[I]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusión de software dañino	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Manipulación de programas	[C]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acceso no autorizado	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acceso no autorizado	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acceso no autorizado	[I]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acceso no autorizado	[I]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acceso no autorizado	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acceso no autorizado	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acceso no autorizado	[C]		[M]	T	[M]	A	{4,2}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acceso no autorizado	[C]		[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[I]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Extorsión	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ingeniería social (picaresca)	[C]	- < - + -	[M]	T	[M]	A	{4,2}

Ilustración 6: Listado de activos con el riesgo potencial y con el riesgo actual más alto.



activo	amenaza	D	V	VA	D	I	N	R
[D.files] ficheros de datos	[A.11] Acceso no autorizado	[C]		[M]	A	[B+]	MA	{3,3}
[D.test] datos de prueba	[A.11] Acceso no autorizado	[C]		[M]	A	[B+]	MA	{3,3}
[D.backup] copias de respaldo	[A.11] Acceso no autorizado	[C]		[M]	A	[B+]	A	{3,2}
[keys.info] protección de la información	[A.11] Acceso no autorizado	[C]		[M]	A	[B]	A	{3,0}
[D.files] ficheros de datos	[A.5] Suplantación de la identidad	[A]		[M]	T	[M-]	A	{3,0}
[D.backup] copias de respaldo	[A.5] Suplantación de la identidad	[A]		[M]	T	[M-]	A	{3,0}
[D.conf] datos de configuración	[A.5] Suplantación de la identidad	[A]		[M]	T	[M-]	A	{3,0}
[D.log] registro de actividad (log)	[A.5] Suplantación de la identidad	[A]		[M]	T	[M-]	A	{3,0}
[D.test] datos de prueba	[A.5] Suplantación de la identidad	[A]		[M]	T	[M-]	A	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extor...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.29] Ext...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.30] Inge...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.30] Ing...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.29] Extor...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.29] Ext...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.5, core] > [A.30] Inge...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.adm] administradores de sistemas	EXT_P@ext > [A.26, core] > [A.30] Ing...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.29] Extor...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.29] Ext...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Inge...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.30] Ing...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.29] Extor...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.29] Ext...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Inge...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.30] Ing...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extor...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Ext...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Inge...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ing...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extor...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Ext...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Inge...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ing...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de ...	[I]		[M]	A	[B]	A	{2,8}
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]		[M]	T	[B+]	A	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,4}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,4}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,3}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,3}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,3}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,3}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acc...	[I]	- < - + -	[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acc...	[I]		[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acc...	[C]	- < - + -	[M]	T	[B+]	M	{2,3}

Ilustración 7: Listado de activos con el riesgo potencial y con el riesgo actual más alto.



activo	amenaza	D	V	VA	D	I	N	R
[P.dba] administradores de BBDD	EXT_P@ext > [A.5, core] > [A.30] Inge...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.dba] administradores de BBDD	EXT_P@ext > [A.26, core] > [A.30] Ing...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extor...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Ext...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Inge...	[I]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ing...	[I]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.29] Extor...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.29] Ext...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.5, core] > [A.30] Inge...	[C]	- < - + -	[M]	T	[M-]	M	{3,0}
[P.sec] administradores de seguridad	EXT_P@ext > [A.26, core] > [A.30] Ing...	[C]	- < - + -	[M]	T	[M-]	A	{3,0}
[D.log] registro de actividad (log)	[A.3] Manipulación de los registros de ...	[I]		[M]	A	[B]	A	{2,8}
[keys.info] protección de la información	[A.5] Suplantación de la identidad	[A]		[M]	T	[B+]	A	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Man...	[I]		[M]	T	[M-]	M	{2,7}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.22] Man...	[C]		[M]	T	[M-]	M	{2,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,4}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,4}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,3}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,3}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Mani...	[I]		[M]	T	[M-]	M	{2,3}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.22] Mani...	[C]		[M]	T	[M-]	M	{2,3}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acc...	[I]	- < - + -	[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acc...	[I]		[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_P@ext > [A.26, core] > [A.11] Acc...	[C]	- < - + -	[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_L@ext > [A.11, core] > [A.11] Acc...	[C]		[M]	T	[B+]	M	{2,3}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acce...	[I]	- < - + -	[M]	T	[B+]	M	{2,2}
[HW.data] que almacena datos	EXT_P@ext > [A.5, core] > [A.11] Acce...	[C]	- < - + -	[M]	T	[B+]	M	{2,2}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acce...	[I]		[M]	T	[B+]	M	{1,9}
[HW.data] que almacena datos	EXT_L@ext > [A.8, core] > [A.11] Acce...	[C]		[M]	T	[B+]	M	{1,9}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.8] Difus...	[I]		[M]	T	[B+]	M	{1,8}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.8] Difus...	[C]		[M]	T	[B+]	M	{1,8}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difus...	[I]		[M]	T	[B+]	M	{1,8}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difus...	[C]		[M]	T	[B+]	M	{1,8}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difus...	[I]		[M]	T	[B+]	M	{1,8}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difus...	[C]		[M]	T	[B+]	M	{1,8}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.11, core] > [A.8] Difus...	[D]		[M]	T	[B]	M	{1,7}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.11, core] > [A.8] Difus...	[D]		[M]	T	[B]	M	{1,7}
[SW.sec.av] anti virus	EXT_L@ext > [A.11, core] > [A.8] Difus...	[D]		[M]	T	[B]	M	{1,7}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[I]		[M]	T	[B+]	M	{1,5}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[C]		[M]	T	[B+]	M	{1,5}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[I]		[M]	T	[B+]	M	{1,5}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[C]		[M]	T	[B+]	M	{1,5}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[I]		[M]	T	[B+]	M	{1,5}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[C]		[M]	T	[B+]	M	{1,5}
[SW.sub] desarrollo a medida (subcon...	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[D]		[M]	T	[B]	M	{1,3}
[SW.std.backup] servicio de backup	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[D]		[M]	T	[B]	M	{1,3}
[SW.sec.av] anti virus	EXT_L@ext > [A.8, core] > [A.8] Difusi...	[D]		[M]	T	[B]	M	{1,3}

Ilustración 8: Listado de activos con el riesgo potencial y con el riesgo actual más alto.

La herramienta PILAR calcula estos valores de riesgo por cada amenaza que afecta a una de las dimensiones de un activo, algo que si se tuviera que hacer de forma manual resultaría pesado. A la hora de mostrar los valores de impacto y riesgo utiliza una escala de valores en la que cada color es asociado a un color. Esta escala se denomina “niveles de criticidad”:

Ilustración 9: Niveles de criticidad en PILAR

6. Fase 4: Definición de Plan de Adecuación al ENS

6.1 Introducción

Se daban doce meses de plazo tras la entrada en vigor del Esquema Nacional de Seguridad para aplicarlo en los servicios que se prestaban en ese momento. El problema llegó al ver que la gran mayoría tras esos doce meses no habían conseguido aplicarlo.

Cuando no es posible hacerlo por cualquier circunstancia, hay que preparar un plan de adecuación, con las tareas a realizar para la completa aplicación de lo exigido por el ENS a lo largo de un plazo que no puede ser superior a 48 meses desde la entrada en vigor del mismo. Los detalles de cómo desarrollarlo se recogen en la **Guía de Seguridad (CCN-STIC-806) Esquema Nacional de Seguridad – Plan de Adecuación**.

Este plan de adecuación contendrá la siguiente información:

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. Declaración de aplicabilidad de las medidas del Anexo II del ENS.
7. Análisis de riesgos.
8. Insuficiencias del sistema.
9. Plan de mejora seguridad, incluyendo plazos estimados de ejecución.

El Plan de Adecuación lo desarrollará el Responsable de Seguridad en el caso de haberlo o la persona que desempeñe esta función de forma temporal durante el proyecto.

6.2 Plan de adecuación

6.2.1 Política de Seguridad

Idealmente, el organismo dispondrá de una política de seguridad conforme a lo que se pide en el Anexo II del Esquema Nacional de Seguridad, por lo que sólo será necesario identificarla y anexarla al plan de adecuación.

Si se dispone de una Política de Seguridad que no satisface los requisitos del Anexo II, se identificará la política de aplicación, se anexará al plan de adecuación y por último se hará constar cómo de planea adaptar la política a las exigencias del Anexo II en el plan de mejora de la seguridad.

Pero si no se dispone, el plan tendrá que recoger la planificación del desarrollo de una nueva política que cumpla con todos los requisitos o exigencias del Anexo II.

6.2.2 Información que se maneja, con su valoración

Hay que detallar toda la información que se maneja y valorarla según se establece en el Anexo I del Esquema nacional de Seguridad.

Pueden darse varias causas que impidan detallar toda la información, entre ellas que la política de seguridad no esté clara y definida, que no esté nombrado el responsable de algunas de las informaciones tratadas o que no esté aprobada formalmente la valoración de la información. Estas tres causas pueden resultar problemáticas a la hora de llevar a cabo tanto el inventario de toda la información utilizada en la prestación de los servicios como posteriormente valorarla, ya que no habrá criterios definidos para hacerlo y faltarán algunos propietarios.

Si fuera así, el Responsable de Seguridad o la persona designada para llevar a cabo sus funciones tendrá que realizar esta valoración, dejando constancia de los motivos y razonamientos para determinar las valoraciones documentadas. Esta valoración es meramente provisional para los efectos del plan y deberá realizarse una valoración formal en un plazo límite, documentándose estas tareas en el plan.

6.2.3 Servicios que se prestan, con su valoración

De manera análoga a lo indicado en la sección anterior para la información, debe realizarse la valoración de los servicios que se prestan. Dicha valoración se realizará según lo establecido en el Anexo I del Esquema Nacional de Seguridad.

Pueden darse varias causas que impidan alcanzar la valoración de los servicios prestados como que la Política de Seguridad no exista o sea insuficiente, que no esté nombrado el responsable de algún servicio prestado o por último, que no esté aprobada formalmente la valoración de la información.

En este caso el Responsable de Seguridad realizará una valoración provisional, a su mejor criterio, dejando constancia de los motivos o razonamientos. Esta valoración solo es vinculante para el organismo mientras no se disponga de la valoración formal. En esta valoración se especifica un plazo de validez, pasado el cual deberá haberse realizado una valoración formal.

6.2.4 Datos de caràcter personal

Cuando el sistema maneja datos de carácter personal, deberá incluirse la relación detallada de dichos datos en el plan de adecuación.

6.2.5 Categoría del sistema

Con las valoraciones disponibles de la información y los servicios, el Responsable de Seguridad establecerá la categoría del sistema, siguiendo los criterios y pasos recogidos en el Anexo I del ENS.

Una estrategia eficaz para reducir la utilización de recursos es segregar los sistemas en sub-sistemas, si es posible. De esta manera se aplicarán las medidas de seguridad exigidas para niveles altos específicamente a aquellos segmentos del sistema que lo requieran y no al sistema completo, que requeriría mucho más esfuerzo. De esta forma también se reducen los recursos necesarios.

6.2.6 Análisis de riesgos

Otro de los puntos a incluir en el Plan de Adecuación es un análisis de riesgos, según lo descrito en el Anexo II del ENS para la categoría establecida para el sistema.

En este análisis de riesgos se valorarán las salvaguardas presentes en la fecha de aprobación del plan de adecuación, de manera que se cuente con un mapa de riesgos actuales.

6.2.7 Declaración de aplicabilidad de las medidas del Anexo II del ENS

Vistas las exigencias del Anexo II del Esquema Nacional de Seguridad y las exigencias derivadas de los datos de carácter personal, el Responsable de Seguridad elaborará una relación de las medidas que son de aplicación al sistema o a cada sub-sistema.

Habitualmente se recurrirá a las medidas detalladas en el Anexo II, enriquecidas o matizadas por características determinadas del sistema o exigencias derivadas del tratamiento de datos de carácter personal.

El Responsable de Seguridad, a la vista del nivel del sistema y de los requisitos planteados para la protección de los datos de carácter personal, documentará la lista de las medidas aplicables al sistema. Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado. Téngase en cuenta que tanto el ENS como la reglamentación de protección de datos de carácter personal, establecen una serie de medidas mínimas que deben ampliarse cuando sea prudente hacerlo.

6.2.8 Insuficiencias del sistema

Hay que identificar y documentar las carencias en el actual sistema de gestión de seguridad de la información, que pueden detectarse en varios aspectos:

- Desviaciones de lo exigido en el Anexo II para valorar el sistema y seleccionar medidas de seguridad.
- Incumplimientos de los requisitos exigidos por el RD 1720/2007 para los datos de carácter personal tratados por el sistema.
- Existencia de riesgos no asumibles por el organismo.

Formalmente los riesgos residuales (los que quedan tras la aplicación de las medidas de seguridad seleccionadas) deben ser aceptados por los responsables de la información y servicios afectados. Puede darse el caso de que no todos los responsables estén designados o que la aceptación del riesgo no sea formal, el Responsable de Seguridad tomará la decisión a su mejor criterio, indicando por qué y cómo ha llegado a esas decisiones de aceptación o no del riesgo residual.

6.2.9 Plan de mejora de la Seguridad

Partiendo de la información recopilada, y teniendo en cuenta las carencias detectadas se elaborará un plan de mejora de la seguridad que detallará las acciones que se van a tomar para subsanarlas.

Además para cada una de las acciones que se tomarán se documentará:

- Las insuficiencias que subsana.
- El plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación.
- Los principales hitos del proyecto.
- Una estimación del coste que supondrá.

La fecha de inicio puede limitarse al año en que se prevé acometer la actuación y la fecha de determinación se puede calcular en función del tiempo que se ha estimado para ejecutar la actuación.

7. Fase 5: Adecuación al ENS

7.1 Introducción

En la disposición transitoria del Real Decreto 3/2010 se articula un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación ha vencido el 30 de enero de 2014.

El **Real Decreto 951/2015, de 23 de octubre**, de modificación del anterior RD establece que los sistemas deberán adecuarse a lo dispuesto **en un plazo de veinticuatro meses (5 de noviembre de 2017)**.

En el anterior punto de este proyecto se ha establecido y definido el plan de adecuación al Esquema Nacional de Seguridad con todas las cuestiones necesarias para una correcta adecuación.

7.2 Definición de sistema documental

Es necesario el apoyo de un sistema documental para la correcta adecuación al ENS. La existencia de estos documentos constituye la evidencia imprescindible para certificar que el Esquema Nacional de Seguridad se adecua correctamente. En este caso se ha establecido una política de seguridad que se encuentra de forma completa en el anexo de este proyecto y también habría que establecer una declaración de aplicabilidad de las medidas del Anexo II del ENS.

Todos los organismos que estén sujetos al cumplimiento del ENS deben contar con una política de seguridad formal, aprobada por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá en base a los principios básicos indicados y se desarrollará aplicando una serie de requisitos mínimos.

Por otra parte también habría que realizar una declaración de aplicabilidad dejando clara la diferencia entre esta y el análisis diferencial visto anteriormente. En la declaración de aplicabilidad se establecen las medidas que se van a implementar dada la situación de la organización. Pueden haber medidas del Anexo II que se decidan no implementar por diversos motivos a pesar de que la categoría del sistema índice que si se debe implementar.

7.3 Seguimiento de la implantación de medidas de Seguridad

Para tener un correcto seguimiento del cumplimento se realizarán de forma anual auditorías internas y se hará una revisión del análisis de riesgos.

El Esquema Nacional de Seguridad (ENS) establece la obligación de evaluar regularmente el estado de seguridad de los sistemas:

Artículo 35. Informe del estado de la Seguridad:
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.

8. Fase 6: Auditoría de conformidad

8.1 Introducción. ¿quién, como?

La Entidad Nacional de Acreditación (ENAC) pone a disposición de los interesados el esquema de acreditación de entidades que quieran certificar el cumplimiento con el Esquema Nacional de Seguridad (ENS).

El esquema de acreditación ha sido desarrollado por ENAC en estrecha colaboración con el Ministerio de Hacienda y Función Pública (MINHAFP) y el Centro Criptológico Nacional (CCN).

En el caso de sistemas clasificados con el grado de DIFUSIÓN LIMITADA (DL) o equivalente, una entidad **debe estar acreditada por ENAC** en el ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 para poder certificar el cumplimiento de requisitos STIC. Además, las entidades auditoras de seguridad deben disponer de Habilitación de Seguridad de Empresa (HSEM) en vigor.

También se podrá certificar el cumplimiento de los requisitos STIC en el ámbito de los sistemas clasificados (DL) entre aquellas entidades auditoras que cumplan alguna de las siguientes opciones (CCN-STIC-101):

1. Ser una entidad, órgano, organismo y unidad vinculada o dependiente de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.
2. Excepcionalmente, ser una empresa validada por el CCN, que haya demostrado la capacidad técnica suficiente para llevar a cabo auditorías/inspecciones STIC sobre sistemas que manejan información clasificada.

Se prevén actividades de certificación de forma transitoria hasta transcurrido un año desde la entrada en vigor de la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad publicada en B.O.E. nº 265, de 2 de noviembre de 2016, de acuerdo con lo indicado en el Apartado VI de Requisitos de las Entidades Certificadoras. Durante este periodo, las certificaciones concedidas por una entidad EN PROCESO seguirán siendo válidas aunque la entidad certificadora no supere el proceso de acreditación de ENAC.

Entidades de certificación acreditadas o en vías de acreditación para expedir certificaciones de conformidad con el ENS y sistemas clasificados con el grado de DIFUSIÓN LIMITADA (DL) o equivalente:

Nombre	Razón social	Enlace web	Estado Acreditación ENS	Estado Acreditación STIC (DL)
AENOR Internacional S.A.U.	AENOR Internacional S.A.U.	www.aenor.com	ACREDITADA (21/04/2017)	-
Audertis Audit Services, S.L.	Audertis Audit Services, S.L.	www.audertis.es	EN PROCESO	-
BDO Auditores, S.L.P.	BDO Auditores, S.L.P.	www.bdo.es	EN PROCESO	-
Ingeniería de Sistemas para la Defensa de España (ISDEFE)	Empresa pública de consultoría e ingeniería	www.isdefe.es	-	EN PROCESO
LEET Security, S.L.	LEET Security, S.L.	www.leetsecurity.com	EN PROCESO	-
LGAI Technological Center, S.A.	LGAI Technological Center, S.A.	www.appluscertification.com/es	EN PROCESO	-

9. Conclusiones

Una vez finalizado el proyecto es momento de analizar las lecciones aprendidas durante el transcurso de la implantación del Esquema nacional de Seguridad en una organización ficticia.

En primer lugar considero necesario que las organizaciones que disponen de sistemas de información que sustentan la aplicación de LAESCP y por tanto de empleados encargados de gestionar dichos sistemas, dispongan de una implementación o adecuación al Esquema Nacional de Seguridad. El primer paso para proteger en materia de seguridad de la información tu organización, es creer en ello. Ser consciente de que existen unas vulnerabilidades en tus activos y que por tanto están expuestos a ataques o incidentes de seguridad con la consecuente pérdida económica.

En segundo lugar considero que el proyecto es una práctica muy realista, puesto que la implantación del Esquema Nacional de Seguridad es una tarea demandada en el sector TI y de obligado cumplimiento en algunas de las organizaciones. También son solicitadas las auditorías de cumplimiento al Esquema nacional de Seguridad.

Por otro lado, el hecho de haber desarrollado un análisis de riesgos con la herramienta PILAR me ha servido por partida doble. Primero por conocer la metodología MAGERIT y las etapas de un análisis de riesgos; segundo por haber conocido la herramienta PILAR y poder saber utilizarla.

Además, el hecho de valorar que propuestas puede llevar a cabo una empresa para mitigar o reducir los riesgos a los que se encuentra expuesta, te hace reflexionar sobre diferentes medidas que el día de mañana como consultor puedo proponer a una entidad con una casuística similar.

Respecto a las fases del proyecto, el tiempo establecido para desarrollar cada una era acorde al contenido que se demandaba. Por ello, no he tenido ningún problema para ir completando cada etapa del trabajo.

Por último, considero que se trata de un Trabajo Final de Máster muy apropiado para la especialidad de Gestión y auditoría de la Seguridad.

10. Glosario

TIC: Abreviatura de Tecnología de la Información y de la Computación.
e-Administración: Hace referencia a la incorporación de las tecnologías de la información y las comunicaciones en las administraciones públicas.
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.
Auditor: El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independientemente. Realiza las tareas de auditoria.
Auditoría: Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoria.
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.

11. Bibliografía

- **BOE.** Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. [Consulta: 4 de octubre de 2017] https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330
- **CCN.** Entidades de certificación acreditadas. [Consulta: 1 de diciembre de 2017] https://www.ccn-cert.cni.es/ens/entidades-de-certificacion.html
- **CCN.** Esquema Nacional de Seguridad. [Consulta: 3 de octubre de 2017] https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=2.html
- **CCN.** Guía de seguridad (CCN-STIC-803) Esquema Nacional de Seguridad valoración de los sistemas. [Consulta: 7 de octubre de 2017] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf
- **CCN.** Guía de seguridad (CCN-STIC-806) Esquema Nacional de Seguridad [Consulta: 1 de octubre de 2017] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/806-Plan_adecuacion_ENS/806_ENS-adecuacion_ene-11.pdf
- **CCN.** Guía de seguridad (CCN-STIC-808) Esquema Nacional de Seguridad verificación del cumplimiento de las medidas en el ENS. [Consulta: 7 de octubre de 2017] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/808/808-Verificacion_del_cumplimiento_medidas_ENS-sep11.pdf
- **CCN.** Guía de seguridad (CCN-STIC-809) Declaración y certificación de conformidad con el ENS y distintivos de cumplimiento. [Consulta: 7 de octubre de 2017] 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-815) ENS métricas e indicadores. [Consulta: 8 de octubre de 2017] https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/815-Metricas_e_Indicadores_en_el_ENS/815_Metricas_e_indicadores_en_el_ENS-feb14.pdf
- **CCN.** Guía de Seguridad de las TIC (CCN-STIC-824) [Consulta: 10 de octubre de 2017] 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
- **CNIS.** Plan de Adecuación al ENS en el Servicio de Modernización Administrativa y Nuevas Tecnologías de la Información de la Diputación de Burgos. [Consulta: 3 de octubre de 2017] http://www.cnis.es/Comunicado_ENS_Diputaci%C3%B3n_BU_3.pdf
- **INGENIA.** ENS: plan de adecuación, implantación y auditoría. [Consulta: 3 de octubre de 2017] https://www.ingenia.es//es/servicio/esquema-nacional-de-seguridad-ens-plan-de-adecuacion-implantacion-y-auditoria
- **Instituto Nacional Tecnologías de la Comunicación (INTECO).** Implantación del ENS. [Consulta: 1 de octubre de 2017] http://ametic.es/sites/default/files//media/INTECO%20-%20Implantaci%C3%B3n%20del%20ENS.pdf

12. Anexos

12.1 Análisis de riesgos

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: 1234

Nombre: Proyecto

Descripción:

Datos administrativos:

- Organización: Invernalia
- Autor: Rubén Lacruz

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
- [V] Valor

1.2 - Agravantes y atenuantes

[base] Base

- [101] Identificación del atacante
  - [101.a] público en general
- [102] Motivación del atacante
  - [102.a] económica (beneficios en dinero)

- [102.f] con ánimo destructivo
- [102.g] con ánimo de causar daño

- [103] Beneficio del atacante
  - [103.a] moderadamente interesado
- [106] Atracción del objetivo
  - [106.c] objetivo atractivo
- [104] Motivación del personal interno
  - [104.a] todo el personal está fuertemente motivado
- [105] Permisos de los usuarios (derechos)
  - [105.a] se permite el acceso a Internet
  - [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

1.3 - Valoración de los activos

capa: [essential] Activos esenciales

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]
[I1] Información web		[B]	[B]	[B]	[B]	
[S1] Portal Web	[M]			[B]	[B]	
[I2] Expedientes		[M]	[M]	[M]	[M]	
[I4] Datos del padrón		[M]	[M]	[M]	[M]	
[S3] Padrón	[B]			[M]	[M]	
[I3] Licencias		[M]	[B]	[M]	[M]	
[S2] Gestión de expedientes	[B]			[M]	[M]	

capa: [arch.ip] sistema de protección de frontera lógica

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [arch.pps] sistema de protección física del perímetro

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [D] Datos / Información

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [keys] Claves criptográficas

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [S] Servicios

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [SW] Aplicaciones (software)

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [HW] Equipamiento informático (hardware)

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [COM] Redes de comunicaciones

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [Media] Soportes de información

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [AUX] Equipamiento auxiliar

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [L] Instalaciones

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

capa: [P] Personal

Activos esenciales

activo	[D]	[I]	[C]	[A]	[T]	[V]

Categoría del sistema

[base] Base

MEDIA

2 - 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

Phase: [potencial]

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[M-]	{4,6}
[A.3] Manipulación de los registros de actividad (log)	I	[M-]	{4,5}
[A.30] Ingeniería social (picaresca)	I	[M]	{4,2}
[A.29] Extorsión	I	[M]	{4,2}
[A.5] Suplantación de la identidad	A	[M]	{4,2}

Phase: [current] situación actual

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[B+]	{3,3}
[A.30] Ingeniería social (picaresca)	I	[M-]	{3,0}
[A.29] Extorsión	I	[M-]	{3,0}
[A.5] Suplantación de la identidad	A	[M-]	{3,0}

Phase: [ENS] Esquema Nacional de Seguridad

amenaza	D	I	R
[A.11] Acceso no autorizado	C	[0]	{1,0}
[A.3] Manipulación de los registros de actividad (log)	I	[0]	{1,0}
[A.5] Suplantación de la identidad	A	[0]	{0,94}

3 - 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

Phase: [potencial]

activo	amenaza	D	I	R
[I2] Expedientes	[A.11] Acceso no autorizado	I, C	[M]	{4,6}
[I4] Datos del padrón	[A.11] Acceso no autorizado	I, C	[M]	{4,6}
[S2] Gestión de expedientes	[A.3] Manipulación de los registros de actividad (log)	T	[M-]	{4,5}
[S3] Padrón	[A.3] Manipulación de los registros de actividad (log)	T	[M-]	{4,5}
[I2] Expedientes	[A.3] Manipulación de los registros de actividad (log)	T	[M-]	{4,5}
[I3] Licencias	[A.3] Manipulación de los registros de actividad (log)	T	[M-]	{4,5}
[I4] Datos del padrón	[A.3] Manipulación de los registros de actividad (log)	T	[M-]	{4,5}
[S1] Portal Web	[A.8] Difusión de software dañino	D	[M]	{4,2}

[S2] Gestión de expedientes	[A.5] Suplantación de la identidad	A, T	[M]	{4,2}
[S3] Padrón	[A.5] Suplantación de la identidad	A, T	[M]	{4,2}
[I2] Expedientes	[A.30] Ingeniería social (picaresca)	I, C	[M]	{4,2}
[I2] Expedientes	[A.29] Extorsión	I, C	[M]	{4,2}
[I2] Expedientes	[A.22] Manipulación de programas	I, C	[M]	{4,2}
[I2] Expedientes	[A.8] Difusión de software dañino	I, C	[M]	{4,2}
[I2] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[M]	{4,2}
[I3] Licencias	[A.30] Ingeniería social (picaresca)	I	[M]	{4,2}
[I3] Licencias	[A.29] Extorsión	I	[M]	{4,2}
[I3] Licencias	[A.22] Manipulación de programas	I	[M]	{4,2}
[I3] Licencias	[A.8] Difusión de software dañino	I	[M]	{4,2}
[I3] Licencias	[A.11] Acceso no autorizado	I	[M]	{4,2}
[I3] Licencias	[A.5] Suplantación de la identidad	I, A, T	[M]	{4,2}
[I4] Datos del padrón	[A.30] Ingeniería social (picaresca)	I, C	[M]	{4,2}
[I4] Datos del padrón	[A.29] Extorsión	I, C	[M]	{4,2}
[I4] Datos del padrón	[A.22] Manipulación de programas	I, C	[M]	{4,2}
[I4] Datos del padrón	[A.8] Difusión de software dañino	I, C	[M]	{4,2}
[I4] Datos del padrón	[A.5] Suplantación de la identidad	I, C, A, T	[M]	{4,2}

Phase: [current] situación actual

activo	amenaza	D	I	R
[I2] Expedientes	[A.11] Acceso no autorizado	C	[B+]	{3,3}
[I4] Datos del padrón	[A.11] Acceso no autorizado	C	[B+]	{3,3}
[S2] Gestión de expedientes	[A.5] Suplantación de la identidad	A, T	[M-]	{3,0}
[S3] Padrón	[A.5] Suplantación de la	A, T	[M-]	{3,0}

	identidad			
[I2] Expedientes	[A.30] Ingeniería social (picaresca)	I, C	[M-]	{3,0}
[I2] Expedientes	[A.29] Extorsión	I, C	[M-]	{3,0}
[I2] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[M-]	{3,0}
[I3] Licencias	[A.30] Ingeniería social (picaresca)	I	[M-]	{3,0}
[I3] Licencias	[A.29] Extorsión	I	[M-]	{3,0}
[I3] Licencias	[A.5] Suplantación de la identidad	I, A, T	[M-]	{3,0}
[I4] Datos del padrón	[A.30] Ingeniería social (picaresca)	I, C	[M-]	{3,0}
[I4] Datos del padrón	[A.29] Extorsión	I, C	[M-]	{3,0}
[I4] Datos del padrón	[A.5] Suplantación de la identidad	I, C, A, T	[M-]	{3,0}

Phase: [ENS] Esquema Nacional de Seguridad

activo	amenaza	D	I	R
[S2] Gestión de expedientes	[A.3] Manipulación de los registros de actividad (log)	T	[0]	{1,0}
[S3] Padrón	[A.3] Manipulación de los registros de actividad (log)	T	[0]	{1,0}
[I2] Expedientes	[A.11] Acceso no autorizado	C	[0]	{1,0}
[I2] Expedientes	[A.3] Manipulación de los registros de actividad (log)	T	[0]	{1,0}
[I3] Licencias	[A.3] Manipulación de los registros de actividad (log)	T	[0]	{1,0}
[I4] Datos del padrón	[A.11] Acceso no autorizado	C	[0]	{1,0}
[I4] Datos del padrón	[A.3] Manipulación de los registros de actividad (log)	T	[0]	{1,0}
[S2] Gestión de expedientes	[A.5] Suplantación de la identidad	A, T	[0]	{0,94}

[S3] Padrón	[A.5] Suplantación de la identidad	A, T	[0]	{0,94}
[I2] Expedientes	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,94}
[I3] Licencias	[A.5] Suplantación de la identidad	I, A, T	[0]	{0,94}
[I4] Datos del padrón	[A.5] Suplantación de la identidad	I, C, A, T	[0]	{0,94}
[I2] Expedientes	[A.15] Modificación de la información	I	[0]	{0,92}
[I3] Licencias	[A.15] Modificación de la información	I	[0]	{0,92}
[I4] Datos del padrón	[A.15] Modificación de la información	I	[0]	{0,92}

4 - Activos

Relación de activos identificados en el sistema de información.

dominio de seguridad: [base] Base

- Activos esenciales
  - [essential] Activos esenciales
    - [S1] Portal Web
    - [S2] Gestión de expedientes
    - [S3] Padrón
    - [I1] Información web
    - [I2] Expedientes
    - [I3] Licencias
    - [I4] Datos del padrón
- activos
  - [arch.ip] sistema de protección de frontera lógica
    - [SP01] Firewall
  - [arch.pps] sistema de protección física del perímetro
    - [SF01] Sistema de protección física
  - [D] Datos / Información
    - [D.files] ficheros de datos
    - [D.backup] copias de respaldo

    - [D.conf] datos de configuración
    - [D.log] registro de actividad (log)
    - [D.test] datos de prueba
- [keys] Claves criptográficas
    - [keys.info] protección de la información
- [S] Servicios
    - [S.prov.www] world wide web
    - [S.prov.email] correo electrónico
    - [S.prov.backup] servicio de copias de respaldo (backup)
- [SW] Aplicaciones (software)
    - [SW.sub] desarrollo a medida (subcontratado)
    - [SW.std.backup] servicio de backup
    - [SW.sec.av] anti virus
- [HW] Equipamiento informático (hardware)
    - [HW.host] grandes equipos (host)
    - [HW.mid] equipos medios
    - [HW.mobile] informática móvil
    - [HW.backup] equipamiento de respaldo
    - [HW.data] que almacena datos
    - [HW.peripheral.print] medios de impresión
    - [HW.peripheral.scan] escáner
    - [HW.pabx] centralita telefónica
- [COM] Redes de comunicaciones
    - [COM.wifi] WiFi
    - [COM.LAN] red local
    - [COM.Internet] Internet
- [Media] Soportes de información
    - [Media] Soportes de información
- [AUX] Equipamiento auxiliar
    - [AUX.ups] sai - sistemas de alimentación ininterrumpida
    - [AUX.ac] equipos de climatización
    - [AUX.cabling.wire] cable eléctrico
    - [AUX.cabling.fiber] fibra óptica
- [L] Instalaciones
    - [L.building] edificio
- [P] Personal
    - [P.ui] usuarios internos

- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.sec] administradores de seguridad
- [P.sub] subcontratas

12.2 Política de seguridad

INTRODUCCIÓN

El Ayuntamiento depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como 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.

La entidad es consciente de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

PREVENCIÓN

La entidad evita, o al menos intenta 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, la entidad:

• Autoriza los sistemas antes de entrar en operación.
• Evalúa regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
• Solicita la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se monitoriza 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.

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.

RESPUESTA

La entidad ha establecido mecanismos para responder eficazmente a los incidentes de seguridad.

Se ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.

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

RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la entidad ha desarrollado planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE

Esta política se aplica a todos los sistemas TIC de El Ayuntamiento y a todos los miembros de la organización, sin excepciones.

MISIÓN

Ofrecer al ciudadano un servicio de Administración Municipal, a través de medios electrónicos, potenciando el uso de las Nuevas Tecnologías en el Ayuntamiento y en la ciudadanía.

Los principales objetivos que se persiguen son:

• Fomentar la relación electrónica del ciudadano con el Ayuntamiento.
• Reducir tiempos de espera de atención al ciudadano.
• Acortar tiempos de espera en la resolución de trámites solicitados por el ciudadano.
• Desarrollar un sistema de gestión de información documental que facilite un rápido acceso del personal del servicio a la información solicitada por el ciudadano.

MARCO NORMATIVO

Esta política se enmarca en la siguiente legislación:

1. RD 3/2010 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. BOE de 29 de enero de 2010.

2. Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal.

4. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

5. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

6. Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.

7. Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.

8. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

9. Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

ORGANIZACIÓN DE LA SEGURIDAD

El Comité de Seguridad TIC estará formado por el concejal responsable de la administración electrónica, el Departamento de Sistemas y los Responsables de los Servicios Electrónicos.

El Secretario del Comité de Seguridad TIC será el Responsable del Departamento de Sistemas que se encargará de convocar las reuniones del Comité y levantar acta de las mismas.

El Comité de Seguridad TIC reportará a la Corporación Municipal.

El Comité de Seguridad TIC tendrá las siguientes funciones:

• Coordinar y aprobar las acciones en materia de seguridad de la información.

• Impulsar la cultura en seguridad de la información.

• Participar en la categorización de los sistemas y el análisis de riesgos.

• Revisar la documentación relacionada con la seguridad del sistema.

• Resolver discrepancias y problemas que puedan surgir en la gestión de la seguridad.

Las responsabilidades del Responsable de Seguridad de la
Información son:

• Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.

• Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.

• Gestionar la formación y concienciación en materia de seguridad TIC.

• Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.

• Revisar, 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, emitiendo informes periódicos sobre los más relevantes al Comité.

Las responsabilidades del Responsable del Sistema son:

• Gestionar el Sistema durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.

• Definir los criterios de uso y los servicios disponibles en el Sistema.

• Definir las políticas de acceso de usuarios al Sistema.

• Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

• Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.

• Realizar el análisis y gestión de riesgos en el Sistema.

• Elaborar y aprobar la documentación de seguridad del Sistema.

• 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.

• Implantar y controlar las medidas específicas de seguridad del Sistema.

• Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

• Suspensión el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por la Corporación Municipal a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta política de seguridad de la Información y la propuesta de revisión o mantenimiento de la

misma. La Política será aprobada por la Corporación Municipal y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

El Ayuntamiento trata datos de carácter personal y estos están bajo los requerimiento del RGPD, el cual entra en vigor este año 2018 de manera obligatoría.

GESTIÓN DE RIESGOS

Todos los sistemas afectados por esta Política están sujetos un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá al menos una vez al año o cuando cambien la información manejada, los servicios prestados, suceda un incidente grave de seguridad o se detecten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política de seguridad de la Información complementa las políticas de seguridad del Ayuntamiento en materia de protección de datos de carácter personal.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Se deberán de implementar medidas proactivas por parte de los responsables y es obligatorio tenir un Delegado de Protección de Datos.

OBLIGACIONES DEL PERSONAL

Todos los miembros del Ayuntamiento 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 del Ayuntamiento 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 del Ayuntamiento, 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.

TERCERAS PARTES

Cuando del Ayuntamiento 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 el Ayuntamiento 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.

12.3 Guias STIC

- Guía 800 - Glosario de Términos y Abreviaturas del ENS
- Guía 801 - Responsables y Funciones en el Esquema Nacional de Seguridad
- Guía 802 - Auditoría del Esquema Nacional de Seguridad
- Guía 803 - Valoración de sistemas en el Esquema Nacional de Seguridad
- Guía 804 - Medidas de implantación del Esquema Nacional de Seguridad
- Guía 805 - Política de Seguridad de la Información
- Guía 806 - Plan de Adecuación del Esquema Nacional de Seguridad.
- Guía 807 - Criptología de empleo en el Esquema Nacional de Seguridad
- Guía 808 - Verificación del cumplimiento de las medidas en el ENS.
- Guía 809 - Declaración de Conformidad del Esquema Nacional de Seguridad