UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Esquema Nacional de Seguridad: Protección de una infraestructura crítica del sector administración

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Jorge Revert Enguix

Tutor: Juan Vicente Oltra Gutiérrez

Curso 2018-2019

Resum

El present treball consisteix en l'estudi de l'Esquema Nacional de Seguretat i la seua normativa, permetent-nos mitjançant un anàlisi de les infraestructures crítiques i el coneixement dels seus sistemes d'informació, elaborar una guia que servisca per a realitzar una correcta adequació a l'Esquema Nacional de Seguretat complint les corresponents mesures de seguretat necessàries per a aquestes estructures.

Aquesta guia servirà per a desenvolupar una aplicació que permeta tant als auditors com als responsables de la protecció d'aquests sistemes crítics, una ràpida i còmoda avaluació de les seues infraestructures verificant que compleixen amb el reglament.

Paraules clau: Esquema Nacional de Seguretat, ENS, Infraestructura Crítica, Auditoria

Resumen

El presente trabajo consiste en el estudio del Esquema Nacional de Seguridad y su normativa, permitiéndonos mediante un análisis de las infraestructuras críticas y el conocimiento de sus sistemas de información, elaborar una guía que sirva para realizar una correcta adecuación al Esquema Nacional de Seguridad cumpliendo las correspondientes medidas de seguridad necesarias para dichas estructuras.

Esta guía servirá para desarrollar una aplicación que permita tanto a los auditores como a los responsables de la protección de estos sistemas críticos una rápida y cómoda evaluación de sus infraestructuras verificando que cumplen con el reglamento.

Palabras clave: Esquema Nacional de Seguridad, ENS, Infraestructura Crítica, Auditoría

Abstract

This work consists in the study of the National Security Scheme and its regulations, allowing us through an analysis of the critical infrastructures and the knowledge of its information systems, to prepare a guide that serves to make a correct adaptation to the National Security Scheme acomplishing with the corresponding security measures necessary for these structures.

This guide will be used to develop an application that allows the auditors and those responsible for the protection of these critical systems a quick and convenient evaluation of their infrastructures verifying that they accomplish with the regulations.

Key words: National Security Scheme, NHIS, Critical Infrastructure, Audit

Índice general

CAPÍTULO 1
Introducción

El uso de las nuevas tecnologías y los Sistemas de la Información ha propiciado que tareas antes realizadas de forma manual, ahora se basen en el uso de estos medios. Debido a esto, multitud de actividades se sustentan o basan sus funciones en el uso de la informática, un cambio que no solo implica una mejora en la calidad de vida, sino que también implica la aparición de nuevas amenazas.

Estos riesgos pueden resultar insignificantes o muy poco perjudiciales en algunos casos, mientras que en otros donde las funciones realizadas sean de vital importancia o se gestione información tanto reservada como sensible, cualquier vulnerabilidad supone un gran peligro, siendo necesario proteger estos sistemas o comunicaciones para evitar daños sobre ellos que conlleven grandes pérdidas en la sociedad.

1.1 Motivación

En el ámbito de la informática, la seguridad es un tema muy importante, ya que la mayoría de tareas se encuentran automatizadas y casi cualquier sistema o aplicación almacena información, tanto propia como de los usuarios. Por este motivo es necesario conocer los riesgos y vulnerabilidades para poder anticiparte y ser capaz de prevenir futuros problemas.

En mi actual trabajo he tenido contacto con algunas entidades públicas y he comprobado de primera mano la necesidad de cuidar información como datos personales de la misma forma que proteger tanto los sistemas como las comunicaciones para impedir que se pueda acceder a esos datos sensibles cuando no son de dominio público.

La motivación de este trabajo es adquirir conocimientos en la protección de sistemas de la información y combinado con lo aprendido durante los estudios del grado ser capaz de realizar una aplicación que sirva de guía para ayudar tanto a empresas como a auditores a detectar y cubrir sus vulnerabilidades con mayor facilidad.

1.2 Objetivos

Para la consecución del trabajo se persigue una premisa principal que es elaborar una guía con las medidas de seguridad a cumplir en una infraestructura crítica en conformidad al Esquema Nacional de Seguridad. Para ello se deben alcanzar distintos objetivos:

- Localizar, en el Esquema Nacional de Seguridad y su entorno (directrices, normas asociadas) aquellas actuaciones del profesional relacionadas con la protección de la información.
- Caracterizar las infraestructuras críticas principales, con un estudio descriptivo de los elementos de sus sistemas de información más relevantes.
- Identificadas las infraestructuras críticas en sus tipos más comunes, relacionar las medidas de seguridad necesarias para el cumplimiento de la normativa.

Con los objetivos cumplidos se va a desarrollar una aplicación para ayudar a evaluar los sistemas de las infraestructuras críticas.

1.3 Impacto esperado

Con el resultado del proyecto se busca exponer un producto que facilite tanto a los auditores como a las empresas o encargados de los correspondientes sistemas de la información el cumplimiento de la normativa del Esquema Nacional de Seguridad. Esta aplicación no solo permitirá evaluar la seguridad de las estructuras consideradas críticas, también proporcionará los medios para superar su correspondiente auditoría.

1.4 Metodología

Para la elaboración de la aplicación se pretende en primer lugar, realizar un estudio teórico sobre el Esquema Nacional de Seguridad y su ámbito de aplicación en las distintas entidades del sector Administración, permitiendo así conocer el alcance de la normativa para el profesional informático.

Acto seguido, se realizará un estudio sobre las infraestructuras críticas, centrándose en el sector administración para determinar qué medidas de seguridad se han de evaluar, proporcionando así los distintos objetivos a cubrir durante la aplicación de la norma de seguridad.

Posteriormente, se desarrollará una guía que recoja las medidas que ha de cumplir un sistema con las características previamente exploradas para adecuarse al Esquema Nacional de Seguridad.

Finalmente, se elaborará una aplicación que permita de forma ágil y sencilla evaluar todas las premisas recogidas en la guía elaborada para garantizar la correcta protección del sistema.

1.5 Estructura de la memoria

La información que se va a encontrar en el trabajo se encuentra estructurada en varias partes que justifican la consecución de los objetivos. El contenido que vamos a encontrar es el siguiente:

1. Estado del arte: Introducción teórica al Esquema Nacional de Seguridad y su normativa asociada. Ámbito de aplicación para el profesional informático. Se realiza un estudio del Esquema Nacional de Seguridad, desde su origen hasta su posterior modificación reseñando el marco de aplicación donde se va actuar.

2. Infraestructuras críticas: identificación de las mismas. Se muestran las características de una infraestructura crítica, haciendo hincapié en las que pertenecen al sector administración.

3. Guía para la implementación de las medidas de seguridad necesarias acorde de una infraestructura crítica. Se elabora una lista con las disposiciones a cumplir para que las estructuras estén acordes al Esquema Nacional de Seguridad.

CAPÍTULO 2
Estado del arte

Los avances en las tecnologías de la información y las comunicaciones afectan a la sociedad, incluyendo de tal forma a las administraciones públicas, permitiendo así su modernización favoreciendo el empleo y la aplicación de las nuevas técnicas y medios electrónicos para desarrollar sus actividades y permitir a los ciudadanos relacionarse con la Administración utilizando estos medios.

Dicha transformación digital que surgió en su momento en el Sector Público necesitaba de una regulación para la protección de la información y los servicios provistos, previniendo así acciones malintencionadas o ilícitas (como podemos destacar las ciberamenazas), los errores o fallos y posibles accidentes o desastres.

2.1 Origen del Esquema Nacional de Seguridad

Esta necesidad de proporcionar una normativa que regulara la actualización de las administraciones en relación a las nuevas tecnologías propició la aparición de una Ley que sentaría las bases para la seguridad electrónica de las administraciones.

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

El principal objetivo de la aprobación de esta ley era regular el derecho de los ciudadanos a consagrar su derecho a comunicarse con las Administraciones por medios electrónicos estableciéndolo como obligación para dichas Administraciones.

Tal derecho se hacía efectivo de modo real con la obligación de poner a disposición de ciudadanos y empresas al menos un punto de acceso general mediante el cual los usuarios pudieran, de forma sencilla, acceder a la información y servicios de su competencia, presentar solicitudes y recursos, poder realizar trámites de audiencia, efectuar pagos o acceder a notificaciones y comunicaciones remitidas por la Administración Pública.

Dentro del reconocimiento del derecho a utilizar estas herramientas se pretendía crear también las condiciones de confianza para su uso, mediante las medidas

oportunas, para garantizar derechos fundamentales como la intimidad y la protección de datos de carácter personal, promoviendo así un mejor funcionamiento de interno de las instituciones públicas con la ayuda del desarrollo de la sociedad de la información. [1]

Para asegurar el cumplimiento de estas bases proporcionando seguridad a los usuarios, encontramos el Artículo 42 Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad, donde se define este último de la siguiente forma:

> El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información

2.1.2. 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

Como consecuencia de la necesidad comentada de proteger tanto los sistemas como las comunicaciones electrónicas surge este Real Decreto con el siguiente objeto:

> 1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.
> 2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias. [2]

El Esquema Nacional de Seguridad se elaboró a la luz del estado del arte y de los principales referentes en materia de seguridad de la información provenientes de la Unión Europea, OCDE, normalización nacional e internacional y actuaciones similares en otros países, entre otros. [3]

Es el resultado de un trabajo coordinado por el Ministerio de Política Territorial y función Pública junto con el Centro Criptológico Nacional (CCN) y la participación de todas las Administraciones Públicas, a través de los órganos colegiados con competencias en materia de administración digital. También se ha tenido presente la opinión de las asociaciones de la Industria del sector TIC. [3]

Su elaboración pretende que se cumplan diversos objetivos:

1. Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

2. Promover la gestión continuada de la seguridad.

3. Motivar la prevención detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.

4. Impulsar un tratamiento homogéneo de la seguridad facilitando la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades.

5. Servir como modelo para buenas prácticas. [3]

2.2 Modificación del Esquema Nacional de Seguridad

Debido al incremento en el uso de los servicios electrónicos, así como los avances en los mismos, la legislación quedaba desfasada y en constante modificación. Como consecuencia, surgen dos nuevas leyes, la 39/2015 y la 40/2015, ambas de 1 de octubre, siendo la primera de ellas la encargada de regular el procedimiento administrativo común y la segunda el régimen jurídico del sector público. [4]

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas recopila los derechos de las personas en sus relaciones con las Administraciones Públicas, todo lo relacionado a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. Por otro lado, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público trata, entre otras cuestiones, tanto la seguridad como la protección de datos personales en relación al uso de los medios electrónicos. [3]

En esta última se recogen, con las adaptaciones necesarias, normas contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público, regulando distintas materias que lo demandaban, adaptándolas como corresponde a un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual. Se establece asimismo la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos. [5]

Se puede encontrar, por tanto, referencias al Esquema Nacional de Seguridad y su papel e importancia en la seguridad de los sistemas, como se refleja en el artículo 46:

> Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenti-

> cidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados. [5]

Para declarar nuevamente el Esquema Nacional de Seguridad en el artículo 156:

> El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.[5]

Debido a la aparición de estas nuevas leyes, la experiencia obtenida en su implantación, la evolución de las tecnologías y las ciberamenazas así como del contexto regulatorio internacional y europeo, se realizó una modificación del Real Decreto 3/2010, de 8 de enero, antes mencionado, en el Real Decreto 951/2015, cuyos cambios conforman y definen el Esquema Nacional de Seguridad que se aplica actualmente. [6]

A partir de la entrada en vigor de estas nuevas leyes, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos quedaría derogada, de ahí la modificación y adaptación del Real Decreto 3/2010, de 8 de enero.

2.3 Ámbito de aplicación del Esquema Nacional de Seguridad

En el artículo 2 de la Ley 11/2007 se establece el ámbito de aplicación del Esquema Nacional de Seguridad, que conforma los siguientes elementos:

- La Administración General del Estado, 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.
- Los ciudadanos en sus relaciones con las Administraciones Públicas.
- Las relaciones entre las distintas Administraciones Públicas.

Se excluyen no obstante los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales y sus normas de desarrollo. [7]

Visto esto, los servicios o sistemas a los que afecta el Esquema Nacional de Seguridad son:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información accesibles electrónicamente por los ciudadanos.
- Sistemas de Información para el ejercicio de derechos.
- Sistemas de Información para el cumplimiento de deberes.
- Sistemas de Información para recabar información y estado del procedimiento administrativo. [7]

Estas estructuras estarán al cargo de un profesional informático, ya sea para su funcionamiento como para su evaluación o auditoría, por tanto debe ser capaz de adaptar o evaluar estos sistemas conforme al Esquema Nacional de Seguridad.

2.4 Adecuación al Esquema Nacional de Seguridad

Para regular las funciones y la seguridad de los sistemas conforme a la normativa hay que realizar un plan de adecuación elaborado por el Responsable de Seguridad del sistema. Este plan de adecuación [8] deberá contener 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. Análisis de riesgos
7. Declaración de aplicabilidad de las medidas del Anexo II del ENS y las requeridas por el tratamiento de datos de carácter personal, si los hubiera
8. Insuficiencias del sistema (gap analysis)
9. Plan de mejora seguridad, incluyendo plazos estimados de ejecución

El estudio de este trabajo se centrará principalmente en la declaración de aplicabilidad de las medidas del Anexo II del Esquema Nacional de Seguridad para la evaluación los distintos sistemas y comprobar que cumplen la norma, sirviendo de ayuda tanto para el propio Responsable de Seguridad del sistema como para los auditores.

Guías similares a la propuesta que aborden la aplicación y el cumplimiento del Esquema Nacional de Seguridad hay de diversa índole, destacando sobre todo las proporcionadas por el Centro Criptológico Nacional, que se encarga de

elaborar diferentes documentos para facilitar el cumplimiento de la seguridad de las tecnologías de la información y las comunicaciones (STIC). Dentro de estos manuales podemos destacar:

- CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS. [11]
- CCN-STIC-804 ENS. Guía de implantación. [10]
- CCN-STIC-802 Auditoría del ENS. [9]

Estos documentos se basan en la aplicación o verificación del cumplimiento del Esquema Nacional de Seguridad en los diferentes sistemas cuya aplicación sea necesaria. También podemos encontrar fuera del CCN algunas guías de implantación de la normativa, como la desarrollada por Ametic que incluye un caso práctico [12].

2.5 Crítica al estado del arte

Dentro de la ETSINF se pueden encontrar diversos trabajos basados en el Esquema Nacional de Seguridad y su aplicación como por ejemplo:

- Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. [13]
- El perito ante el ENS. [14]
- Esquema Nacional de Seguridad: Protección de una infraestructura crítica hospitalaria. [15]

El primero consta de un análisis y estudio de técnicas y amenazas sobre los sistemas de la información con efectos en estructuras bajo la normativa.

El segundo se basa en la caracterización de las estructuras críticas y que pasos o normas ha de seguir un auditor cuando trata este tipo de infraestructuras basándose en el marco de la normativa del Esquema Nacional de Seguridad.

El último consta del desarrollo de una aplicación que sirva a los auditores para la evaluación de los sistemas de una infraestructura crítica hospitalaria.

Observándolos detenidamente se pretende, siguiendo con la misma línea que el último de los trabajos analizados, realizar una aplicación que pueda servir al resto de infraestructuras críticas, no centrándose solamente en única de ellas, sirviendo para que los auditores tengan una herramienta que les facilite su labor en estas instalaciones siguiendo con la idea que presentaba el segundo de los trabajos visto.

2.6 Propuesta

La propuesta diferencial de este trabajo es por tanto, proporcionar una herramienta que facilite la evaluación o auditoría de los sistemas de la información a

los que afecte la normativa del Esquema Nacional de Seguridad y que sirva para cualquier infraestructura crítica, permitiendo así ayudar a la recopilación de datos en estas estructuras tan vitales para la sociedad donde la seguridad juega un papel fundamental.

CAPÍTULO 3
Infraestructuras críticas: identificación de las mismas

Una vez analizada la normativa del Esquema Nacional de Seguridad, su estado y el ámbito de aplicación sobre el que se va a actuar, se pretende investigar las infraestructuras críticas para poder aplicar correctamente el reglamento sobre sus sistemas de información y comunicaciones.

Para conocer mejor que tipo de estructuras son, se puede utilizar la definición que se le otorga en el artículo 2 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas: [16]

> Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales

Con esta definición se comprende la importancia que tiene la seguridad en ellas, hasta tal punto que cualquier incidente, así como una interrupción en sus servicios acarrearía graves consecuencias sobre el normal desarrollo de las actividades básicas de la sociedad. Debido a esto surge la Ley 8/2011 [16] mencionada anteriormente, donde se valora la importancia de dichas infraestructuras así como la necesidad de su protección desde el plano tanto de la seguridad física como en el de la protección de las tecnologías de la información y las comunicaciones.

> Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población. [16]

Para lograr su consecución se requiere la aplicación de diferentes planes de actuación:

1. El Plan Nacional de Protección de las Infraestructuras Críticas.
2. Los Planes Estratégicos Sectoriales.
3. Los Planes de Seguridad del Operador.
4. Los Planes de Protección Específicos.
5. Los Planes de Apoyo Operativo. [16]

Para regular los mismos y el resto de medidas promulgadas para la seguridad de las estructuras surge el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. [17]

3.1 Instrumentos de planificación

Dentro de las medidas desarrolladas para proteger las infraestructuras críticas, este estudio se centra en los instrumentos de planificación, que se encargarán de, mediante la revisión del Centro Nacional de Protección de Infraestructuras Críticas, la identificación y designación de infraestructuras críticas, así como la evaluación de la necesidad de mejorar su protección.

3.1.1. El Plan Nacional de Protección de las Infraestructuras Críticas

Está elaborado por la Secretaría de Estado de Seguridad y dirigido a mantener seguras las infraestructuras españolas que proporcionan los servicios esenciales a la sociedad. Establecerá también los criterios y las directrices precisas para movilizar las capacidades operativas de las Administraciones públicas en coordinación con los operadores críticos, articulando las medidas preventivas necesarias para asegurar la protección permanente. [17]

Los distintos niveles de seguridad contendrán la adopción graduada de dispositivos y medidas de protección ante situaciones de incremento de la amenaza contra las infraestructuras estratégicas nacionales.

3.1.2. Los Planes Estratégicos Sectoriales

Son los instrumentos de estudio y planificación con alcance en todo el territorio nacional que permitirán conocer, en cada uno de los sectores contemplados, cuáles son los servicios esenciales proporcionados a la sociedad, el funcionamiento general de éstos, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento. [17]

Cada uno de los Planes Estratégicos Sectoriales estarán basados en un análisis general de riesgos donde se contemplen las vulnerabilidades y amenazas potenciales, tanto de carácter físico como lógico, que afecten al sector o subsector en cuestión en el ámbito de la protección de las infraestructuras estratégicas.

Los elementos mínimos que se recogerán son:

- Análisis de riesgos, vulnerabilidades y consecuencias a nivel global.
- Propuestas de implantación de medidas organizativas y técnicas necesarias para prevenir, reaccionar y, en su caso, paliar, las posibles consecuencias de los diferentes escenarios que se prevean.
- Propuestas de implantación de otras medidas preventivas y de mantenimiento (por ejemplo, ejercicios y simulacros, preparación e instrucción del personal, articulación de los canales de comunicación precisos, planes de evacuación o planes operativos para abordar posibles escenarios adversos).
- Medidas de coordinación con el Plan Nacional de Protección de las Infraestructuras Críticas.

3.1.3. Los Planes de Seguridad del Operador

Son los documentos estratégicos que definen las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.

Estos planes deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos. [17]

3.1.4. Los Planes de Protección Específicos

Son los informes operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de sus infraestructuras críticas.

Estos incluirán todas aquellas medidas que los respectivos operadores críticos consideren necesarias en función de los análisis de riesgos realizados respecto de las amenazas, sobre sus activos, incluyendo los sistemas de información.

Cada Plan de Protección Específico deberá contemplar la adopción tanto de medidas permanentes de protección, sobre la base de lo dispuesto en el párrafo anterior, como de medidas de seguridad temporales y graduadas, que vendrán en su caso determinadas por la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien como consecuencia de las comunicaciones que las autoridades competentes puedan efectuar al operador crítico en relación con una amenaza concreta sobre una o varias infraestructuras por él gestionadas. [17]

3.1.5. Los Planes de Apoyo Operativo

Son los documentos operativos donde se deben plasmar las medidas concretas a poner en marcha por las Administraciones Públicas en apoyo de los operadores críticos para la mejor protección de las infraestructuras críticas.

Cada uno de ellos deberá contemplar, si las instalaciones lo precisan, las medidas planificadas de vigilancia, prevención, protección y reacción que deberán adoptar las unidades policiales y, en su caso, de las Fuerzas Armadas, cuando se produzca la activación del Plan Nacional de Protección de las Infraestructuras Críticas, o bien de confirmarse la existencia de una amenaza inminente sobre dichas infraestructuras. Estas medidas serán siempre complementarias a aquellas de carácter gradual que hayan sido previstas por los operadores críticos en sus respectivos Planes de Protección Específicos. [17]

3.2 Ámbito de aplicación de la normativa del Esquema Nacional de Seguridad

La protección de estos servicios fundamentales se sustenta cada vez más en el correcto funcionamiento de sistemas de información y comunicaciones. De este modo, la Ciberseguridad cobra especial importancia de cara a proteger y garantizar el correcto desempeño de las infraestructuras críticas que se basan en dichos sistemas tecnológicos. Un incidente de Ciberseguridad podría afectar a la confidencialidad, integridad o disponibilidad de los sistemas, siendo éste último componente el que debe primar a la hora de garantizar la protección tanto de las infraestructuras críticas como de los servicios esenciales que éstas proporcionan. [19]

Respecto a esto, los sistemas de información y sus comunicaciones en una infraestructura crítica deben estar tecnológicamente protegidos, incluido el sector de la administración, que forma parte de la coordinación del Plan Nacional de Protección de las Infraestructuras Críticas visto anteriormente e involucrado en la coordinación y colaboración en la planificación de las medidas de seguridad a implantar.

Para gestionar la protección de las redes y sistemas de información en las infraestructuras críticas surge el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [18] cuyo objeto se define como:

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario

Estas medidas se aplicarán a las entidades que presten servicios esenciales para la comunidad y que a su vez, dependan de las redes y sistemas de información para el desarrollo de su actividad.

En el artículo 16 se nombran las obligaciones de seguridad de estas funciones básicas y de los proveedores de servicios digitales donde se establece las disposiciones reglamentarias, instrucciones y guías elaboradas que tendrán en cuenta, entre otros, los requisitos en materia de seguridad de la información, a las que estuviera sometido el operador en virtud de otras normas, como el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero. [18]

Como consecuencia, todos los sistemas críticos que manejen información del sector público deberán adaptarse a la norma del Esquema Nacional de Seguridad. Estas estructuras críticas donde se aplique se van a encontrar mayoritariamente en el sector estratégico de la administración

CAPÍTULO 4

Guía para la implementación de las medidas de seguridad necesarias acorde una infraestructura crítica

Vista la importancia y necesidad de las infraestructuras críticas de mantener la seguridad de sus redes y sistemas de información, se pretende mostrar y recopilar de forma intuitiva una serie de medidas para garantizar su correcta protección, cumpliendo así con la normativa recogida 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. [2]

Estas medidas de seguridad se recogen en el Anexo 2 del Real Decreto 3/2010 [2] y son proporcionales a:

- Las dimensiones de seguridad relevantes en el sistema a proteger.
- La categoría del sistema de información a proteger.

La categoría del sistema viene determinada por las distintas dimensiones de seguridad, así como por los niveles que adquieran. Los distintos niveles (ALTO, MEDIO y BAJO) vienen marcados por las consecuencias que un incidente de seguridad pueda suponer sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados, siendo ALTO el que represente resultados más graves sobre la entidad. Las dimensiones de seguridad que se utilizan para evaluar los diferentes sistemas son:

- Disponibilidad [D].
- Autenticidad [A].
- Integridad [I].
- Confidencialidad [C].
- Trazabilidad [T].

Según la normativa, un sistema pertenecerá a una categoría cuando una de sus dimensiones alcance dicho nivel y ninguna sea superior. En el caso de cualquier

infraestructuras críticas se puede asegurar que es de nivel ALTO debido a su propia definición, donde se establece que su funcionamiento es indispensable, por lo que el nivel para la Disponibilidad [D] es ALTO. Esto no significa que sea la única dimensión con nivel ALTO, pero sirve para demostrar que todas infraestructuras críticas por definición son de categoría ALTA.

Una vez categorizado, utilizando el Anexo 2 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [2] se recogerán las medidas a implantar para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos.

4.1 Marco organizativo [org]

Se constituye por un conjunto de medidas relacionadas con la organización global de la seguridad. [2]

4.1.1. Política de seguridad [org.1]

Documento escrito que ha de contener lo siguiente:

- Los objetivos o misión de la organización.
- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

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

4.1.2. Normativa de seguridad [org.2]

Documentos que describan:

- El uso correcto de equipos, servicios e instalaciones.
- Lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas.

4.1.3. Procedimientos de seguridad [org.3]

Se requerirán informes con la siguiente información:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.

4.1.4. Proceso de autorización [org.4]

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:

- Utilización de instalaciones, habituales y alternativas.
- Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Entrada de aplicaciones en producción.
- Establecimiento de enlaces de comunicaciones con otros sistemas.
- Utilización de medios de comunicación, habituales y alternativos.
- Utilización de soportes de información.
- Utilización de equipos móviles.
- Utilización de servicios de terceros, bajo contrato o Convenio.

4.2 Marco operacional [op]

Constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin. [2]

4.2.1. Planificación [op.pl]

Análisis de riesgos [op.pl.1]

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

- Identifique y valore cualitativamente los activos más valiosos del sistema.
- Identifique y cuantifique las amenazas posibles.
- Identifique las vulnerabilidades habilitantes de dichas amenazas.

- Identifique y valore las salvaguardas adecuadas.
- Identifique y valore el riesgo residual

Arquitectura de seguridad [op.pl.2]

Son requeridos planteamientos integrales detallados de diversos aspectos:

- Documentación de las instalaciones (áreas y puntos de accesos)
- Documentación del sistema (equipos, redes, puntos de acceso)
- Esquemas de líneas de defensa.
- Sistemas de identificación y autenticación de usuarios.
- Sistema de gestión, organización y control de los recursos relativos a la seguridad de la información.
- Sistema de gestión de seguridad de la información con actualización y aprobación periódica.
- Controles técnicos internos (validación de datos de entrada, salida y datos intermedios)

Adquisición de nuevos componentes [op.pl.3]

Se deberá realizar un proceso formal donde se atienda a los análisis de riesgos ([op.pl.1]), se siga la arquitectura de seguridad escogida ([op.pl.2]) y se tomen en cuenta las necesidades técnicas de formación y de financiación, para añadir nuevos componentes al sistema.

Dimensionamiento / Gestión de capacidades [op.pl.4]

Se deberán cubrir las siguientes necesidades antes de la puesta en explotación:

- Procesamiento.
- Almacenamiento de información.
- Necesidades de comunicación.
- Personal.
- Instalaciones y medios auxiliares.

Componentes certificados [op.pl.5]

Los sistemas deben estar reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información en cuanto a sus funcionalidades de seguridad. Todo ello se detalla en una instrucción técnica de seguridad.

4.2.2. Control de acceso [op.acc]

Identificación [op.acc.1]

Se regulará la identificación de los usuarios al sistema de tal forma que se pueda saber quién y qué se ha realizado en cada momento y con que permisos mediante un identificador único diferenciado en función de los roles que ocupe en el sistema.

Requisitos de acceso [op.acc.2]

Se regulara la utilización de los recursos del sistema a cada usuario en función de sus privilegios (particularmente a ficheros o registros de configuración y componentes del sistema).

Segregación de funciones y tareas [op.acc.3]

Para las tareas críticas se requerirá la concurrencia de dos o más personas para evitar que un individuo pueda abusar de sus derechos.

Proceso de gestión de derechos de acceso [op.acc.4]

Los derechos de acceso se gestionan en función de la necesidad de cada uno para realizar sus funciones, cuyos privilegios se componen desde limitarse a lo estrictamente necesario hasta poder conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

Mecanismo de autenticación [op.acc.5]

Se requiere la utilización de credenciales obtenidas tras registro previo. En caso de utilización de componentes lógicos o dispositivos físicos se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados. Estas credenciales se suspenderán tras un periodo definido de no utilización.

Acceso local (local logon) [op.acc.6]

Se regula el horario, fecha y lugar desde donde se accede al sistema, siendo necesario en ciertos puntos que este requiera una renovación de la autenticación del usuario.

Acceso remoto (remote login) [op.acc.7]

Debe establecerse una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.

4.2.3. Explotación [op.exp]

Inventario de activos [op.exp.1]

Se mantendrá un inventario actualizado de los elementos del sistema, detallando su naturaleza e identificando a su responsable.

Configuración de seguridad [op.exp.2]

Se prepararán los dispositivos para realizar las funcionalidades básicas requeridas y que no sea posible realizar ninguna acción de riesgo que no sea voluntaria.

Gestión de la configuración [op.exp.3]

Se debe gestionar continuamente la configuración de los elementos del sistema para mantener la configuración de seguridad ([op.exp.2]), se adapte a nuevas necesidades ([op.acc.4]), reaccione a vulnerabilidades informadas ([op.exp.4]) y responda a incidentes ([op.exp.7]).

Mantenimiento [op.exp.4]

Se regulará el equipamiento del sistema mediante un seguimiento de las novedades en el mantenimiento de los mismos, como sus defectos, actualizando cuando se considere oportuno en función del riesgo que se corra.

Gestión de cambios [op.exp.5]

Se analizarán todos los cambios que anuncie el fabricante o proveedor comprobando en un equipo equivalente, que no se encuentre en producción, si los cambios funcionan correctamente y sin reducir el rendimiento de sus funciones. Los cambios tratarán de no influir o que el impacto sea el menor en la prestación de los servicios.

Protección frente a código dañino [op.exp.6]

Se dispondrá de mecanismos de prevención y reacción frente a código dañino, conocido como "malware", con mantenimiento de acuerdo a las recomendaciones del fabricante.

Gestión de incidentes [op.exp.7]

Se debe disponer de un proceso integral para hacer frente a los incidentes que afecten a la seguridad del sistema, teniendo la capacidad de reportar los eventos, tomar decisiones urgentes, asignación de recursos para investigar las causas y poder evitar que vuelvan a aparecer.

Registro de la actividad de los usuarios [op.exp.8]

Se debe registrar la actividad de los usuarios para conocer quién realiza cada actividad, cuando y sobre qué información.

Registro de la gestión de incidentes [op.exp.9]

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que se conserven el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

Protección de los registros de actividad [op.exp.10]

Es necesario aplicar las siguientes medidas para proteger los registros del sistema y evitar que sean manipulados:

- Se determinará el periodo de retención de los registros.
- Se asegurará la fecha y hora ([mp.info.5]).
- Los registros no podrán ser modificados ni eliminados por personal no autorizado.
- Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

Protección de las claves criptográficas [op.exp.11]

Se protegerán las claves durante todo su ciclo de vida utilizando programas evaluados o dispositivos criptográficos certificados ([op.pl.5]) y empleando algoritmos acreditados por el Centro Criptológico Nacional.

4.2.4. Servicios externos [op.ext]

Contratación y acuerdos de nivel de servicio [op.ext.1]

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.

Gestión diaria [op.ext.2]

Se tendrá un control rutinario para regular que se cumplan las obligaciones del servicio y se pueda neutralizar cualquier desviación del margen de tolerancia acordado ([op.ext.1]). Es necesario también establecer el mecanismo y los procedimientos de coordinación para mantener los sistemas afectados por el acuerdo de uso y para coordinar posibles incidentes ([op.exp.7])

Medios alternativos [op.ext.9]

Se deberá disponer del servicio por medios alternativos (con las mismas garantías de seguridad) en caso de indisponibilidad del servicio contratado.

4.2.5. Continuidad del servicio [op.cont]

Análisis de impacto [op.cont.1]

Se debe analizar qué elementos son críticos para la prestación de cada servicio y el impacto que conllevaría su interrupción durante un periodo de tiempo.

Plan de continuidad [op.cont.2]

Se elaborará un plan de continuidad a seguir en caso de interrupción del servicio por parte de los medios habituales. En él, se debe detallar las funciones, responsabilidades y actividades a realizar, así como los medios alternativos que se van a utilizar.

Pruebas periódicas [op.cont.3]

Se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad.

4.2.6. Monitorización del sistema [op.mon]

Detección de intrusión [op.mon.1]

Se debe disponer de herramientas de detección o de prevención de intrusión.

Sistema de métricas [op.mon.2]

Se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido sobre el estado de la seguridad del sistema. Se recopilaran además datos para valorar el sistema de gestión de incidentes y la eficiencia del sistema de seguridad TIC (Recursos consumidos: horas y presupuesto).

4.3 Medidas de protección [mp]

Estas se centran en la protección de activos específicos, ajustándose, según su naturaleza, al nivel requerido en cada dimensión de seguridad.

4.3.1. Protección de las instalaciones e infraestructuras [mp.if]

Áreas separadas y con control de acceso [mp.if.1]

Los equipos se instalarán en diferentes áreas según su función, donde se controlará el acceso para su utilización.

Identificación de las personas [mp.if.2]

Se registrarán las entradas y salidas del personal para identificar a las personas que accedan a las zonas donde se encuentren los sistemas de información protegidos.

Acondicionamiento de los locales [mp.if.3]

Se requiere que el área donde se ubiquen los sistemas de información y sus elementos cumplan con las condiciones de temperatura y humedad para su correcto funcionamiento, así como su protección frente amenazas establecidas en el análisis de riesgos y posibles incidentes sobre el cableado.

Energía eléctrica [mp.if.4]

Se debe disponer de energía eléctrica en los locales donde se encuentren los equipos de forma que se garantice su actividad, su distribución y el correcto funcionamiento de las luces de emergencia. Además, se debe proporcionar suministro, en caso de fallo del abastecimiento general, para terminar de forma ordenada todos los procesos, evitando así pérdidas de información.

Protección frente a incendios [mp.if.5]

Se aplicará la normativa industrial pertinente para proteger los sistemas frente a incendios.

Protección frente a inundaciones [mp.if.6]

Se protegerán las zonas donde se encuentren los diferentes equipos y sus componentes para evitar incidentes causados por el agua.

Registro de entrada y salida de equipamiento [mp.if.7]

Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.

Instalación de alternativas [mp.if.9]

Se obliga a contar con instalaciones alternativas para trabajar en caso de indisponibilidad de las habituales, las cuáles deben disponer de las mismas garantías de seguridad que las normales.

4.3.2. Gestión del personal [mp.per]

Caracterización del puesto de trabajo [mp.per.1]

Se ha de definir las responsabilidades en materia de seguridad relacionadas con cada puesto de trabajo y definir los requisitos que se deben satisfacer por el trabajador en términos de confidencialidad. Quién vaya a ocupar el puesto debe ser escogido teniendo en cuentas estas condiciones.

Deberes y obligaciones [mp.per.2]

Se ha de informar a los trabajadores que utilicen el sistema, tanto personal interno como externo, de sus deberes y responsabilidades, especificándoles las medidas disciplinarias existentes así como su deber de confidencialidad (durante su tiempo de trabajo como posteriormente).

Concienciación [mp.per.3]

Se recordará al personal continuamente la normativa de seguridad para un buen uso de los sistemas, la necesidad de identificación de incidentes o actividades sospechosas y el procedimiento para reportar incidentes de seguridad, sean alarmas reales o falsas.

Formación [mp.per.4]

Se instruirá a los trabajadores en materias para el desempeño de sus funciones, destacando la configuración de los sistemas, la detección y reacción a incidentes y la gestión de la información en cualquier soporte que se encuentre.

Personal alternativo [mp.per.9]

Se debe garantizar la disponibilidad de personal alternativo para desempeñar las funciones en caso de indisponibilidad del habitual, que cumpla con las mismas garantías de seguridad.

4.3.3. Protección de los equipos [mp.eq]

Puesto de trabajo despejado [mp.eq.1]

Los puestos de trabajo han de estar despejados sin la presencia de material no requerido para la realización de la actividad que se vaya a efectuar, guardándose este en un lugar cerrado mientras no se utiliza.

Bloqueo de puestos de trabajo [mp.eq.2]

Se bloqueará el puesto de trabajo tras un tiempo de inactividad, requiriendo su autenticación para reanudar las funciones en curso. Si se supera cierto margen en cuanto al tiempo de inactividad se cancelarán, además, todas las sesiones abiertas desde ese equipo.

Protección de equipos portátiles [mp.eq.3]

Los equipos que deban salir de las instalaciones de la organización deben estar identificados y asociados a un responsable. Estos no deben tener, siempre que sea posible, claves de acceso remotos a la organización, así como su uso debe estar limitado a los servicios mínimos cuando se conecte a redes fuera del control de la institución, disponiendo de un canal para informar de pérdidas o sustracciones. La información que contengan de nivel alto debe encontrarse cifrada y se dispondrá de medios capaces de detectar si el equipo ha sido manipulado y activar los procedimientos de gestión de incidentes.

Medios alternativos [mp.eq.9]

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información en el caso de que fallen los medios habituales. Estos estarán sujetos a las mismas garantías de protección. Del mismo modo, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento.

4.3.4. Protección de las comunicaciones [mp.com]

Perímetro seguro [mp.com.1]

Se dispondrá de un sistema cortafuegos para separar la red interna del exterior, comprendido de dos o más equipos de distinto fabricante dispuestos en cascada. Se habilitarán además sistemas redundantes.

Protección de la confidencialidad [mp.com.2]

Se deben utilizar redes privadas virtuales para la comunicación fuera de las redes del propio domino de seguridad, empleando dispositivos hardware en el

establecimiento y utilización de la misma. Los algoritmos de uso serán acreditados por el Centro Criptológico Nacional y se emplearán productos certificados ([op.pl.5]).

Protección de la autenticidad y de la integridad [mp.com.3]

- Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información ([op.acc.5]).
- Se prevendrán ataques activos.
- Se aceptará cualquier mecanismo de autenticación de los previstos en normativa de aplicación.
- Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
- Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
- Se valorará positivamente el empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
- Se emplearán productos certificados ([op.pl.5]).

Segregación de redes [mp.com.4]

Se pretende acotar el acceso a la información, evitando así la propagación de incidentes de seguridad. Para ello se debe controlar la llegada de los usuarios a cada segmento de la red así como la salida de información disponible en cada segmento. Los puntos de interconexión entre los distintos sectores deben estar particularmente asegurados, mantenidos y monitorizados ([mp.com.1]).

Medios alternativos [mp.com.9]

Se dispondrá de medios alternativos de comunicación, con las mismas garantías de protección, para suplir a los medios habituales. Estos recursos garantizarán un tiempo máximo de entrada en funcionamiento.

4.3.5. Protección de los soportes de información [mp.si]

Etiquetado [mp.si.1]

Se etiquetarán los soportes de información para indicar el nivel de seguridad de la información contenida de mayor calificación. Los usuarios han de estar capacitados para entender el significado de las etiquetas.

Criptografía [mp.si.2]

Esta medida se aplica en particular a dispositivos removibles, los cuáles garantizarán la confidencialidad e integridad de la información contenida mediante el uso de mecanismos criptográficos. Se deben emplear tanto algoritmos acreditados por el Centro Criptológico Nacional como productos certificados ([op.pl.5]).

Custodia [mp.si.3]

Se mantendrá la diligencia y control de los soportes de información garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]), lógicas ([mp.si.2]) o ambas, respetando además las exigencias de mantenimiento del fabricante.

Transporte [mp.si.4]

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro mediante:

- Registro de salida que identifique al transportista que recibe el soporte para su traslado.
- Registro de entrada que identifique al transportista que lo entrega.
- Procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes si se detecta algún incidente.
- Utilización de medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.
- Gestión de claves ([op.exp.11]).

Borrado y destrucción [mp.si.5]

Se aplicará a todos los soportes susceptibles de almacenar información (electrónicos o no electrónicos), destruyéndose de forma segura en caso de no permitirse un borrado seguro, o que así se requiera por el procedimiento asociado al tipo de información contenida. En este proceso se emplearán productos certificados ([op. pl.5]).

4.3.6. Protección de las aplicaciones informáticas [mp.sw]

Desarrollo [mp.sw.1]

No se debe realizar el desarrollo de aplicaciones sobre el sistema de producción, utilizando otro sistema que utilice datos ficticios, salvo que se asegure el nivel de seguridad correspondiente. El sistema debe contar con mecanismos de

identificación y autenticación, dispositivos de protección de la información tratada y generación y tratamiento de pistas de auditoría.

La metodología que se ha de aplicar es la siguiente:

- Tomar en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
- Tratar específicamente los datos usados en pruebas.
- Permitir la inspección del código fuente.
- Incluir normas de programación segura.

Aceptación y puesta en servicio [mp.sw.2]

Para poder pasarla a producción, debe comprobarse el correcto funcionamiento de la aplicación, asegurándose que no se deteriora la seguridad de ningún componente y que se cumplen los criterios de aceptación en materia de seguridad. También se han de realizar inspecciones para comprobar el análisis de vulnerabilidades, las pruebas de penetración y el análisis de coherencia en la integración en los procesos, considerándose además la oportunidad de realizar una auditoría de código fuente.

4.3.7. Protección de la información [mp.info]

Datos de carácter personal [mp.info.1]

Cuando se traten datos de carácter personal se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo.

Calificación de la información [mp.info.2]

La información se ha de clasificar en función de lo establecido legalmente sobre su naturaleza, estableciendo su política de seguridad quién es el responsable de la misma, que se encargará de asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.

Se han de redactar 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; y precisando cómo se ha de realizar:

- Su control de acceso.
- Su almacenamiento.
- La realización de copias.
- El etiquetado de soportes.
- Su transmisión telemática.
- Cualquier otra actividad relacionada con dicha información.

Cifrado [mp.info.3]

La información con un nivel alto de confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión, encontrándose en claro solo mientras se está haciendo uso de ella.

Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2], mientras que para los soportes de información, se aplicará lo dispuesto en [mp.si.2].

Firma electrónica [mp.info.4]

Se utilizará como instrumento para comprobar la autenticidad e integridad de la información, utilizándose firmas electrónica cualificadas, que incorporen certificados y dispositivos cualificados de creación de firma, así como el empleo de productos certificados ([op.pl.5]).

Sellos de tiempo [mp.info.5]

Prevendrán la posibilidad del repudio posterior, aplicándose a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro, renovándose regularmente hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte. Para ello se utilizarán productos certificados ([op.pl.5]) o servicios externos admitidos ([op.exp.10]). Se utilizarán "sellos cualificados de tiempo electrónicos"que deben ser acordes con la normativa europea en la materia.

Limpieza de documentos [mp.info.6]

Se debe retirar de los documentos 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. Esta medida es especialmente relevante cuando el documento se difunde ampliamente, ya que su incumplimiento puede perjudicar, sobre todo, a la confidencialidad de la información.

Copia de seguridad (backup) [mp.info.9]

Se realizarán copias de seguridad que permitan recuperar datos perdidos con una antigüedad determinada las cuáles deben poseer el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. Estas 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.

4.3.8. Protección de los servicios [mp.s]

Protección del correo electrónico (e-mail) [mp.s.1]

Se debe estar asegurado frente a las amenazas propias de este servicio mediante la protección de la información distribuida por este medio, así como la prevención de los problemas generados tanto por correo no solicitado como por programas dañinos o código móvil de tipo «applet».

Se establecerán además normas de uso del correo electrónico por parte del personal determinado que contendrán:

- Limitaciones al uso como soporte de comunicaciones privadas.
- Actividades de concienciación y formación relativas a su uso.

Protección de servicios y aplicaciones web [mp.s.2]

Se deben tomar las respectivas medidas de seguridad para hacer frente a las amenazas en aquellos sistemas donde se publique información. Para ello hay que evitar, cuando la información tenga algún tipo de control de acceso, la posibilidad de acceder a ella obviando la autenticación, aplicando para ello diversas medidas:

- Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
- Se prevendrán ataques de manipulación de URL.
- Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».
- Se prevendrán ataques de inyección de código.
- Se prevendrán intentos de escalado de privilegios.
- Se prevendrán ataques de «cross site scripting».
- Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».

Para ello se emplearán «certificados cualificados de autenticación del sitio web» acordes a la normativa europea en la materia.

Protección frente a la denegación de servicios [mp.s.8]

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service) que consistirán en:

- Planificar y dotar al sistema de capacidad suficiente para atender a la carga prevista con holgura.
- Desplegar tecnologías para prevenir los ataques conocidos.
- Establecer un sistema de detección de contra estos ataques.
- Establecer procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.
- Impedir el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Medios alternativos [mp.s.9]

Se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales, los cuales estarán sujetos a las mismas garantías de protección que los medios usuales.

CAPÍTULO 5
Diseño de la solución

Una vez que se conocen las medidas de seguridad que debe cumplir cualquier infraestructura crítica, se va a elaborar una aplicación que permita de forma sencilla revisar dichas medidas, ya sea por un auditor al evaluar los sistemas o como guía a los mismos responsables de la seguridad de los equipos.

5.1 Arquitectura del sistema

Para la elaboración de la aplicación se ha seguido el patrón modelo-vista-controlador, que sirve de referencia para distinguir las tres partes o capas de la aplicación, separando así la parte visual de la parte lógica. En esta arquitectura cada capa tendrá una función diferenciada que, conectadas entre sí, logran el correcto desempeño la funcionalidad.

En la parte del modelo se definirá la información que maneja la aplicación, así como las operaciones que se hagan sobre ella, ya sea de consulta, actualización... Es la capa que conectará con la base de datos, con la que interaccionará para realizar sus funciones y gestionar los datos que se le presentarán al usuario.

La capa vista muestra las interfaces que se van a visualizar por el usuario y que le van a permitir el navegar y utilizar la aplicación.

El controlador, por su parte, actúa como intermediario entre las anteriores capas mencionadas, permitiendo que las acciones realizadas por el usuario se manejen y realicen las operaciones pertinentes, ya sea mediante peticiones al modelo para mostrar o actualizar información o como para gestionar algún evento dentro de la propia interfaz.

5.2 Diseño detallado

5.2.1. Modelo

Aquí se encontrarán clases que definirán los objetos que utilizará la aplicación, que se corresponden, a su vez, con la información que se encontrará en la base de datos. Cabe destacar tres clases necesarias, que permitirán la creación de

nuevas auditorías, la visualización de las medidas y almacenar el resultado de la evaluación.

Auditoria

Esta clase recoge el objeto Auditoria, que consiste en un identificador único y una descripción para diferenciar cada auditoría que se crea y poder así asociar cada una a las medidas que se evalúan.

Medidas

Recoge las medidas que se encuentran en la guía desarrollada en este trabajo, identificadas por un id (como puede ser [mp.info.6]), su título y su descripción para orientar sobre la medida que se está evaluando. Esta clase solo ofrecerá métodos de consulta, ya que no se va a modificar ninguna de las normas.

Medidas Auditadas

Podría definirse como la unión de las dos anteriores, ya que permitirá asociar para cada medida, que auditoría la evalúa y los valores que se recopilan en cada una. Consta por tanto del identificador de auditoría, del id de la medida que corresponde, si ha sido auditada favorable o desfavorablemente, texto con los documentos, el texto con los muestreos y las observaciones.

5.2.2. Vista

Inicio

Contiene la interfaz que se mostrará al arrancar la aplicación, donde se podrá elegir entre crear una nueva auditoría, cargar una ya existente o salir de la aplicación.

Nueva Auditoria

Ventana muy sencilla que permitirá introducir el título de la infraestructura que se evalúa para, a continuación, crear una nueva auditoría.

Cargar Auditoria

Interfaz que cargará las auditorías existentes en base de datos y las mostrará para seleccionarlas y poder seguir evaluando la infraestructura.

Evaluacion Medidas

Se podría considerar la ventana más importante, ya que en ella se muestra la medida que se está evaluando, con su descripción, donde se indicará si se evalúa

o no, los documentos que se le puedan presentar, los muestreos y las observaciones que se consideren pertinentes. Desde esta interfaz se podrá cambiar de norma a evaluar y guardar los datos introducidos. El diseño de esta ventana pretende recopilar el contenido que se evalúa en cada medida de forma similar a la guía CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS [11].

5.2.3. Controlador

Recopilará los métodos necesarios para mostrar la información al usuario, ya sea cargando las medias en la interfaz diseñada para su evaluación como mostrando las auditorías existentes para su carga. Se encargará también de guardar las evaluaciones realizadas sobre cada medida y gestionará también los cambios de interfaz, las acciones que pueda hacer el usuario...

5.3 Tecnología utilizada

5.3.1. Java

La aplicación se ha desarrollado en lenguaje Java, que es un lenguaje de programación orientado a objetos y una plataforma informática comercializada por primera vez en 1995 por Sun Microsystems[1]. Se ha utilizado este lenguaje de programación por la familiaridad con su uso debido a su estudio y utilización durante el grado.

5.3.2. JavaFX

Para dar apariencia a la aplicación y gestionar las interfaces se ha escogido JavaFX, ya que permite crear aplicaciones tanto para escritorio, como para móvil o sistemas embebidos construidos sobre Java.[2] Esto permitía crear una aplicación que fuera "portable", aprovechando así las ventajas que ofrece.

5.3.3. SQL

Para la gestión de la información se ha elegido SQL, que es un lenguaje estándar para almacenar, manipular y recuperar datos en bases de datos. [20] En algunas asignaturas del grado se ha estudiado y tratado este lenguaje, por lo cual es una buena opción conocida para el tratamiento de la información de la aplicación.

[1] https://java.com/es/download/faq/whatis_java.xml
[2] https://openjfx.io/

5.3.4. Scene Builder

Para la manipulación de las interfaces, se ha escogido el uso de Scene Builder, con el cual se había trabajado ligeramente, por su sencillez para diseñar interfaces de usuario[3], permitiendo de forma visual gestionar las ventanas de la aplicación.

5.3.5. Eclpise

Como entorno de desarrollo, se ha utilizado Eclipse, debido a que es un entorno sobre el que se han desarrollado multitud de proyectos durante los estudios y hay cierta confianza en su uso.

[3]https://gluonhq.com/products/scene-builder/

CAPÍTULO 6
Desarrollo de la solución propuesta

Para la realización de la aplicación siguiendo el diseño explicado, se ha iniciado el desarrollo por las interfaces, creando en primer lugar todas las ventanas por las que podrá navegar el usuario. Con las interfaces diseñadas, se ha establecido la navegación, permitiendo que al pulsar los distintos botones se realicen los cambios de ventana pertinentes.

En el siguiente paso se han introducido los valores necesarios en la base de datos, los correspondientes a las medidas, que no las debe crear la aplicación si no solo consultarlas. Estos valores son los que se han desarrollado durante este trabajo.

A continuación, se comprueba que la creación de una nueva auditoría funciona según lo esperado, lo cual presentaba distintos problemas, sobre todo a la hora de cargar las medidas correctamente cuando se iniciaba la auditoría. Cuando se consiguen visualizar correctamente, cargando los textos en sus correspondientes campos, se implementa tanto la navegación entre las distintas medidas, como su inserción en la base de datos cuando se guarda cada medida. Una vez completado este proceso se obtiene una auditoría con distintas medidas evaluadas, ya que no tiene porque evaluarse todas de golpe.

La gran problemática surge al tratar de recuperar las auditorías existentes y mostrarlas mediante botones o distintos campos para su selección a la hora de cargar. Está creación dinámica de los componentes que permitieran realizar modificaciones sobre las auditorías impidió, por falta de tiempo, recuperar esos valores para poder modificar o continuar con la evaluación de la infraestructura.

CAPÍTULO 7
Pruebas

Completado el desarrollo comentado, se han realizado distintas pruebas para comprobar su funcionalidad. Cabe destacar las siguientes comprobaciones:

- Iniciar la aplicación.
- Crear una nueva auditoría.
  - Introducir título a la nueva auditoría.
  - Visualizar las medidas existentes de forma correcta.
  - Evaluar las medidas y guardar el resultado.
  - Navegar entre las distintas normas a evaluar.
- Cargar una auditoría ya existente.
  - Visualizar las auditorías existentes.
  - Visualizar las medidas existentes de forma correcta con sus anteriores cambios.
  - Actualizar las medidas y guardar el resultado.
  - Navegar entre las distintas normas evaluadas o por evaluar.

Como se ha comentado en el desarrollo, la parte de cargar los datos existentes de las auditorías no se ha completados, por tanto sus pruebas no han sido satisfactorias. Respecto al resto, la creación de una nueva evaluación así como sus medidas evaluadas se han almacenado en la base de datos de forma correcta y se visualizan sin ningún problema.

CAPÍTULO 8
Conclusiones

Durante la elaboración de este proyecto se ha buscado elaborar una guía con las medidas de seguridad que debe cumplir cualquier infraestructura crítica para cumplir con el Esquema Nacional de Seguridad, lo cual ha quedado plasmado en el apartado 3 de este trabajo. Para ello se ha revisado la normativa del ENS, muy extensa y con multitud de guías, hasta encontrar donde se podía aplicar esas normas para la protección de los sistemas informáticos. Con el estudio de las infraestructuras críticas y su plan de protección se enmarcó en que ámbitos es necesaria la aplicación del Esquema Nacional de Seguridad en todos ellos, permitiendo elaborar una guía común para todas las infraestructuras críticas que estuviera enfocada en el sector administración, cumpliendo así con el objetivo principal del trabajo.

Con el objetivo principal alcanzado, se proponía la elaboración de una aplicación que permitiera utilizar esta guía para facilitar el trabajo de evaluación del los sistemas tanto a los auditores como a los propios responsables de su seguridad. Esta aplicación se ha desarrollado con algunos fallos debidos a la falta de tiempo, ya que la investigación y recopilación de información ha sido extensa, como consecuencia de la multitud de normativas influyentes y la gran cantidad de guías que se encuentran para velar por la correcta aplicación de la normativa. Como consecuencia, fallan algunas de sus funcionalidades y se podrían realizar muchas mejoras, así como añadir más funciones para explotar al máximo el uso de esta guía.

Personalmente el trabajo me ha permitido ser más consciente, si cabe, de la importancia de la seguridad en los sistemas informáticos, debido al hecho de que gran parte del funcionamiento de la sociedad se sustenta en ellos. Esto es aplicable a mi trabajo, ya que me permite aprender buenas prácticas en materia de seguridad, no solo como ingeniero informático, sino también como usuario, que es un eslabón a tener en cuenta a la hora de establecer la seguridad de una infraestructura. Me ha permitido además mejorar en términos de programación y uso de distintas aplicaciones para el desarrollo de aplicaciones, pese a no finalizar el desarrollo esperado.

8.1 Relación del trabajo desarrollado con los estudios cursados

En elaboración del trabajo ha sido necesario combinar los conocimientos adquiridos en diversas asignaturas, sobre todo en relación al desarrollo de la aplicación. Estas asignaturas son tanto troncales, básicas para la formación de cualquier ingeniero informático, como optativas de la rama escogida, en este caso "Tecnologías de la información".

- Bases de datos y sistemas de información
- Ingeniería del software
- Interfaces persona computador
- Seguridad en redes y sistemas informáticos
- Desarrollo centrado en el usuario
- Tecnología de bases de datos

Los conocimientos que se han adquirido en estas asignaturas han permitido, tanto evaluar la importancia de la seguridad y algunas buenas prácticas para su aplicación, como el completo desarrollo de una aplicación pensada para el uso de unos usuarios específicos, integrando en el proceso algunas tecnologías vistas en distintas asignaturas (ampliando en algunos casos esos conocimientos aprendidos para alcanzar el objetivo), como es el uso de base de datos, el uso de las interfaces...

CAPÍTULO 9
Trabajos futuros

A la vista de que el desarrollo de la aplicación ha quedado incompleto o con pocas funcionalidades, el principal camino a seguir sería tanto completarla como mejorarla, ya que se puede sacar provecho de la guía elaborada para realizar auditorías.

Dejando de lado el hecho de conseguir cargar las auditorías ya existentes, la principal mejora sería el desarrollo de una funcionalidad que permitiera evaluar las medidas que se han evaluado, proporcionando en una vista previa las medidas evaluadas tanto favorablemente como desfavorablemente. Esta mejora podría conducir a una función que permitiera generar un informe de la auditoría, mostrando si la infraestructura cumple con la normativa de Esquema Nacional de Seguridad o no.

Como extra, se podría mejorar el diseño de la interfaz, ya que el existente es bastante simple debido al hecho de que se ha primado la funcionalidad sobre la estética, así como revisar y perfeccionar la adaptabilidad a dispositivos móviles como tablets, permitiendo así que el usuario pueda realizar la evaluación de forma fácil mientras recorre los distintos equipos a revisar.

Bibliografía

[1] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Consultado en https://www.boe.es/eli/es/l/2007/06/22/11/con.

[2] 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. Consultado en https://www.boe.es/eli/es/rd/2010/01/08/3/con.

[3] Esquema Nacional de Seguridad - ENS. Consultado en https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.XW7LvigzbIX.

[4] De la Ley 30/1992 a la Ley 39/2015: el procedimiento administrativo del siglo XXI. Consultado en https://www.abogacia.es/2016/10/27/.

[5] Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Consultado en https://www.boe.es/eli/es/l/2015/10/01/40/con.

[6] Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Consultado en https://www.boe.es/eli/es/rd/2015/10/23/951.

[7] Esquema Nacional de Seguridad - Preguntas Frecuentes. Consultado en https://www.ccn-cert.cni.es/publico/dmpublidocuments/ENS-FAQ.pdf.

[8] CCN-STIC-806 Plan de Adecuación al ENS. Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/511-ccn-stic-806-plan-de-adecuacion-al-ens/file.html.

[9] CCN-STIC-802 Auditoría del ENS. Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html.

[10] CCN-STIC-804 ENS. Guía de implantación. Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html.

[11] CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS. Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad.

[12] Guía de Implantación del Esquema Nacional de Seguridad de AMETIC. Consultado en http://www.esquemanacionaldeseguridad.es/web/content/Guia_de_Implantacion_del_Esquema_Nacional_de_Seguridad_de_AMETIC.pdf.

[13] Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. Consultado en http://hdl.handle.net/10251/56042.

[14] El perito ante el ENS. Consultado en http://hdl.handle.net/10251/106729.

[15] Esquema Nacional de Seguridad: protección de una infraestructura crítica hospitalaria Consultado en http://hdl.handle.net/10251/86739.

[16] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Consultado en https://www.boe.es/eli/es/l/2011/04/28/8/con.

[17] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Consultado en https://www.boe.es/eli/es/rd/2011/05/20/704/con.

[18] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Consultado en https://www.boe.es/eli/es/rdl/2018/09/07/12/con.

[19] CNPIC - Preguntas Frecuentes. Consultado en http://www.cnpic.es/Ciberseguridad/2_Preguntas_frecuentes/index.html.

[20] SQL Tutorial. Consultado en https://www.w3schools.com/sql/.