UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica

Universitat Politècnica de València

Guía para la Adecuación de Organizaciones al Esquema Nacional de Seguridad

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Alba Serrat Troncho

Tutor: Juan Vicente Oltra Gutiérrez

Curso 2020-2021

Resum

Aquest treball té com a objectiu el desenvolupament d'una guia que servisca com a suport a les organitzacions, tant públiques com privades, per al correcte compliment del Reial decret 3/2010.

Es centra en el procés d'adequació a l'Esquema Nacional de Seguretat, seguint la metodologia PDCA i creant eines que permeten: la identificació d'actius essencials per part de l'entitat, la categorització dels sistemes d'informació sobre la base de l'Annex II del RD 3/2010, l'anàlisi de riscos dels sistemes, el pla de millora de la seguretat, la declaració d'aplicabilitat i la resta de documentació necessària per al compliment de la citada norma.

La guia està anivellada en funció dels coneixements tècnics del lector, a fi de facilitar l'aplicació de mesures de seguretat de manera eficaç. Per això, s'han establit tres nivells de dificultat que *permitien que siga un document accessible a totes les persones, independentment de la profunditat dels seus coneixements en l'àmbit de l'Enginyeria Informàtica.

A més, se segueixen les bones pràctiques suggerides pel Centre *Criptológico Nacional i s'entrega a les persones usuàries la documentació necessària per a dur a terme una adequació completa amb el menor cost temporal possible.

Paraules clau: Auditoria, compliment normatiu, guia, Esquema Nacional de Seguretat

Resumen

Este trabajo tiene como objetivo el desarrollo de una guía que sirva como apoyo a las organizaciones, tanto públicas como privadas, para el correcto cumplimiento del Real Decreto 3/2010.

Se centra en el proceso de adecuación al Esquema Nacional de Seguridad, siguiendo la metodología PDCA y creando herramientas que permitan: la identificación de activos esenciales por parte de la entidad, la categorización de los sistemas de información en base al Anexo II del RD 3/2010, el análisis de riesgos de los sistemas, el plan de mejora de la seguridad, la declaración de aplicabilidad y el resto de documentación necesaria para el cumplimiento de la citada norma.

La guía está nivelada en función de los conocimientos técnicos del lector, a fin de facilitar la aplicación de medidas de seguridad de forma eficaz. Por ello, se han establecido tres niveles de dificultad que permitien que sea un documento accesible a todas las personas, independientemente de la profundidad de sus conocimientos en el ámbito de la Ingeniería Informática.

Además, se siguen las buenas prácticas sugeridas por el Centro Criptológico Nacional y se entrega a las personas usuarias la documentación necesaria para llevar a cabo una adecuación completa con el menor coste temporal posible.

Palabras clave: Auditoría, cumplimiento normativo, guía, Esquema Nacional de Seguridad

Abstract

This work aims to develop a guide that serves as support to organizations, both public and private, for the correct fulfillment of Royal Decree 3/2010.

It is focused on the process of adaptation to the National Security Framework, following the PDCA methodology and creating tools that allow: the identification of essential assets by the entity, the categorization of information systems based on Annex II to RD 3/2010, the risk analysis of the systems, the security enhancement plan, the declaration of applicability and any other documentation necessary for compliance of that standard.

The guide is graded according to the technical knowledge of the reader in order to facilitate the application of safety measures effectively. Therefore, three levels of difficulty have been established that allow it to be a document accessible to all people, regardless of the depth of their knowledge in the field of Computer Engineering.

In addition, the best practices suggested by the National Cryptological Centre are being followed and the users are given the necessary documentation to carry out a complete adaptation with the least possible temporary cost.

Key words: Audit, Standard Compliance, guide, National Security Scheme

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1

Introducción

La confianza de los ciudadanos en el uso de las nuevas tecnologías a la hora de relacionarse con la Administración Pública, tiene relación directa con el nivel de seguridad que perciben de esta forma de interacción.

A fin de generar esa confianza en el ciudadano, y a raíz de la Ley de Administración Electrónica, se aprueba en el año 2010 el Esquema Nacional de Seguridad, en adelante ENS. Este marco normativo pretende establecer unas mínimas medidas de seguridad comunes a todas las Administraciones Públicas, para asegurar los sistemas de información de la Administración e incentivar el uso de estas nuevas formas de relacionarse con la misma.

La situación derivada de la COVID-19 ha acelerado esa naturalización de la relación con la Administración Pública a través de medios electrónicos, pero este crecimiento en el uso de la administración electrónica no ha venido acompañado del cumplimiento del Esquema Nacional de Seguridad por parte de las diferentes entidades.

Esto hace que los servicios que se prestan a los ciudadanos y los datos almacenados en organismos públicos no estén tan protegidos como deberían, siendo especialmente vulnerables a ciberataques y creando así el caldo de cultivo perfecto para que sean las organizaciones públicas los objetivos preferidos de los ciberdelincuentes.

Es por tanto necesario que a la normalización y extensión del uso de nuevas tecnologías como medio de relación con el sector público, se una el cumplimiento de esta norma. Esto es así porque cumplir con el ENS implica directamente proteger la información y los servicios de las organizaciones, y no solo del sector público sino también de todas las entidades que se relacionan con este y que podrían llegar a ser causa de un incidente de seguridad.

El objetivo que marcaba el Esquema Nacional de Seguridad, era el de garantizar que esa relación electrónica entre ciudadano y poder público fuera lo más segura posible. Pero para ser capaz de cumplir este ambicioso objetivo, antes se ha de ser capaz de alcanzar un hito que hoy en día queda lejos aún: el cumplimiento del Esquema Nacional de Seguridad por parte de todas las entidades implicadas.

Por esta razón, este trabajo se centra en facilitar el cumplimiento de este último objetivo. Se analizarán los problemas más frecuentes que impiden a las organizaciones cumplir con esta ley y se creará una guía que les permita superar esas dificultades y conseguir

una adecuación al Esquema Nacional de Seguridad aún cuando el personal carezca de conocimientos técnicos para hacerlo por su cuenta.

1.1 Motivación

En el ámbito de la Ingeniería Informática, el cumplimiento normativo, la auditoría y la consultoría parecen las grandes olvidadas. Al preguntar por las tareas que realiza una persona graduada en Ingeniería Informática a muchas personas les cuesta encontrar salidas distintas al desarrollo web o de aplicaciones o al campo de la Inteligencia Artificial. Muchas veces se deja de lado que los conocimientos que nos otorga el grado sobre los Sistemas de Información son muy útiles en el mundo laboral, llegando a ser en ocasiones fundamentales para las organizaciones en las que desempeñamos nuestras funciones.

La consultoría de Sistemas de Información es un campo en el cual existe un alto grado de demanda de profesionales de perfil técnico, siendo en ocasiones casi imposible cubrir la demanda de graduados y graduadas en Ingeniería Informática en este área e impensable conseguir la paridad en la plantilla.

Para poner en valor el trabajo de los y las profesionales especialistas en consultoría, se ha optado por llevar a cabo un trabajo en el que se muestre el proceso por el que se pasa para adecuar sistemas a determinados marcos normativos. Se han empleado técnicas de auditoría recomendadas por las autoridades en la materia, se han desarrollado las herramientas que utilizaría un profesional de la materia en su día a día, se han elaborado los documentos que se entregarían a los clientes y se han dejado a disposición de aquel que los pueda necesitar a coste cero.

Además, se escogió el Esquema Nacional de Seguridad por generar desigualdades entre los ciudadanos cuyas administraciones cumplían con la norma y aquellos cuyas entidades no cumplían. Se favorecía la existencia de ciudadanos de primera y segunda clase tecnológica, ya que unos podían disfrutar de sus derechos con la tranquilidad de estar protegidos y los otros no lo hacían.

La decisión fue la de poner al servicio de la sociedad los conocimientos adquiridos a lo largo del grado para que, en la medida de lo posible, estas administraciones que tienen menos recursos y a las que les cuesta mayor esfuerzo conseguir dar esos servicios de forma segura lo tuvieran más fácil. De esta manera, se optó por el Esquema Nacional de Seguridad, que parecía la norma técnica que más dificultades suponía a las organizaciones que habrían de cumplirla, ya que muchas de ellas no disponen ni siquiera un técnico informático en plantilla, y muchas de las medidas exigidas por la ley no se entienden si no se tiene cierta formación en la materia.

Por todas estas organizaciones con dificultades, la adecuación al ENS fue la opción más viable como tema de este trabajo. Pensando en ser de utilidad al máximo número de organizaciones posibles en la misma guía, se abrió no solo a las entidades locales pequeñas sin conocimientos técnicos, sino que se contempla también a los prestadores de servicios (que también han de cumplir esta ley) y a las administraciones con personal técnico que tienen el tiempo y el personal justo y no pueden dedicar el tiempo necesario al estudio detallado de las medidas a cumplir en el ENS.

1.2 Objetivos

Este trabajo tiene como objetivo principal el desarrollo de una guía que permita a cualquier organización cumplir con las 75 medidas del Esquema Nacional de Seguridad. Como objetivos más específicos tendríamos, por ejemplo:

- Obtener una guía comprensible por cualquier lector, independientemente de los conocimientos técnicos en informática de quien la lee.
- Simplificar al máximo el proceso de adecuación al ENS.
- Seguir las guías de buenas prácticas de la autoridad de control.

1.3 Impacto esperado

Se espera que este trabajo resulte en una mayor facilidad para las organizaciones para cumplir con el Esquema Nacional de Seguridad.

Esa facilidad se verá reflejada principalmente en el tiempo que se invertirá en conseguir realizar las fases de «Planificar» y «Hacer», que actualmente son las más costosas este aspecto para las organizaciones. Además, también será más accesible para personas sin formación específica en Ingeniería Informática, con lo que será viable cumplir con el ENS incluso si no se dispone de personal especializado en la materia.

Esto resultará también en un decremento directo del coste en seguridad de las entidades, independientemente de si hubieran optado por una consultoría profesional o no. El ahorro vendría motivado, en el caso de las organizaciones que hubieran buscado ayuda profesional, por el coste directo de los servicios de consultoría, que suele ser de varios miles de euros dependiendo del tamaño de la organización.
En cuanto a las entidades que hubieran optado por no contratar un servicio de consultoría en esta materia, el ahorro se vería tanto en las que quisieran cumplir con su propio personal (ya que se debería de tener en cuenta el coste de las horas laborables que se invertirían en el proceso de adecuación), como en las que decidieran no intentar cumplir con el ENS (ya que a medio o largo plazo lo más probable es que se materializara un incidente de seguridad que conllevara pérdidas económicas muy superiores a los costes de la adecuación).

1.4 Metodología

En cuanto a la metodología de trabajo utilizada para el desarrollo de este trabajo, se ha optado por PRINCE2. Esta elección viene motivada por mi conocimiento específico sobre ella y porque históricamente tiene una estrecha relación con las tecnologías. Y digo esto porque PRINCE2 nació como PROMPTII y fue desarrollado específicamente para afrontar los problemas que surgían en los proyectos informáticos en la época de 1975. Esta metodología fue adoptada por el Centro de Informática y la Agencia de Telecomunicaciones del Gobierno Reino Unido y tras ello, se la bautizó como PRINCE (PRojects IN

Controlled Enviroments). A día de hoy, y tras su última actualización en 2017, PRINCE2 2017 se ha erigido como lo más cercano al estándar ISO-21500 de gestión de proyectos.

En esto nos basaremos para gestionar todo el trabajo, tal y como se detallará más adelante en el plan de trabajo.

1.5 Estructura

El trabajo se estructura en cinco bloques. En el primer bloque se explicará la situación actual del ENS de forma detallada de forma que se tengan todos los datos necesarios para poder realizar un análisis en profundidad del momento actual en materia de cumplimiento de este marco. También se identificarán fallos e insuficiencias en las soluciones ya existentes y se indagará en las razones que llevan a crear esta guía, se explicará de forma detallada y motivada el proyecto que se lleva a cabo y la forma de implementarlo. En el segundo bloque, nos centraremos en identificar los aspectos clave que deben abordarse para mejorar lo ya existente.Así mismo, se determinarán los principales aspectos legales a tener en cuenta durante la ejecución del proyecto, se plantearán varias soluciones posibles a los problemas identificados y se presentará la opción escogida como óptima y se desarrollarán las particularidades de la misma. En este mismo bloque también se determinarán las tareas que conlleva la solución escogida y se planificarán en el tiempo y se hará una estimación económica del coste del trabajo. En el tercer bloque se explicará cómo se estructura la solución de forma clara y se ahondará en el planteamiento de la solución, entrando en el detalle de la misma. En el siguiente bloque se describirá cómo se ha pasado de la propuesta a la solución final, los problemas y dificultades encontradas y se presentarán las pruebas realizadas para verificar que la solución funciona correctamente. En el último bloque, se extraerán las reflexiones finales de la ejecución del proyecto y el aprendizaje obtenido a partir del mismo.

1.6 Convenciones

A lo largo del texto se seguirán las siguientes normas de estilo:

- Las palabras extranjeras se remarcarán en cursiva.
- Se entrecomillarán las citas textuales.
- Se utilizará ENS como abreviación de Esquema Nacional de Seguridad.
- Se utilizará CCN como abreviación de Centro Criptológico Nacional.

CAPÍTULO 2

Estado del arte

En 2014, la Comisión Europea enunciaba, en su Estrategia para el Mercado Único Digital de Europa [2] que «Las tecnologías de la información y la comunicación (TIC) ya no son un sector específico sino el fundamento de todos los sistemas económicos innovadores modernos.». Actualmente, tras la pandemia de la COVID-19 no cabe duda de que las TIC son no solo el futuro sino una parte fundamental del presente de nuestra sociedad. Pero esta digitalización no siempre se ha llevado a cabo de forma en que se proteja la información que se trata y los servicios que se prestan, pese a que de ello depende ahora más que nunca la economía mundial.

Centrando nuestra atención en España, según el *Digital Economy and Society Index 2020* [3] nuestro país es el segundo de la Unión Europea en el indicador «*e-Government*», que mide la demanda y oferta de administración electrónica, y ocupa el puesto 11 de 28 en el índice compuesto por los cinco indicadores de dicho índice. Asimismo, el *E-Government Survey 2020* [4] de las Naciones Unidas nos sitúa en un índice de desarrollo de gobierno digital del 88,82 %, siendo considerado un índice muy alto, que nos sitúa en el decimoséptimo puesto mundial en este índice.

Con este nivel de digitalización de la actividad del sector público de nuestro país, es si cabe más necesario que estos servicios sean seguros, tanto como sea posible. Ante la dificultad de la tarea, en 2010 se publicó el Esquema Nacional de Seguridad, de obligado cumplimiento, y que centrará buena parte del contenido de este Trabajo Fin de Grado.

Pese a que el 30 de enero del año 2021 el Esquema Nacional de Seguridad cumplió once años desde su entrada en vigor, según el Informe Nacional del Estado de la Seguridad más reciente, el del año 2019 [5], aporta datos poco edificantes sobre el nivel de cumplimiento de este marco normativo. En ese informe, el índice de madurez (que es la unidad con la que se mide la implantación de la seguridad) se cifra en un 47,04 % en sistemas de categoría BÁSICA, un 54,75 % de sistemas de categoría MEDIA y el 57,93 % de sistemas de categoría ALTA. Ese índice debería ser del 100 % en todas las categorías desde el 30 de enero de 2012 según establece la Disposición transitoria «Adecuación de sistemas»[1]. Esto supone que tras casi 10 años de esta obligación los sistemas siguen sin cumplir las medidas de seguridad que se les exigían. Y las cifras si nos referimos a las entidades certificadas en el ENS son asimismo desalentadoras.

Dada la situación, cabe reflexionar sobre el porqué de que un porcentaje tan elevado de sistemas continúen sin adecuarse a este marco once años y medio después de su entrada en vigor.

2.1 Crítica al estado del arte

En primer lugar, la implantación del ENS requiere de un análisis de la organización y de sus servicios TIC. Para esta tarea es necesario contar con personal cualificado, algo especialmente complicado en un entorno como el de las Administraciones Públicas, dadas las restricciones en materia de personal que llevan sufriendo desde hace años, y la enorme variabilidad de tamaño y estructura de las mismas. Esto ha hecho que sea habitual recurrir a servicios de profesionales externos para estas tareas, lo cual ha proporcionado sin embargo otras ventajas colaterales, como, por ejemplo, evitar suspicacias y malentendidos entre diferentes grupos de interés dentro de la misma Administración a la hora de evaluar los riesgos o las medidas de protección de esa organización de acuerdo al ENS.

En segundo lugar, los cambios que el ENS pretende introducir han de «calar» en la organización, lo que genera una problemática organizacional típica de gestión del cambio. La principal razón de la resistencia al cambio fue perfectamente definida por Kotter[6] : «Baja tolerancia al cambio». Esto significa que las personas que se resisten tienen ansiedad o dificultad para cambiar.

Justo en las Administraciones Públicas, por la naturaleza del personal a su servicio y sus derechos laborales, donde hay tantas personas en puestos inamovibles y a los que es complejo asignarles nuevas funciones relacionadas con la ciberseguridad para la que tampoco están formadas, esta gestión del cambio es, si cabe, más compleja. A todo esto, habría que añadir la percepción que tiene la inmensa mayoría de responsables políticos y directivos públicos profesionales de que el cumplimiento del Esquema Nacional de Seguridad es responsabilidad de los informáticos, cuando la realidad es que debe ser un proceso integral en el que participe toda la organización y esté liderado por la dirección de la misma. Esto mismo se ratifica en el Prontuario de ciberseguridad para entidades locales [7] que implica a todos los puestos electos de las Administraciones en el cumplimiento del ENS. Dice, por ejemplo que «Los responsables locales deben encontrar formas nuevas e innovadoras de garantizar la sostenibilidad de tales servicios. » refiriéndose a los servicios electrónicos, o «una ciberseguridad adecuada y proporcionada a los riesgos es esencial para garantizar el funcionamiento eficiente de todas las entidades locales y el mejor servicio al ciudadano». Enlazando así el cumplimiento del ENS con el buen funcionamiento de la entidad, por el cual han de velar sus dirigentes.

Finalmente, desde el punto de vista económico cumplir con el Esquema Nacional de Seguridad requiere de ciertos gastos, tanto para asumir los planes de adecuación como para mantener el proceso de mejora continua de la seguridad que define este reglamento. Por lo general, se suelen contratar servicios de consultoría y auditoría de esta norma, cuyos precios varían en función de las necesidades de cada organización. Podemos ver algunos ejemplos de este tipo de proyectos en la Plataforma de Contratación del Sector Público:

- En el caso de la Sindicatura de Comptes de la Generalitat Valenciana, se resolvió una licitación de consultoría y asesoramiento del ENS por valor de 30.000€ [8].

- En el caso de la Fundación Colección Thyssen Bornemisza, se resolvió una licitación de 18.150€ [9] en concepto de adecuación, mantenimiento y soporte del ENS y del RGPDGDD.
- En el caso del Ayuntamiento de Cáceres, la licitación ascendió a 49.000€ [10].

De esto se extrae que la inversión necesaria para conseguir tener claro cómo adecuarse a este marco normativo, si se quiere contratar especialistas en la materia, no es nimia. Además, hemos de tener en cuenta que de manera habitual el proceso de adecuación va acompañado de la adquisición de todo tipo de equipos, productos y servicios para lograr el nivel adecuado de cumplimiento. Y entre esos elementos hay uno imprescindible y adicional, la adquisición de licencias de uso de *software* específico para la gestión de todos los aspectos relacionados con el Sistema de Gestión de la Seguridad de la Información y la gestión documental de la norma. Producto específico del que actualmente no hay una oferta variada de fabricantes, y está principalmente limitada a las siguientes opciones:

1. Las soluciones propias del Centro Criptológico Nacional. Para la adecuación al ENS, el CCN recomienda utilizar las siguientes:
   a) INÉS. Para la realización del Plan de Adecuación del Sistema.
   b) AMPARO. Para la Implantación de Seguridad y la Conformidad con el ENS.
   c) ANA. En el proceso de Mejora Continua de la Seguridad.
   d) Otras. Como EMMA o ÁNGELES para el Control de Acceso a las Infraestructuras de Red y para Formación en Ciberseguridad.
2. La solución de Telefónica, SANDAS GRC.
3. GConsulting Compliance.

Sabiendo esto, y teniendo en cuenta que de las más de 18000 administraciones públicas españolas, 8131 son municipios[11], además el 95,0 % de ayuntamientos tiene menos de 20.000 habitantes, y el 83,9 % tiene menos de 5.000 hab.[12], lo que implica que esos ayuntamientos no tienen los recursos temporales ni económicos necesarios para hacer frente a una adecuación por sus propios medios. A esto hemos de añadir que los ayuntamientos de menos de 5000 habitantes no suelen tener empleados con conocimientos de Ingeniería Informáticos, con lo que carecen también del personal y la formación necesarios para aplicar muchas guías y muy extensas que a veces desconocen y no saben cómo empezar a abordar, y que a pesar de su alta calidad utilizan lenguaje muy técnico.

Con todo lo expuesto, obtenemos como resultado un Esquema Nacional de Seguridad sin cumplir objetivos once años después de su entrada en vigor, un elevado número de entidades que no tienen recursos humanos, temporales ni monetarios suficientes para afrontar un proceso de adecuación difuso y otras tantas que pese a tenerlos deciden no aplicarlo por no comprender la importancia de la seguridad en sus organizaciones.

2.2 Propuesta

La propuesta a desarrollar en este Trabajo de Fin de Grado es una guía que pueda leer y aplicar cualquier persona, tenga esta o no una base de conocimiento de informática.

Con ella, ahorraremos el tiempo a las entidades recopilando todas las recomendaciones de las diferentes guías ya existentes en una única localización que irá acompañada de las explicaciones pertinentes y que permitirá realizar los primeros pasos para la adecuación de forma autónoma, solo quedando fuera la auditoría que ha de ser necesariamente realizada por una persona externa.

CAPÍTULO 3

Análisis del problema

Este capítulo contiene el análisis de la legalidad vigente, el estudio de posibles soluciones a desarrollar, el detalle de la solución por la que se optará finalmente y de cómo se organizará el desarrollo, así como el coste estimado de esta solución.

3.1 Análisis del marco legal y ético

Todo buen profesional ha de tener en consideración la legalidad vigente y la manera en la que esta puede llegar a influir en el desempeño de sus funciones. En esta sección, se detallará el marco normativo a tener en cuenta a la hora de desarrollar este trabajo. Al se un trabajo genérico para organizaciones tanto privadas como públicas se analizará la normativa aplicable al sector privado por un lado, la aplicable al sector público del otro y la común a ambos sectores en conjunto.

3.1.1. Propiedad intelectual

En cuanto a la Ley de Propiedad Intelectual, hemos de tener en cuenta que todo el contenido que se utilice en la guía estará sujeto a una serie de condiciones.

Durante la realización de este trabajo, se ha hecho uso de distintas imágenes. Éstas provienen de las siguientes fuentes:

- ***Pixabay.*** Se trata de un banco de fotografías, ilustraciones, vectores, vídeos y música sin derechos de autor en el que no se exige reconocimiento.
- ***Pexels.*** Al igual que *Pixabay*, es un banco de imágenes y vídeos. En este caso hay fotografías de uso gratuito, aunque algunas necesitan de reconocimiento al autor.
- ***Unsplash.*** Este banco de imágenes tiene fotografías conceptuales de forma gratuita y sin derechos de autor. Se da la opción de dar crédito al autor pero no se está obligado a ello.
- **Creación propia.** También se han diseñado muchas de las imágenes que se ven en la guía, en concreto una de ellas es la de los indicadores de nivel de lectura.

Se ha hecho un esfuerzo para evitar el uso de fotografías con derechos de autor y de textos sujetos a *copyright* u otras licencias similares.

3.1.2. Marco legal del sector privado

Si tenemos en cuenta que solamente aquellas organizaciones privadas que tengan relación con la Administración han de cumplir con el Esquema Nacional de Seguridad, extraeremos que el marco legal más destacable aplicable a estas organizaciones es el que sigue:

- 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, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- 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.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Código de Derecho de la Ciberseguridad.[13]

Además, habría que revisar la normativa propia de la autonomía en la que prestase los servicios cada entidad.

3.1.3. Marco legal del sector público

En cuanto a las leyes que aplican al conjunto de todas las administraciones públicas, como principales tendíamos:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que señala en su art. 17.3 que los medios o soportes en que

se almacenen documentos , deberán contar con las medidas de seguridad que establece el Esquema Nacional de Seguridad, que garanticen una serie de principios (como integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados); y, establece también, en su art. 27.3 que las Administraciones Públicas deberán cumplir con el Esquema Nacional de Seguridad para garantizar la identidad y contenido de las copias electrónicas o en papel, es decir, el carácter de copias auténticas. Por último, dispone en su Disposición Adicional segunda que, tanto las Comunidades Autónomas, como las Entidades Locales, deberán garantizar su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas mediante el cumplimiento, igualmente, del Esquema Nacional de Seguridad. Y que, además, deroga la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

- 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.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión

- Código de Derecho de la Ciberseguridad.[13]

3.1.4. Marco legal común a ambos sectores

El marco común a ambos sectores es, por tanto:

- 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, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.

- 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.

- Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

- Código de Derecho de la Ciberseguridad.[13]

3.2 Identificación y análisis de soluciones posibles

Tras el análisis profundo del problema, se identifican las siguientes soluciones posibles:

1. Desarrollo de una aplicación totalmente gratuita que acompañe al usuario a lo largo de todo el proceso y que pueda realizar las verificaciones necesarias para emitir un informe que pueda ser de ayuda para los auditores.

    - Pros. Sería una solución que facilitaría mucho el proceso de adecuación y verificación del cumplimiento del ENS.
    - Contras. Sería muy costosa de desarrollar, no solucionaría la problemática de la nula formación en ciberseguridad del personal y podría no utilizarse correctamente con lo que podría llegar a ser contraproducente.

2. Diseño de un MOOC obligatorio para todos los sistemas que no estén adecuados al ENS que explique la necesidad de proteger los sistemas y que tenga como tareas los diferentes pasos para conseguir el cumplimiento del ENS.

    - Pros. Sería una solución muy útil para fomentar el acatamiento del ENS.
    - Contras. Necesitaría personal que estuviera de forma continua revisando las tareas de no pocas entidades, con su correspondiente coste económico.

3. Redacción de una guía a cualquier organización, sea pública o privada, llevar a cabo el proceso de adecuación al Esquema Nacional de Seguridad de forma satisfactoria independientemente del nivel de conocimiento de su personal.

    - Pros. Sería una solución parecida a las anteriores pero con menor coste temporal.
    - Contras. No soluciona el problema del desentendimiento de los altos cargos en materia de seguridad.

3.3 Solución propuesta

La solución propuesta es la realización de una guía que permita a cualquier organización, sea pública o privada, llevar a cabo el proceso de adecuación al Esquema Nacional de Seguridad de forma satisfactoria independientemente del nivel de conocimiento de su personal.

Esto se va a conseguir del siguiente modo:

1. **Redacción de una guía nivelada.** La guía estará escrita teniendo en cuenta tres posibles perfiles de lector:

   - **Lector de nivel experto.** Será aquella persona que desee cumplir con el ENS y tenga los conocimientos técnicos necesarios para hacerlo por sí mismo. La guía no entrará en detalles, sino que solamente describirá los pasos a seguir para adecuarse.
   - **Lector de nivel intermedio.** Será aquella persona que desee adecuar el sistema al Esquema Nacional de Seguridad y esté familiarizada con algunos términos de seguridad pero no tenga los conocimientos técnicos necesarios para llevar a cabo el proceso de adecuación. La guía no entrará en la definición de los términos, pero la acompañará para que pueda realizar correctamente las tareas más técnicas.
   - **Lector de nivel básico.** Será aquella persona que quiera cumplir con lo establecido en el RD 3/2010 pero que desconozca por completo los términos de seguridad y carezca de conocimientos técnicos necesarios para llevar a cabo el proceso de adecuación. La guía entrará en la definición de los términos y la acompañará para que pueda realizar correctamente las tareas más técnicas.

2. **Desarrollo de toda la documentación necesaria.** La guía vendrá acompañada de la mínima documentación exigible para el cumplimiento de la norma. Esta será personalizable para cada entidad.

3. **Desarrollo de una página web.** Se desarrollará una página web en la plataforma Wordpress que permitirá a cualquiera descargar la guía y su documentación o seguirla en línea si se prefiere.

Para conseguir esta solución final, se comenzará por identificar y producir todo el material que será necesario para la adecuación exitosa de las organizaciones. Una vez identificada y producida la documentación, se procederá a la redacción de la guía completa, que posteriormente será trasladada a una web en Wordpress.

Una vez terminado todo el proceso, se buscarán dos organizaciones dispuestas a probar la guía y todo lo relacionado con ella. Una de las organizaciones deberá tener personal con conocimientos técnicos y la otra no.

De su satisfacción dependerá el éxito del trabajo realizado.

3.4 Plan de Trabajo

El plan de trabajo estimado para la elaboración de la guía se basó en las directrices de la metodología de gestión de proyectos PRINCE 2 [14], que recomienda aplicar siete principios. Uno de estos principios es "Gestión por fases".

A fin de dividir el proyecto en fases, se identificaron primero todas las partes del mismo y las tareas que se asociarían a cada una. Se realizó una clasificación como la de la siguiente:

1. Fase 1. Elaboración de la documentación necesaria
    - *a*) Creación del libro de cálculo para la fase de Plan.
    - *b*) Creación de la hoja de registro de activos.
    - *c*) Creación de la hoja de Categorización del Sistema.
    - *d*) Creación de la Declaración de Aplicabilidad automática.
    - *e*) Creación de la hoja de Análisis de Riesgos.
    - *f*) Creación de la hoja de Perfil de Cumplimiento.
    - *g*) Creación de la hoja con las medidas del Anexo II.
    - *h*) Creación de la hoja de Amenazas según MAGERIT v.3.
    - *i*) Creación de la Política de Seguridad de la Información.
    - *j*) Creación del Manual de Seguridad
    - *k*) Creación del Plan de Adecuación
2. Fase 2. Redacción de la Guía para la Adecuación de Organizaciones al Esquema Nacional de Seguridad.
    - *a*) Cómo utilizar esta guía.
    - *b*) Introducción.
    - *c*) Temática y destinatarios de la guía.
    - *d*) Objetivo de la guía.
    - *e*) Metodología de trabajo.
    - *f*) Plan de adecuación.
    - *g*) Identificación del alcance del sistema.
    - *h*) Categorización del sistema.
    - *i*) Obtención de la Declaración de Aplicabilidad Provisional.
    - *j*) Realización del Análisis de Riesgos .
    - *k*) Validación y Perfil de Cumplimiento.
    - *l*) Política de Seguridad.
    - *m*) Implantación de la seguridad.
    - *n*) Hoja de ruta.
    - *ñ*) Marco Normativo y medidas técnicas de seguridad.
    - *o*) Aprobación del SGSI por el COMSEG.
    - *p*) Declaración o Certificación de Conformidad.
    - *q*) Vigilancia y Mejora Continua.

3. Fase 3. Desarrollo de la página web.
    a) Página de Inicio.
    b) Página de Índice.
    c) Introducción.
    d) Temática y destinatarios de la guía.
    e) Objetivo de la guía.
    f) Metodología de trabajo.
    g) Plan de adecuación.
    h) Identificación del alcance del sistema.
    i) Categorización del sistema.
    j) Obtención de la Declaración de Aplicabilidad Provisional.
    k) Realización del Análisis de Riesgos.
    l) Validación y Perfil de Cumplimiento.
    m) Política de Seguridad.
    n) Implantación de la seguridad.
    ñ) Hoja de ruta.
    o) Marco Normativo y medidas técnicas de seguridad.
    p) Aprobación del SGSI por el COMSEG.
    q) Declaración o Certificación de Conformidad.
    r) Vigilancia y Mejora Continua.
    s) Página de Descarga
4. Fase 4. Testeo de la solución.
    a) Búsqueda de una organización con personal profesional.
    b) Prueba en una organización con personal profesional.
    c) Búsqueda de una organización con personal no profesional.
    d) Prueba en una organización con personal no profesional.

Se ha adaptado la extensión del proyecto a las posibilidades, teniendo en cuenta la dedicación de una sola persona durante un total aproximado de 300 horas.

A continuación, se muestra un diagrama de Gantt con la distribución temporal de las fases definidas teniendo en cuenta una dedicación diaria de cuatro horas diarias de lunes a viernes.

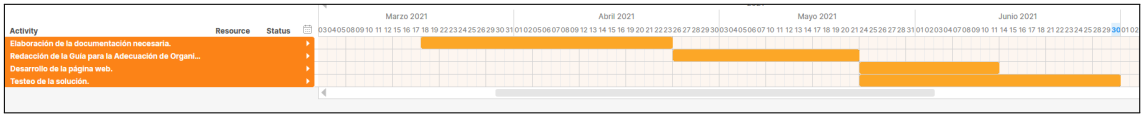


Figura 3.1: Vista general de todas las fases

Como podemos observar, la primera fase del proyecto se llevaría a cabo entre los días 18 de marso y 23 de abril de 2021. Empezaría entonces la segunda fase el 26 de abril, terminando el 21 de mayo y empezando el 24 de este mismo mes las fases tercera y

cuarta. En el caso de la tercera fase, terminaría el 11 de junio, extendiéndose la cuarta hasta el 30 de ese mismo mes.

En la primera fase las tareas se desarrollar se distribuyeron del siguiente modo:

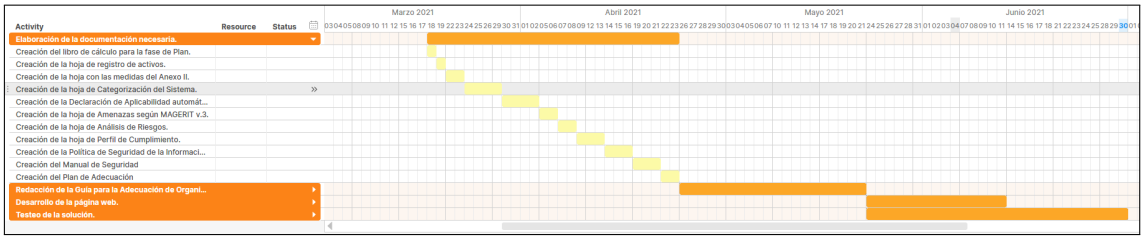


Figura 3.2: Vista de la fase 1

Se ha estimado que las tareas de «Creación de la hoja de Categorización del Sistema» y «Obtención de la Declaración de Aplicabilidad Provisional» serán las que mayor inversión de tiempo requerirán y por ello se les van a dedicar 4 jornadas.

La segunda fase ha sido organizada como sigue:

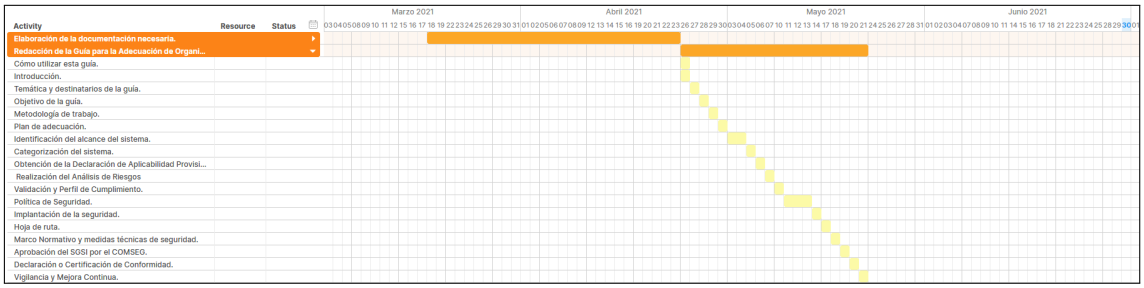


Figura 3.3: Vista de la fase 2

Cabe destacar que estas tareas se estiman como menos costosas porque consistirán en explicar lo ya existente, siendo menos costoso al no requerir de un esfuerzo creativo tan grande como la primera fase.

La tercera fase se planificó de la siguiente manera:

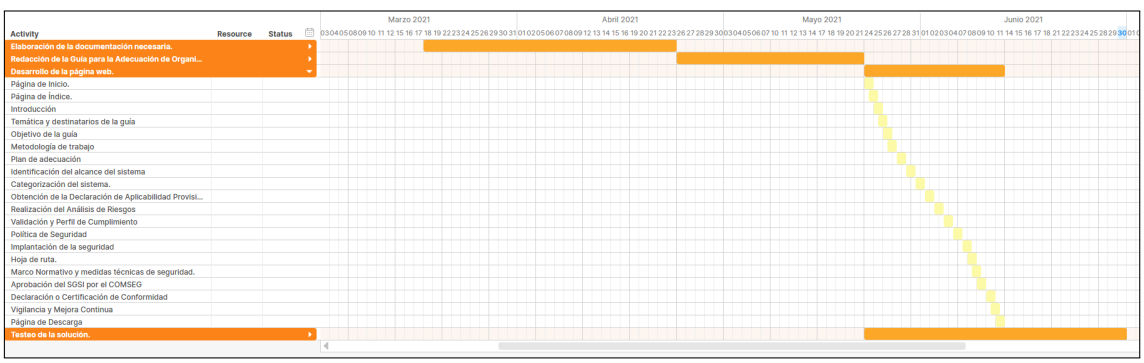


Figura 3.4: Vista de la fase 3

En este caso, las tareas consisten principalmente en trasladar todo lo que se escribió en el documento de la primera fase a una página web. Esa es la razón por la que las tareas duran menos en esta fase.

Por último la cuarta fase se dividió así:

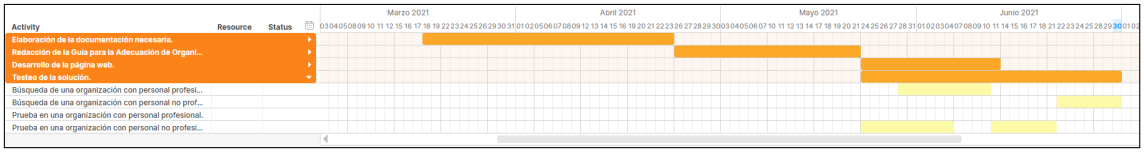


Figura 3.5: Vista de la fase 4

Se buscarán organizaciones dispuestas a probar la solución entre el 24 de mayo y el 10 de junio y se les acompañará en el proceso de adecuación durante siete jornadas para recoger posibles dudas y problemas que puedan surgir.

Tras esto, el proyecto estaría completo y testado y podría concluir.

3.5 Presupuesto

Se ha realizado un presupuesto que estima el valor del proyecto en caso de que hubiera de replicarse en otra ocasión. Este se muestra en la imagen a continuación:

Proyecto	ara la Adecuación de Organizaciones al Esquema Nacional de Seg		
Concepto	**Cantidad**	**Precio**	**Total**
Horas de trabajo	300	5,60 €	1.680,00 €
Licencias MS Office	1	54,51 €	54,51 €
Licencias LibreOffice	1	0 €	0,00 €
Suscripción a Canva Pro	1	85,23 €	85,23 €
		Base imponible	1.819,74 €
		IVA 21%	382,14 €
		Total	**2.201,88 €**

Figura 3.6: Presupuesto

Tal y como se puede observar, se presupuestan trescientas horas de trabaja a un precio por hora de 5,60€ al ser este el salario medio de una persona graduada en Ingeniería Informática en España.
Se ha tenido en cuenta también el coste de adquisición de las licencias de software utilizadas para el desarrollo del presente trabajo. Estas fueron:

- Licencia dde Microsoft Office. El paquete ofimático de Microsoft.

- Licencia de LibreOffice. Paquete ofimático gratuito.
- Suscripción a Canva Pro. Programa de diseño y maquetación.

Esto eleva el montante del presupuesto a 2201,88€ IVA incluido.

CAPÍTULO 4

Diseño de la solución

En este capítulo, se explicará de forma detallada la manera en la que se ha diseñado la solución para que esta sea eficaz y eficiente.

4.1 Diseño detallado

4.1.1. Estudio del Esquema Nacional de Seguridad

En este caso, el primer paso que se siguió para desarrollar esta guía fue la lectura comprensiva del Esquema Nacional de Seguridad.

De esta se extrajeron una serie de conclusiones:

1. La seguridad de un sistema se basa en identificar correctamente los servicios que se prestan y la información que se maneja.
2. El conjunto de servicios e información se denomina activos del sistema.
3. Existen cinco dimensiones de seguridad a tener en cuenta:
    a) Disponibilidad. «Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.»[1].
    b) Autenticidad.«Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.»[1]
    c) Integridad.«Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.»[1].
    d) Confidencialidad.«Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.»[1].
    e) Trazabilidad. «Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.»[1].
4. Cada activo impactará en un nivel sobre cada una de las dimensiones de seguridad.

5. Cada dimensión de seguridad tendrá una valoración que será la máxima de entre todos los activos del sistema. Estas podrán ser valoradas como sigue:

   a) Nivel bajo. Se utilizará cuando se considere que un incidente de seguridad podría causar daños limitados a la organización.

   b) Nivel medio. Se utilizará cuando se considere que un incidente de seguridad podría causar daños graves a la organización.

   c) Nivel alto. Se utilizará cuando se considere que un incidente de seguridad podría causar daños muy graves a la organización.

6. Las valoraciones de las dimensiones de seguridad serán las que determinarán la categoría del sistema. Existen tres categorías de sistema:

   a) Categoría básica. Un sistema pertenecerá a esta categoría cuando una de sus dimensiones alcance nivel bajo y ninguna otra lo supere.

   b) Categoría media. Un sistema pertenecerá a esta categoría cuando una de sus dimensiones alcance nivel medio y ninguna otra lo supere.

   c) Categoría alta. Un sistema pertenecerá a esta categoría cuando una de sus dimensiones alcance nivel alto.

7. En función de la categoría de un sistema y de la categoría de cada una de las dimensiones de seguridad, le serán de aplicación unas u otras medidas de seguridad.

4.1.2. Estudio de las directrices de la entidad de control

Tras el estudio detallado de la norma, se pasó a investigar las directrices de la entidad de control para el proceso de adecuación. A este efecto, el Centro Criptológico Nacional ha desarrollado una web específica para el ENS[15]. En ella, se encuentra una sección dedicada expresamente a la conformidad especialmente interesante para el trabajo que se va a desarrollar.

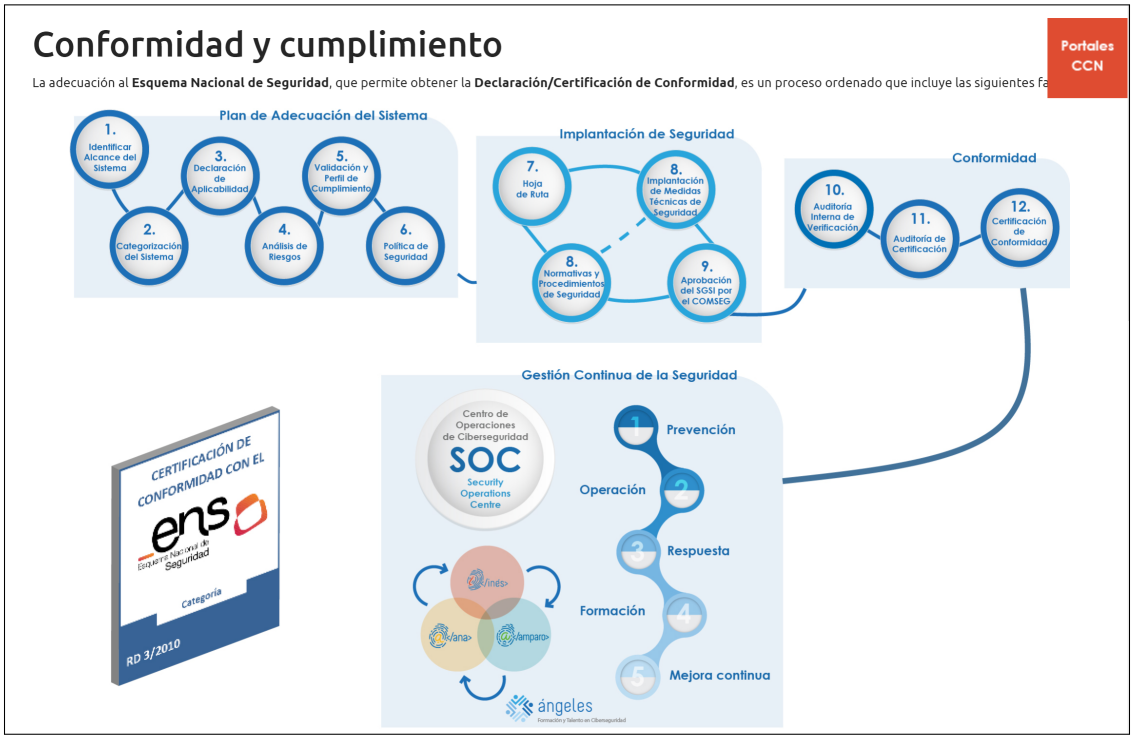


Figura 4.1: Detalle de los pasos que da el CCN

Como se observa en la figura 4.1, el Centro Criptológico Nacional divide ese proceso de obtención de la Declaración/Certificación de Conformidad con el Esquema Nacional de seguridad en doce tareas que forman parte de un ciclo de mejora continua. Estas serán exactamente las tareas que se realizarán, y se seguirá el orden establecido por esta autoridad a fin de garantizar el éxito a la hora de alcanzar el cumplimiento íntegro de la norma.

Además, el CCN pone a disposición pública una serie de guías que facilitan el proceso de adecuación. En concreto, en este trabajo se van a aplicar las siguientes guías:

1. CCN-STIC-800 Glosario de términos y abreviaturas del ENS [16].
2. CCN-STIC-801 Responsabilidades y Funciones en el ENS [17].
3. CCN-STIC-802 Auditoría del ENS [18].
4. CCN-STIC-803 Valoración de Sistemas en el ENS [19].
5. CCN-STIC-804 ENS. Guía de implantación [20].
6. CCN-STIC-805 Política de Seguridad de la Información [21].
7. CCN-STIC-806 Plan de Adecuación al ENS [22].
8. CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS [23].
9. CCN-STIC-809 Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento[24].
10. CCN-STIC-821 Normas de Seguridad en el ENS[25].

11. CCN-STIC-822 Procedimientos de Seguridad [26].
12. CCN-STIC-824 Información del Estado de Seguridad[27].
13. CCN-STIC-882 Guía de Análisis de Riesgos para Entidades Locales[28].
14. CCN-STIC-883 Guía de implantación del ENS para Entidades Locales[29].
15. CCN-CERT BP/14 Declaración de Aplicabilidad en el ENS.

Asimismo, para el análisis de riesgos se empleará la metodología de análisis y gestión de riesgos MAGERIT v.3, desarrollada por el Consejo Superior de la Administración Electrónica.

4.1.3. Diseño de la documentación adjunta

Una vez aclaradas las posibles dudas sobre la documentación necesaria, se llevó a cabo una recopilación de todo aquello que se exigía como mínimo para el cumplimiento del ENS.

Esto resultó en la siguiente relación de documentos:

- Política de seguridad.
- Normativa General de Utilización de los Recursos y Sistemas de Información.
- Normas de acceso a intenet.
- Normas de uso del correo electrónico.
- Normas para trabajar fuera de las instalaciones.
- Normas de creación y uso de contraseñas.
- Acuerdo de confidencialidad para terceros.
- Modelo de contenido de buenas prácticas para terceros.
- Normativa de uso de redes sociales.
- Procedimiento de gestión de usuarios: altas, bajas, identificación, autenticación y control de acceso lógico.
- Procedimiento de clasificación y tratamiento de la información clasificada.
- Procedimiento de generación de copias de respaldo y recuperación de la información.
- Plan de adecuación al ENS.
- Informe del estado de la Seguridad.
- Declaración de Aplicabilidad.
- Plan de mejora de la Seguridad.

- Hoja de ruta.

Para simplificar la tarea al usuario, se identificaron los puntos en común de los diferentes documentos, siendo finalmente estos los documentos resultantes:

1. Política de Seguridad
2. Manual de Seguridad. Que agrupará todas las normativas y todos los procedimientos arriba mencionados.
3. Plan de adecuación al ENS. Que contendrá también la Declaración de Aplicabilidad y el Plan de Mejora de la Seguridad.
4. Hoja de Ruta.

Toda esta documentación se entregaría en un sistema de carpetas con la siguiente estructura:

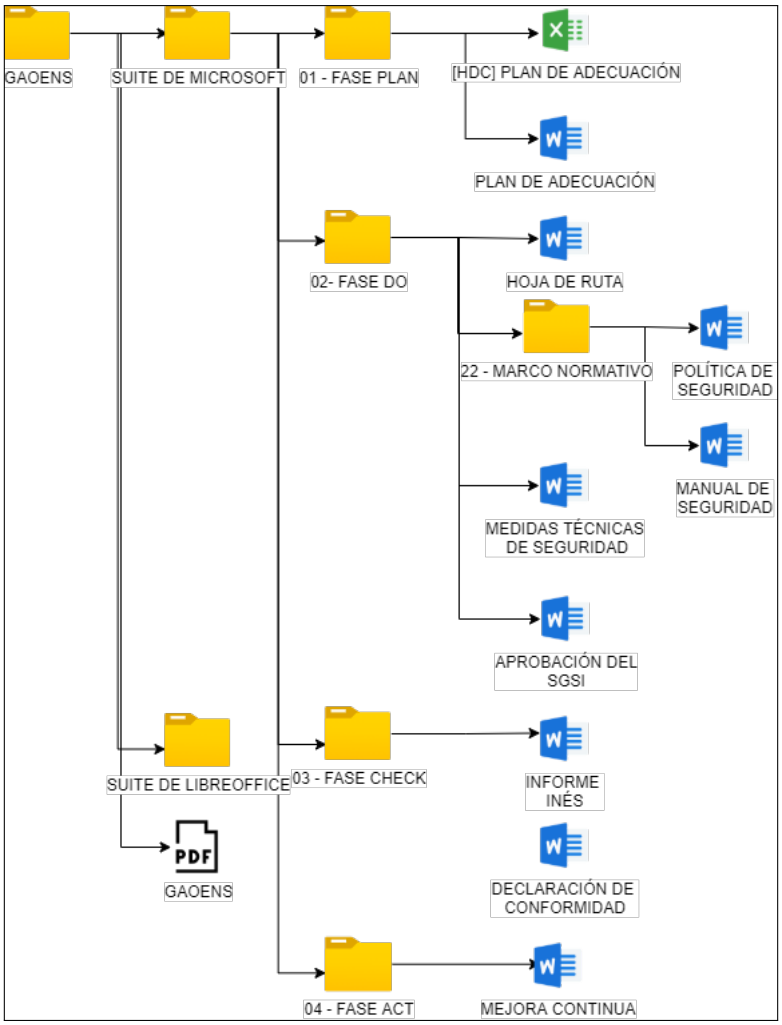


Figura 4.2: Sistema de carpetas

Cabe destacar que, para mayor legibilidad, no se ha desplegado la carpeta «SUITE DE LIBREOFFICE», pero su contenido es el mismo que el de la carpeta «SUITE DE MICROSOFT» pero adaptada al formato que exigen sus herramientas.

Diseño de las hojas de cálculo

A la hora de diseñar el libro de cálculo en el que se basaría el primer paso en este proceso de adecuación se tuvieron en cuenta una serie de aspectos. El conjunto de las hojas de este libro deberían contemplar una serie de elementos característicos del ENS, estos se plasmaron en un diseño UML para mayor claridad. El resultado fue el siguiente:

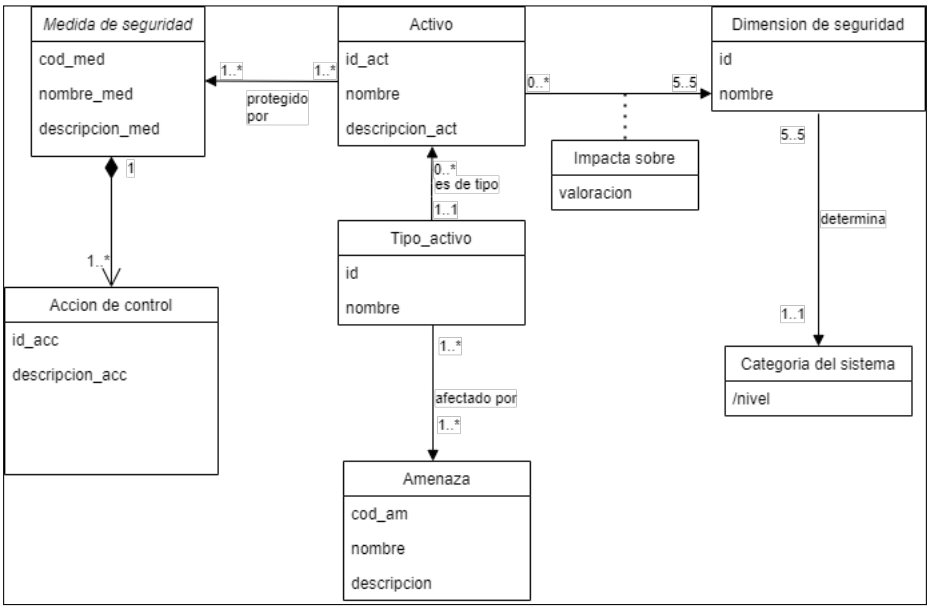


Figura 4.3: Diseño UML del funcionamiento del libro de cálculo

Era por tanto necesario tener claro que la pieza central de nuestro libro debían ser los activos identificados. Además, de cada activo sería necesario un identificador, un nombre y una descripción. Cada activo pertenecería a un tipo de activo de los especificados por MAGERIT v.3, que a su vez estaría identificado de algún modo y tendría asignado un nombre. Además, cada tipo de activo iría asociado a unas determinadas amenazas, a tener en cuenta a la hora de realizar el análisis de riesgos.

Por otro lado, cada activo impactaría sobre cinco dimensiones de seguridad. A este impacto se le valorará de forma que para cada activo y para cada una de las cinco dimensiones se obtenga una puntuación de «BAJO,MEDIO o ALTO» en función de la repercusión negativa que pudiera tener que se materializase un incidente de seguridad sobre ese activo en concreto. Las cinco dimensiones, debidamente identificadas y nombradas, determinarían la categoría del sistema. Este nivel sería calculado en función del máximo de los niveles en que el conjunto de los activos afectase a todas las dimensiones.

Desde otra perspectiva de organización, se optó por estructurar el libro de cálculo en diferentes pestañas que siguieran el orden de los pasos a seguir para facilitar al usuario la interacción con el libro.

Diseño de los documentos de texto

En cuanto a los documentos de texto que se adjuntarían a la guía, se decidió que estos tuvieran una estética que hiciese reconocible el documento como perteneciente a la guía.

Esta estética también debería ser soportada por los dos procesadores de texto que se utilizaran en el trabajo.

Esto llevó a una búsqueda de las fuentes compatibles con ambos sistemas, que acabó por determinar que la fuente a utilizar sería «Arial».

Asimismo, en lo que respecta a la estructura de los documentos, se va a seguir la recomendada en las guías del Centro Criptológico Nacional. Esta consta de:

- Portada
- Índice
- Introducción
- Alcance
- Misión
- Marco Normativo
- Contenido

Por otro lado, los documentos deberían ser personalizables para cada entidad, puesto que habrá aspectos diferenciadores que harán que el contenido se ajuste mejor a la realidad de cada una, ya que este (mostrar la situación particular de la seguridad de cada organización) es el objetivo principal de los documentos proporcionados.

4.1.4. Diseño de la guía

Para el diseño de la guía se empezó por determinar qué estructura tendría. A fin de hacer más sencilla la comprensión de qué se estaba realizando en cada momento, se optó por diferenciar en la guía las cuatro fases del ciclo PDCA del que hace uso el CCN. Además, en cada fase se incluirían los pasos que se habían definido también por la autoridad de control.

Cada paso estará explicado en tres niveles de dificultad, entrando en el detalle de cómo llevar a cabo cada pequeña tarea o dando pinceladas que permitan al lector que ya tiene los conocimientos continuar con el proceso. Esta explicación iría acompañada de una serie de iconos que irían indicando a cada nivel de usuario qué partes debe leer para comprender completamente lo que ha de hacer en cada momento.

Además, se diseñará una guía lo más visual posible, para evitar al cerebro la percepción de que algunas tareas son demasiado farragosas o complejas, y motivar a las personas a continuar leyendo.

Por último, y para hacer más sencilla la interacción a quien utilice la guía, se utilizarán códigos de color para cada fase del ciclo. Con esto se pretende que se pueda saber fácilmente en qué momento nos encontramos y de esta manera evitar que alguien se pierda en algún punto.

4.1.5. Diseño de la web

La web se diseña para facilitar el acceso de los usuarios finales al contenido de esta. Por eso mismo se decidió que la página de inicio explicara qué era la guía y después invitase a los usuarios primero a descargarla y luego a seguirla *online* a través de esa misma web.

Una vez tomada esa decisión, se planteó la forma en la que se navegaría por la guía en esta página web. Se pensó en hacer un apartado para cada fase del ciclo Plan, Do, Check and Act, pero se decidió que esto podía resultar muy incómodo.

A continuación, se pensó en hacer una sección que sirviese de índice y que llevase a cada una de las tareas y que una vez dentro de cada tarea, se pudiera navegar a la anterior y a la siguiente a través de botones. Esta última idea fue la preferida, puesto que haría mucho más ágil la lectura de y la interacción con la guía.

Después de decidir la estructura, era hora de decidir la forma de mostrar el contenido. Se optó por seguir una imagen limpia y poco recargada, se utilizaría una combinación de colores con dos colores más sobrios y oscuros como son el azul marino y el negro, que dan sensación de profesionalidad y de seriedad, con otros dos colores más vivos como el magenta y el amarillo, que dan un aspecto más animado y vitalizante. De este modo se intenta transmitir que el trabajo realizado es profesional. pero ligero de leer y aplicar.

4.2 Tecnología utilizada

4.2.1. Tecnología utilizada para la documentación adjunta

Las opciones posibles para desarrollar la documentación que se adjuntaría a la guía eran:

1. OpenOffice
2. LibreOffice
3. Microsoft Office
4. Pages

Teniendo en cuenta que Windows es el sistema operativo mayoritario en los ordenadores españoles, y que el software desarrolado por Microsoft es también compatible con Mac (segundo en el mercado), tenía sentido utilizar la suite de Microsoft Office para realizar la documentación.

No obstante, había que tener en cuenta que la mayor parte de los sistemas que debían cumplir con el ENS pertenecían al sector público, donde se suele trabajar con el sistema operativo Linux. Es por ello que había que elegir una opción compatible sin licencia de pago, con lo cual se tenía que escoger entre OpenOffice y LibreOffice. Para hacerlo, se hizo una lista de los pros y contras de cada opción.

OpenOffice	**LibreOffice**
Pros	*Pros*
Es multiplataforma Consume pocos recursos del ordenador. Permite guardar los documentos en diferentes formatos poco restrictivos.	Es multiplataforma. Consume pocos recursos del ordenador. Permite guardar los documentos en diferentes formatos poco restrictivos. Actualizaciones frecuentes. Interfaz parecida a MS Office
Contras	*Contras*
Interfaz poco intuitiva. Sin soporte técnico	Sin soporte técnico

Tabla 4.1: Comparativa entre OpenOffice y LibreOffice

A raíz de esta comparativa, se escogió LibreOffice como la segunda tecnología en la que desarrollar la documentación.

4.2.2. Tecnología utilizada para la guía

Para la guía se buscaba sobretodo un enfoque muy visual. Se buscaba evitar grandes textos que se hiciesen demasiado pesados y un diseño serio pero desenfadado. Fue por eso que se optó por no utilizar un procesador de textos, sino una herramienta de maquetación.

A este efecto, se barajaban las siguientes opciones:

1. Adobe InDesign
2. Canva Pro
3. Crello Unlimited
4. Adobe Photoshop

Un factor muy importante en la selección fue el precio de las licencias de uso. En el caso de Adobe InDesign, una suscripción mensual tenía un precio de 60,49€. Sin embargo, la suscripción a Canva Pro costaba solo 11,99€ al mes IVA incluido, precio mucho más asequible. En cuanto a Crello Unlimited, la suscripción ascendía a 9,99€ mensuales, que contrastan con los 60,49€ del servicio de Adobe Photoshop. Con el criterio económico, las dos herramientas de Adobe fueron descartadas por completo, quedando solamente Canva Pro y Crello Unlimited como opciones posibles.

En este momento se pasaron a valorar otros aspectos de los editores, resultando ambos prácticamente iguales. La diferencia que inclinó la balanza hacia Canva Pro fue que ya se había hecho trabajos previamente utilizando esta herramienta, y que era más prudente realizar un trabajo de esta envergadura con una herramienta de la que ya se conocían las limitaciones y fortalezas.

4.2.3. Tecnología utilizada para la web

En cuanto al desarrollo de la web, se optó por no añadir más complejidad al desarrollo del TFG. Esto pasaba por hacer uso de algún sistema de gestión de contenidos, también llamado CMS, que tornase la compleja tarea de la creación de una web en algo más sencillo e intuitivo.

A este efecto, se buscaron los CMS más populares y se compararon a fin de escoger el más apropiado para este trabajo. Mediante búsquedas en internet se vio que las herramientas más recomendadas eran Wordpress, Joomla y Drupal. Entre estas tres se hizo una comparación que tuvo el siguiente resultado:

	Wordpress	**Joomla**	**Drupal**
Nivel de dificultad	Bajo	Medio	Alto
Coste económico	Gratiuito	Gratiuito	Gratiuito
Presencia en la web	Más del 58 %	Más del 7 %	Menos del 5 %

Tabla 4.2: Comparación entre Wordpress, Joomla y Drupal

En base a la comparativa que se realizó, la decisión fue la de utilizar Wordpress debida su alta presencia en el mercado. Esta cuota tan alta implicaba una mayor probabilidad de encontrar soluciones en internet a los posibles problemas que pudieran surgir, ya que tendría una comunidad mucho mayor y por tanto mayor probabilidad de que alguien tuviera los mismos problemas que pudieran surgir.

CAPÍTULO 5

Desarrollo de la solución propuesta

Este capítulo detalla el desarrollo de la solución propuesta y los problemas y dificultades encontradas en el proceso.

5.1 Fase 1. Elaboración de la documentación necesaria

Durante esta primera fase del trabajo se llevó a cabo la redacción y organización de toda la documentación que se entregaría para facilitar el proceso de adecuación a los usuarios finales de la guía.

5.1.1. Creación del libro de cálculo para la fase Plan

Tal y como se estableció en el plan de trabajo, la primera tarea a desarrollar fue la creación del libro de cálculo.

Esta tarea se hizo por duplicado para asegurar que funcionase correctamente tanto en *Excel* como en *Calc*. Se crearon las pestañas en el orden en el que serían utilizadas para facilitar la navegación del usuario por el libro y se asignaron colores a cada pestaña para que resultase más sencilla la identificación de las mismas. Esta tarea transcurrió sin incidencias.

5.1.2. Creación de la hoja de registro de activos

Teniendo en cuenta los requisitos que se habían extraído y se mostraban en la figura 4.3, para crear la hoja de activos se debía crear antes un listado con los diferentes tipos de activos. Estos tipos se extrajeron de MAGERIT v.3, concretamente del libro II [32] y eran los siguientes:

1. [D] Datos / Información
2. [K] Claves criptográficas

3. [S] Servicios
4. [SW] Software - Aplicaciones informáticas
5. [HW] Equipamiento informático (hardware)
6. [COM] Redes de comunicaciones
7. [MEDIA] Soportes de información
8. [AUX] Equipamiento auxiliar
9. [L] Instalaciones
10. [P] Personal

Para limitar las opciones de los usuarios a los tipos de activo propuestos por MAGERIT se restringió la entrada de datos de la columna «Tipo de activo» de forma en que solamente pudiera escogerse uno de los valores de la lista anterior. El resultado fue el siguiente:

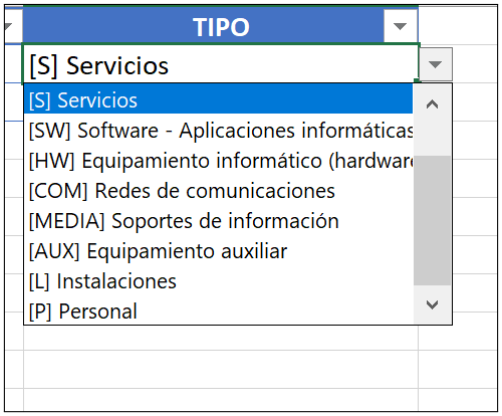


Figura 5.1: Listado desplegable de tipos de activo

De esta forma, era posible limitar las posibles clasificaciones del usuario y evitar valores no contemplados en el futuro, facilitando a la vez la tarea del usuario permitiéndole escoger entre los elementos de esa lista.

Se añadieron además las columnas nombre y descripción de activo para recoger toda la información necesaria.

5.1.3. Creación de la hoja de Categorización del Sistema

Para calcular la categoría de un sistema, es necesario asignar,para cada activo, una puntuación a cada una de las cinco dimensiones de seguridad.

Esta puntuación no debe dejarse al azar, de modo que se creó una hoja de cálculo en que se establecían una serie de criterios que servían de baremo para decidir qué puntuación otorgar en cada momento. A esta hoja se le dio el nombre de «Criterios de Categorización» y su contenido fue extraído directamente de la guía 803 [19].

Su aspecto final fue el siguiente:

NOMBRE	N/A	B	M	A
Disposición legal o administrativa	No existe ninguna disposición legal o administrativa que condicione su nivel.	Por disposición legal o administrativa: ley, decreto, orden, resolución...	Por disposición legal o administrativa: ley, decreto, orden, resolución...	Por disposición legal o administrativa: ley, decreto, orden, resolución...
Perjuicio Directo al ciudadano (de cualquier índole)	No supone ningún perjuicio directo al ciudadano.	Algún perjuicio.	Daño importante, aunque subsanable	Grave daño, de difícil o imposible reparación
Incumplimiento de una Norma: Legal o administrativa	No implica incumplimiento de una norma jurídica.	Incumplimiento formal leve de una norma jurídica, de carácter subsanable	Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable	Incumplimiento formal y material grave de una norma jurídica.
Incumplimiento de una Norma: Regulatoria	No implica incumplimiento de normativa de un regulador.	Implica incumplimiento de normativa de un regulador.	Implica sanción significativa de un regulador.	Implica sanción grave de un regulador y/o pérdida de licencia de operar.
Incumplimiento de una Norma: Contractual	No implica incumplimiento de una obligación contractual.	Incumplimiento formal leve de una obligación contractual.	Incumplimiento material o formal de una obligación contractual.	Incumplimiento formal o material grave de una obligación contractual.
Incumplimiento de una Norma: Interna	No implica incumplimiento de normativa interna.	Incumplimiento formal leve de una norma interna.	Incumplimiento material o formal de una norma interna.	Incumplimiento formal o material grave de una norma interna.
Pérdidas económicas	No implica pérdidas económicas.	Pérdidas económicas apreciables (no superiores al 4% del presupuesto anual de la organización).	Pérdidas económicas importantes (superiores al 4% e inferiores al 10% del presupuesto anual de la organización).	Pérdidas económicas o alteraciones financieras significativas (superiores al 10% del presupuesto anual de la
Reputación	No implica daño reputacional.	Daño reputacional moderado con los ciudadanos o con otras organizaciones.	Daño reputacional significativo con los ciudadanos o con otras organizaciones.	Daño reputacional grave con los ciudadanos o con otras organizaciones.
Protestas	No se prevé que pueda desembocar en protestas.	Múltiples protestas individuales.	Protestas públicas (alteración del orden público).	Protestas masivas (alteración seria del orden público).
Delitos	No facilitaría la comisión de delitos ni dificultaría su investigación.	Favorecería la comisión de delitos	Favorecería significativamente la comisión de delitos o dificultaría su investigación.	Podría incitar a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.
RTO – Tiempo Objetivo de Recuperación	La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO)	La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO)	La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO)	La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO)
	0	1	2	3

Figura 5.2: Criterios de categorización de activos

Una vez claros los criterios con los que otorgar puntuaciones se pasó a crear la hoja de «Categorización». Esta estaría formada por todos los activos identificados en la anterior hoja, que son automáticamente importados a la siguiente pestaña, y cinco columnas, una para cada dimensión de seguridad, que solo pueden valorarse con una de las cuatro opciones que se mencionan en los criterios. Para esto nuevamente se volvió a añadir una lista desplegable a cada celda de las pertenecientes a las dimensiones de seguridad.

Tras esto se procedió al cálculo de la categoría del sistema y de las distintas dimensiones. En primer lugar, se obtuvo el nivel máximo para cada dimensión siendo este el nivel de la misma y, tras esto, se midió la categoría del sistema como el máximo entre los niveles de las dimensiones. Estos resultados se muestran en la misma hoja así:

BAJO	**0**	**0**	**0**	**0**	**0**
MEDIO	**1**	**0**	**0**	**0**	**0**
ALTO	0	0	0	0	0
	[C]	[I]	[D]	[A]	[T]
RESULTADO	M	B	B	B	B
				TOTAL	M
	CATEGORÍA	MEDIA			

Figura 5.3: Cálculo de la categoría del sistema

5.1.4. Creación de la Declaración de Aplicabilidad automática

Una vez hecha la categorización, era necesario averiguar qué medidas eran de aplicación a cada sistema y qué acciones de control se debían implementar teniendo en cuenta no solamente qué categoría tenía nuestro sistema en general sino cada una de las dimensiones de seguridad. Esto es así porque existen medidas que solo afectan a algunas dimensiones de seguridad y estas solo han de ser protegidas obligatoriamente al nivel máximo de la dimensión que se está protegiendo.

Por esa razón, se hace un mapeo de la relación entre las distintas medidas y las dimensiones en las que afectan. Este mapeo se basa en lo establecido en el Anexo II del ENS [1] y después de realizarlo tiene el siguiente aspecto:

ID	Disponibilidad [D]	Autenticidad [A]	Integridad [I]	Confidencialidad [C]	Trazabilidad [T]
00.000.0000					
00.000.0001	Sí	Sí	Sí	Sí	Sí
00.000.0010	Sí	Sí	Sí	Sí	Sí
00.000.0011	Sí	Sí	Sí	Sí	Sí
00.000.0100	Sí	Sí	Sí	Sí	Sí
01.000.0000					
01.000.0001	Sí	Sí	Sí	Sí	Sí
01.000.0010	Sí	Sí	Sí	Sí	Sí
01.000.0011	Sí	Sí	Sí	Sí	Sí
01.000.0100	Sí	No	No	No	No
01.000.0101	Sí	Sí	Sí	Sí	Sí
01.001.0000					
01.001.0001	No	Sí	No	No	Sí
01.001.0010	No	Sí	Sí	Sí	Sí
01.001.0011	No	Sí	Sí	Sí	Sí
01.001.0100	No	Sí	Sí	Sí	Sí
01.001.0101	No	Sí	Sí	Sí	Sí
01.001.0110	No	Sí	Sí	Sí	Sí
01.001.0111	No	Sí	Sí	Sí	Sí
01.010.0000					
01.010.0001	Sí	Sí	Sí	Sí	Sí
01.010.0010	Sí	Sí	Sí	Sí	Sí
01.010.0011	Sí	Sí	Sí	Sí	Sí
01.010.0100	Sí	Sí	Sí	Sí	Sí
01.010.0101	Sí	Sí	Sí	Sí	Sí
01.010.0110	Sí	Sí	Sí	Sí	Sí
01.010.0111	Sí	Sí	Sí	Sí	Sí
01.010.1000	No	No	No	No	Sí
01.010.1001	Sí	Sí	Sí	Sí	Sí
01.010.1010	No	No	No	No	Sí
01.010.1011	Sí	Sí	Sí	Sí	Sí
01.011.0000					
01.011.0001	Sí	Sí	Sí	Sí	Sí
01.011.0010	Sí	Sí	Sí	Sí	Sí
01.011.0011	Sí	No	No	No	No
01.100.0000					
01.100.0001	Sí	No	No	No	No
01.100.0010	Sí	No	No	No	No
01.100.0011	Sí	No	No	No	No
01.101.0000					

Figura 5.4: Impacto de cada medida sobre las distintas dimensiones de seguridad

Teniendo claro como afecta esto a los niveles exigidos por el ENS, se creó una fórmula que mostrase automáticamente las medidas exigidas a ese sistema.

Además, la categoría del sistema influye directamente en el nivel de protección que se pide. A este nivel se le llama «nivel de madurez», y su escala es la siguiente [27]:

1. **L0 - Inexistente.** Con una cobertura del 0 %, supone no aplicar esa medida de seguridad.
2. **L1 - Inicial/ ad hoc.** Con una cobertura del 10 %, supone que las medidas existen pero no se están gestionan.
3. **L2 - Reproducible pero intuitivo.** Con una cobertura del 50 %, supone tener unas medidas que se gestionan de forma intuitiva, sin tener planes ni similares. Es el mínimo exigible para sistemas de categoría básica.

4. **L3 - Proceso definido.** Con una efectividad del 90 %, las medidas se gestionan y despliegan con conocimiento de causa y se mantienen adecuadamente. Es el mínimo exigible para sistemas de categoría media.
5. **L4 - Gestionado y medible.** Con una efectividad del 95 %, implica una gestión que permite controlar la efectividad de las medidas e incorporar procesos de control de la calidad de forma contrastable. Es el mínimo exigible para sistemas de categoría alta.
6. **L5 - Optimizado.** Con una eficacia del 100 %, se centra en mejorar de forma continuada las medidas implementadas, estableciendo objetivos concretos de mejora de los procesos. Se llevan a cabo revisiones periódicas que se utilizan como indicadores en la gestión de mejora de los procesos.

Este nivel de madurez se determinó en base a la categoría del sistema y de la valoración de las dimensiones de seguridad a las que afectaba cada medida. De este modo, la «Declaración de Aplicabilidad» se calcula automáticamente a medida que se van valorando las dimensiones en el paso anterior del proceso de adecuación.

5.1.5. Creación de la hoja de Análisis de Riesgos

Una vez identificadas las medidas que hay que cumplir de manera obligatoria, se debe realizar un análisis de riesgos para averiguar otras posibles acciones a tomar para proteger la organización.

Esta hoja de cálculo se crea pensando en las amenazas de MAGERIT v.3, que se importarán más tarde a otra hoja. El cálculo del riesgo se hace mediante la siguiente fórmula:

$$R = P \cdot I \tag{5.1}$$

Siendo «R» el riesgo al que se expone un determinado activo, «P» la probabilidad de que una amenaza se materialice e «I» el impacto que esa materialización tendría en la organización.

Es por ello que la hoja se diseñó para que a cada activo identificado se le puedan asignar todas las amenazas que le corresponden a su tipo de activo, y valorar entonces la probabilidad de que se produzca dicha amenaza y el impacto sobre cada dimensión de seguridad. Con todo ello, se calcula un nivel de riesgo con valor entre 1 y 100 para el que se tendrá que establecer un nivel de riesgo aceptable y tras ello tomar medidas que reduzcan los riesgos no tolerados.

5.1.6. Creación de la hoja de Perfil de Cumplimiento

Habiendo realizado las anteriores tareas con normalidad y dentro de los plazos previstos, se pasó a implementar la hoja de perfil de cumplimiento. En primer lugar, se tuvieron en cuenta los umbrales de madurez que establece la guía 824 del CCN[27]:

- **Sistema de categoría básica.** Se considera un nivel inaceptable y incumplimiento casi total un porcentaje de menos del 40 %. Tampoco es un nivel aceptable el menor

del 50 %, aunque el incumplimiento ya no es tan flagrante. Se considerará un nivel adecuado todo aqueñ mayor o igual al 50 %.

- **Sistema de categoría media.** Se considera un nivel inaceptable y incumplimiento casi total un porcentaje de menos del 50 %. Tampoco es un nivel aceptable el menor del 80 %, aunque el incumplimiento ya no es tan flagrante. Se considerará un nivel adecuado todo aqueñ mayor o igual al 80 %.

- **Sistema de categoría alta.** Se considera un nivel inaceptable y incumplimiento casi total un porcentaje de menos del 80 %. Tampoco es un nivel aceptable el menor del 90 %, aunque el incumplimiento ya no es tan flagrante. Se considerará un nivel adecuado todo aqueñ mayor o igual al 90 %.

Teniendo claros los umbrales citados y las coberturas aportadas por los niveles de madurez, se optó por generar una hoja de cálculo que mostrase para cada medida de seguridad el nivel de protección, de modo que se calculara para cada marco el umbral alcanzado y para el sistema también.

5.1.7. Creación de la hoja con las medidas del Anexo II

Una vez finalizadas las hojas con mayor dificultad de diseño, se procedió a crear todas las hojas relacionadas con el cumplimiento del Anexo II del ENS. Estas hojas eran:

- Medidas del Anexo II

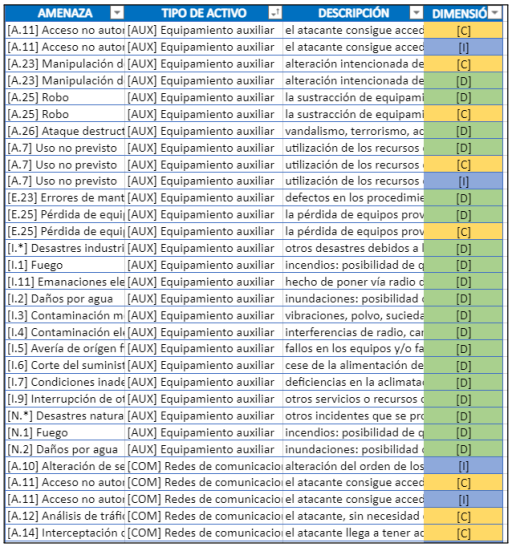
- Medidas del AII por Dimensiones

- Medidas del AII por Categoría del Sistema.

Todas ellas consistían en trasladar los distintos aspectos del citado anexo a una hoja de cálculo para basar en esto las medidas y niveles correspondientes a cada organización.

5.1.8. Creación de la hoja de Amenazas según MAGERIT v.3

En esta tarea, se trasladó el contenido del segundo libro de MAGERIT v.3 a una hoja que relacionaba cada tipo de activo sus correspondientes amenazas y a las dimensiones que se veían afectadas por esta. El resultado fue el siguiente:



AMENAZA	TIPO DE ACTIVO	DESCRIPCIÓN	DIMENSIÓ
[A.11] Acceso no autor	[AUX] Equipamiento auxiliar	el atacante consigue acced	[C]
[A.11] Acceso no autor	[AUX] Equipamiento auxiliar	el atacante consigue acced	[I]
[A.23] Manipulación d	[AUX] Equipamiento auxiliar	alteración intencionada de	[C]
[A.23] Manipulación d	[AUX] Equipamiento auxiliar	alteración intencionada de	[D]
[A.25] Robo	[AUX] Equipamiento auxiliar	la sustracción de equipami	[D]
[A.25] Robo	[AUX] Equipamiento auxiliar	la sustracción de equipami	[C]
[A.26] Ataque destruct	[AUX] Equipamiento auxiliar	vandalismo, terrorismo, ac	[D]
[A.7] Uso no previsto	[AUX] Equipamiento auxiliar	utilización de los recursos	[D]
[A.7] Uso no previsto	[AUX] Equipamiento auxiliar	utilización de los recursos	[C]
[A.7] Uso no previsto	[AUX] Equipamiento auxiliar	utilización de los recursos	[I]
[E.23] Errores de mant	[AUX] Equipamiento auxiliar	defectos en los procedimie	[D]
[E.25] Pérdida de equi	[AUX] Equipamiento auxiliar	la pérdida de equipos prov	[D]
[E.25] Pérdida de equi	[AUX] Equipamiento auxiliar	la pérdida de equipos prov	[C]
[I.*] Desastres industri	[AUX] Equipamiento auxiliar	otros desastres debidos a l	[D]
[I.1] Fuego	[AUX] Equipamiento auxiliar	incendios: posibilidad de q	[D]
[I.11] Emanaciones ele	[AUX] Equipamiento auxiliar	hecho de poner vía radio c	[D]
[I.2] Daños por agua	[AUX] Equipamiento auxiliar	inundaciones: posibilidad	[D]
[I.3] Contaminación m	[AUX] Equipamiento auxiliar	vibraciones, polvo, suciedad	[D]
[I.4] Contaminación el	[AUX] Equipamiento auxiliar	interferencias de radio, ca	[D]
[I.5] Avería de orígen f	[AUX] Equipamiento auxiliar	fallos en los equipos y/o fa	[D]
[I.6] Corte del suminist	[AUX] Equipamiento auxiliar	cese de la alimentación de	[D]
[I.7] Condiciones inade	[AUX] Equipamiento auxiliar	deficiencias en la aclimata	[D]
[I.9] Interrupción de ot	[AUX] Equipamiento auxiliar	otros servicios o recursos	[D]
[N.*] Desastres natura	[AUX] Equipamiento auxiliar	otros incidentes que se pro	[D]
[N.1] Fuego	[AUX] Equipamiento auxiliar	incendios: posibilidad de q	[D]
[N.2] Daños por agua	[AUX] Equipamiento auxiliar	inundaciones: posibilidad	[D]
[A.10] Alteración de se	[COM] Redes de comunicacio	alteración del orden de los	[I]
[A.11] Acceso no autor	[COM] Redes de comunicacio	el atacante consigue acced	[C]
[A.11] Acceso no autor	[COM] Redes de comunicacio	el atacante consigue acced	[I]
[A.12] Análisis de tráfi	[COM] Redes de comunicacio	el atacante, sin necesidad	[C]
[A.14] Interceptación c	[COM] Redes de comunicacio	el atacante llega a tener ac	[C]

Figura 5.5: Relación entre tipo de activo y amenaza

Esta tabla tiene 274 filas y se puede filtrar en función del tipo de activo a valorar para facilitar el análisis de riesgos.

5.1.9. Creación de la Política de Seguridad de la Información

Para realizar la Política de Seguridad de la Información se siguió la plantilla del Centro Criptológico Nacional. Se redactó conforme a la guía CCN-STIC 805[21], introduciendo campos de texto en los que indicar aquello que más se repite en el documento a fin de que la edición sea lo más ágil posible.

5.1.10. Creación del Manual de Seguridad

Este documento está formado por todos los procedimientos y normativas de seguridad que se deben aprobar para cumplir con el ENS. Se redactó en base a lo establecido por las guías 821[25] y 822[26], y se incluyeron los 11 anexos que en estas figuran para asegurar el cumplimiento de los mínimos que solicita el RD 3/2010.

5.1.11. Creación del Plan de Adecuación

Este documento está basado en la guía CCN-STIC 806 de «Plan de Adecuación al ENS», y contiene todos los aspectos que se recogen en el libro de cálculo completamente redactados y listos para personalizarse. Esta tarea fue laboriosa aunque especialmente sencilla debido a la gran cantidad de material que aporta el Centro Criptológico Nacional en este ámbito.

5.2 Fase 2. Redacción de la Guía para la Adecuación de Organizaciones al Esquema Nacional de Seguridad

5.2.1. Cómo utilizar esta guía

La guía está graduada en función del nivel de conocimiento del lector del ámbito informático y de sus competencias técnicas. Consta de tres niveles de lectura: básico, intermedio y avanzado.

Para aquel lector que desconoce por completo los conceptos y herramientas técnicas relacionados con el Esquema Nacional de Seguridad se recomienda un seguimiento de la guía en nivel básico. En este nivel, se utiliza un vocabulario asequible y se pretenderá que el lector comprenda los conceptos clave y sea capaz de llevar a cabo una adecuación al ENS de su organización siguiendo los pasos que en esta guía se detallen.

En el caso un lector que tiene nociones básicas de los conceptos y métodos que tienen relación directa con este marco normativo, se recomienda la lectura en un nivel medio. En este nivel, se utiliza un vocabulario asequible, pero se dan por asumidos los conceptos más básicos. Se pretende que el usuario de la guía consiga adecuar su organización al Esquema Nacional de Seguridad con instrucciones claras de los pasos a seguir sin entrar en profundidad en las partes técnicas.

Por último, en caso del leyente que tiene un perfil más técnico y conoce el significado de los términos utilizados en el Esquema Nacional de Seguridad, se recomienda la lectura en el nivel avanzado. La guía le da una vista más general de las tareas a desarrollar y le dota de los recursos necesarios para conseguir la adecuación de su organización a los cánones establecidos en la ley 3/2010.

5.2.2. Contenido de la guía

El grueso de la guía está dedicado a la explicación en detalle de cada paso a realizar. Desde los pasos a seguir establecidos por el CCN hasta los pasos a seguir para hacer un buen uso del material que se ha desarrollado en la primera fase de este trabajo.

El contenido se dividió en tres bloques diferenciados mediante unos iconos que contenían la misma explicación a los tres niveles de conocimiento que se contemplan como público de la guía. Todos los puntos se estructuraron de la misma forma y se introdujeron imágenes que intentaban ser ilustrativas del contenido que se estaba explicando a fin de hacer más fácil su comprensión.

5.2.3. Declaración o Certificación de Conformidad

En este apartado, la guía difiere y explica los motivos por los cuales una organización no puede auditarse a sí misma, especialmente cuando se trata de asuntos de seguridad del sistema.

Se expone también cómo la autoridad de control es la que impone que este proceso se debe realizar mediante una auditoría externa y que no será evitable. Se recomienda buscar profesionales reconocidos en el ámbito para intentar que esa inversión sea lo más fructífera posible y se pone a disposición del usuario la guía 808 de «Verificación del Cumplimiento del ENS» en la que se plantean las diferentes preguntas que hará un auditor para determinar su cumplimiento a fin de facilitar una autoevaluación previa al desembolso. De esta manera se pretenden evitar situaciones en las que las organizaciones gasten un dinero en una auditoría que no les dará el distintivo de conformidad.

5.2.4. Vigilancia y Mejora Continua

En el último apartado de la guía, se expone la necesidad de invertir tiempo y recursos en el mantenimiento y mejora de la seguridad de los sistemas. Sirve como un pequeño seminario de concienciación y aporta un documento con periodicidades recomendables de revisión del trabajo del ENS.

Por último, se recuerda al lector que esta última fase no implica finalizar con el ENS, sino que este marco es una cosa que deberán tener siempre en mente en adelante, y que el hecho de tener un distintivo de seguridad en el presente no implica que se conserve en el futuro.

5.3 Fase 3. Desarrollo de la página web

5.3.1. Página de inicio

La página de inicio consiste en una plantilla proporcionada por Wordpress. El trabajo a realizar ha sido el de conseguir los enlaces de las páginas para hacer funcionar los botones. No es una tarea compleja ni costosa en el tiempo y Wordpress pone todas las facilidades.

El resultado final de esta página es el siguiente:

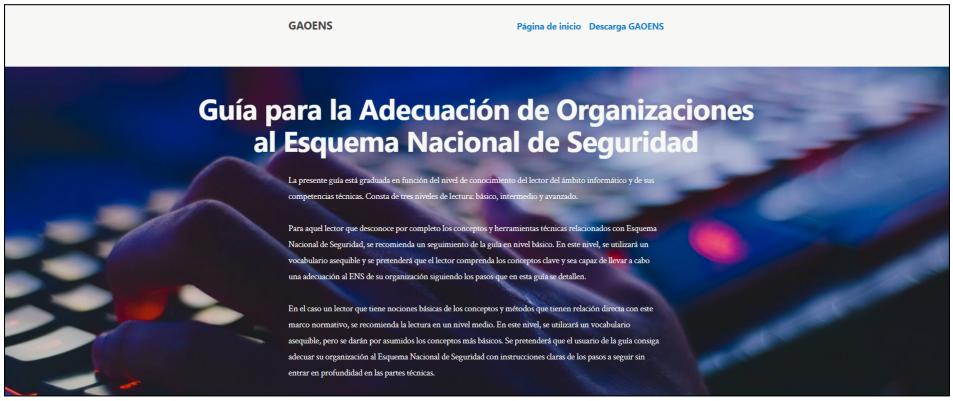


Figura 5.6: Menú superior y primer vistazo de la web

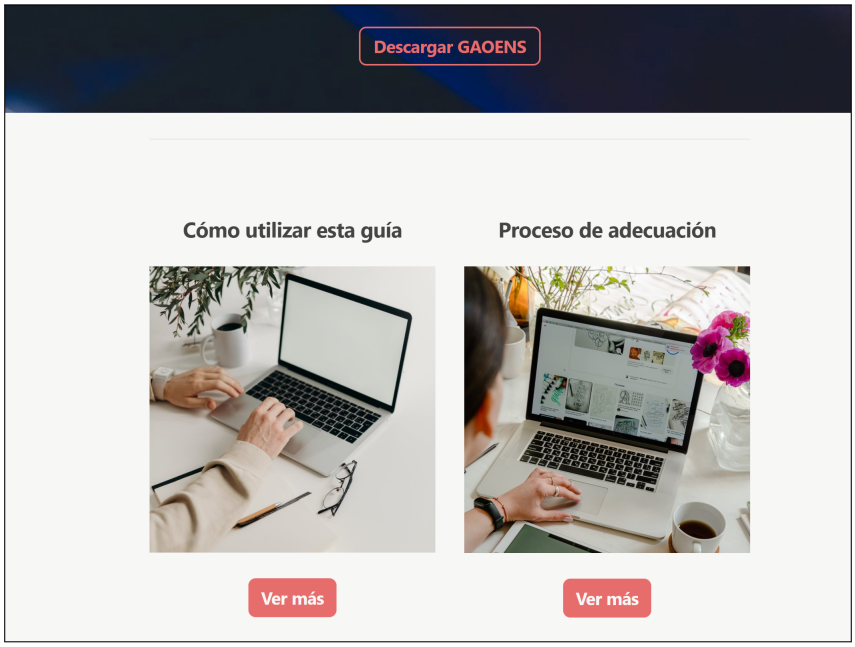


Figura 5.7: Botón de descarga y enlaces a páginas temáticas

5.3.2. Página de índice

La página de índice es, una vez más, la plantilla que se había establecido con anterioridad, solo que esta vez con texto y enlaces mediante botones a las páginas con el contenido de la guía. La apariencia final es la siguiente:

Figura 5.8: Página de índice

5.3.3. Páginas de contenido

En cuanto a las páginas de contenido, todas siguen una misma estructura:

- Encabezado con título en magenta corporativo.
- Bloques de colores alternos con las diferentes secciones del punto.
- Bloque final con botones al punto anterior y al punto siguiente.

Con ello se consigue una estética semejante a la que se ve a continuación.

Figura 5.9: Página de contenido general

5.3.4. Página de descarga

A fin de diferenciar esta página del resto de páginas de contenido, la estética de la página de descarga de la guía es más similar a la página de inicio.

Se ha optado por una imagen de fondo con letras superpuestas a ella y botones llamativos que inviten a descargar el contenido disponible.

El resultado es el siguiente:

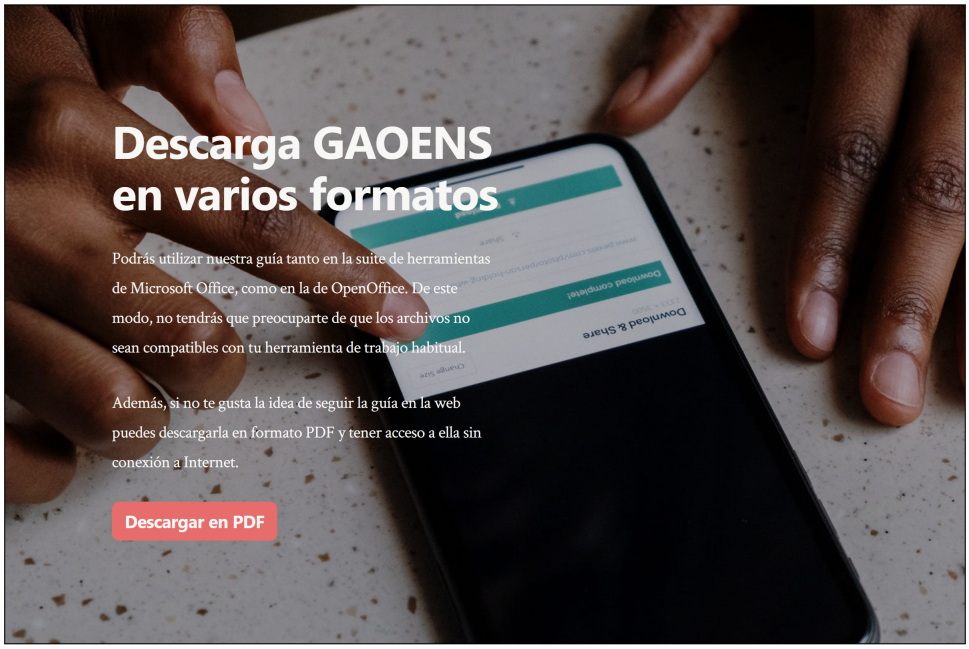


Figura 5.10: Página de descarga, descarga PDF

Figura 5.11: Página de descarga, contenido en ZIP y RAR

CAPÍTULO 6

Pruebas

En este apartado, se presentan las pruebas realizadas para verificar que la guía funciona correctamente. Se explican a continuación los procesos a los que se ha sometido al producto de este trabajo para averiguar si se ha cumplido con su cometido.

6.1 Búsqueda de organizaciones

En primer lugar, se ha procedido a buscar posibles organizaciones que estuvieran dispuestas a llevar a cabo un proceso de adecuación al Esquema Nacional de Seguridad sin coste alguno, dejándose hecho el trabajo para poder conseguir una Declaración de Conformidad.

En primer lugar, se contactó a entidades locales de pequeño tamaño donde se sabía que no había personal especializado en Informática. Fueron contactadas un total de 20 entidades locales de la provincia de Valencia con menos de mil habitantes, de estas solo 2 contestaron a la propuesta y ninguna lo hizo de forma afirmativa. Las razones que se dieron fueron falta de tiempo que dedicarle al proceso y que creían que sería una carga de trabajo demasiado alta para el poco personal del que se disponía.

Tras este fracaso, se contactó a una entidad de la que se sabía que se estaba llevando a cabo una consultoría del Esquema Nacional de Seguridad y que tenía personal con formación específica. Esta entidad se mostró dispuesta a colaborar a condición de no revelar los datos que se iban a dar ni el nombre de la misma, y fue la que finalmente testeó la solución.

6.2 Prueba en organización con personal profesional

Esta entidad, a la que llamaremos por el pseudónimo de «la Naranja», recibió la guía y toda la documentación adjunta el lunes 21 de junio. Para comprobar cómo se desenvolvería una organización cualquiera en condiciones normales, simplemente se les indicó que se proporcionara información del avance del proceso.

Se recibieron noticias de la Naranja por primera vez el miércoles 23 de junio, indicando que habían terminado la fase de«*Plan*». Se mantuvo entonces una reunión en la que se revisó toda la información que se había introducido en la guía y se compararon los resultados obtenidos con los de la consultoría que se estaba llevando a cabo de forma paralela. El resultado de la comparación fue que la guía que se había desarrollado ajustaba mejor la Declaración de Aplicabilidad de lo que lo había hecho la consultoría externa contratada por más de 10.000€, ya que esta simplemente tomaba el nivel del sistema como nivel a cumplir para todas las medidas y la guía desarrollada en este trabajo tenía en cuenta de forma individual cada dimensión de seguridad, ajustando a ese nivel las medidas que correspondían. Además, la Naranja estaba especialmente satisfecha con la información que se proporcionaba en el Perfil de Cumplimiento, al poder saber de forma precisa en qué medidas debía centrar los esfuerzos de mejora de la seguridad.

Tras esta primera comprobación, se pasó a la fase de «*Do*». En este punto, la consultoría privada tuvo mejor valoración, al proporcionar toda la documentación ya completamente personalizada a la Naranja con el correspondiente ahorro de tiempo. No obstante, se valoró positivamente la figura del Manual de Seguridad, puesto que comentaban que la existencia de tantos documentos por separado implicaba repeticiones entre los apartados de algunos de los documentos.

La Naranja obtuvo una puntuación favorable al cumplimiento del ENS y valoró el trabajo con una media de 8,5 entre los componentes del equipo técnico.

CAPÍTULO 7

Conclusiones

Con el índice de satisfacción conseguido, se puede decir que los objetivos han sido alcanzados ya que:

- Se ha obtenido una guía comprensible.
- Se ha simplificado al máximo el proceso de adecuación al ENS.
- Se han seguido las guías de buenas prácticas de la autoridad de control.

Gracias al desarrollo de este trabajo, se han adquirido competencias y conocimientos muy profundos del ENS que serán de utilidad para el desempeño de las funciones de Consultora de TI en este ámbito.

7.1 Relación del trabajo desarrollado con los estudios cursados

A lo largo del grado se han cursado las siguientes asignaturas relacionadas con el presente trabajo:

1. Deontología y profesionalismo.
2. Gestión de proyectos.
3. Gestión de Servicios de SI y TI.
4. Comportamiento Organizativo y Gestión del Cambio

Cabe destacar que gracias a la realización de este trabajo he podido experimentar de primera mano las dificultades a las que se enfrentan los profesionales del sector de la consultoría de Sistemas de la Información. A raíz de encontrarme sola frente a una norma que desconocía completamente y tener que desarrollar por mi cuenta las utilidades que me ayudarían no solo a mí, sino también a potenciales clientes, he podido llegar a valorar realmente el trabajo que desarrollan los y las consultores y consultoras y he extraído de ello que su labor es de un valor inestimable.

7.2 Trabajos futuros

En cuanto a posibles trabajos se plantea lo siguiente:

- Desarrollo de una aplicación de adecuación al ENS que cubra todas las fases del proceso y sea compatible con las guías del CCN.
- Diseño de un manual de ciberseguridad para el personal público.
- Diseño de una estrategia de concienciación de ciberseguridad para directivos y cargos electos de Administraciones Públicas.
- Automatización de la creación de documentación necesaria para el cumplimiento del ENS.

Bibliografía

[1] 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/buscar/act.php?id=BOE-A-2010-1330

[2] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Estrategia para el Mercado Único Digital de Europa.
Consultado en https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:52015DC0192

[3] Digital Economy and Society Index (DESI) 2020.
Consultado en https://digital-strategy.ec.europa.eu/en/policies/desi

[4] E-Government Survey 2020. Digital Government in the Decade of Action for Sustainable Development.
Consultado en https://www.un.org/development/desa/publications/publication/2020-united-nations-e-government-survey

[5] CCN-CERT AV 46/20 Informe Nacional del Estado de la Seguridad.
Consultado en https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/10124-ccn-cert-av-46-20-informe-nacional-del-estado-de-la-seguridad-resultado-general.html

[6] John P. Kotter.
Leading Change Harvard Business Review Press, New edition , 2012

[7] Centro Criptológico Nacional y Federación Española de Municipios y Provincias Prontuario de ciberseguridad para entidades locales.
ENS en Entidades Locales, abril de 2021.

[8] Plataforma de Contratación del Sector Público. Expediente: SC/08/2020.
Consultado en https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQjDSq9HIuzLCqzHQtzC40MSysykhLDAm1t9Qtycx0Bp4nuVA!!/

[9] Plataforma de Contratación del Sector Público. Expediente:MTB004/19.
Consultado en

[10] Plataforma de Contratación del Sector Público. Expediente:
Consultado en

[11] España Municipal 2021, INE
Consultado en https://www.ine.es/infografias/infografia_padron.pdf

[12] Cifras oficiales de población resultantes de la revisión del Padrón municipal a 1 de enero, INE
Consultado en https://www.ine.es/jaxiT3/Datos.htm?t=2917#!tabs-tabla

[13] Código de Derecho de la Ciberseguridad. Agencia Estatal Boletín Oficial del Estado.
Consultado en https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1

[14] Wiki de la metodología de gestión de proyectos PRINCE2.
Consultada en https://prince2.wiki/es/

[15] Página web del CCN para el Esquema Nacional de Seguridad.
Consultado en https://ens.ccn.cni.es/es/

[16] Guía de Seguridad de las TIC CCN-STIC-800 Glosario de términos y abreviaturas del ENS.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/499-ccn-stic-800-glosario-de-terminos-y-abreviaturas-del-ens/file.html

[17] Guía de Seguridad de las TIC CCN-STIC- 801 Esquema Nacional de Seguridad. Responsabilidades y funciones.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/501-ccn-stic-801-responsibilidades-y-funciones-en-el-ens/file.html

[18] Guía de Seguridad de las TIC 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

[19] Guía de Seguridad de las TIC CCN-STIC-803. ENS. Valoración de los sistemas.Actualizada en mayo de 2020.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html

[20] Guía de Seguridad de las TIC 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

[21] Guía de Seguridad de las TIC CCN-STIC- 805 Modelo de Política de Seguridad.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html

[22] Guía de Seguridad de las TIC CCN-STIC-806. Plan de Adecuación al ENS. Actualizada en junio de 2020.
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

[23] Guía de Seguridad de las TIC 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/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

[24] Guía de Seguridad de las TIC CCN-STIC-809 Declaración, certificación y aprobación provisional de conformidad con el ENS y distintivos de cumplimiento.
Consultado en 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

[25] Guía de Seguridad de las TIC CCN-STIC-821 Normas de Seguridad en el ENS.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/529-ccn-stic-821-normas-de-seguridad-en-el-ens/file.html

[26] Guía de Seguridad de las TIC CCN-STIC-822 Procedimientos de Seguridad.
Consultado en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/537-ccn-stic-822-procedimientos-de-seguridad/file.html

[27] Guía de Seguridad de las TIC CCN-STIC-824 Información del Estado de Seguridad.
Consultado en 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

[28] Guía de Seguridad de las TIC CCN-STIC-882 Guía de Análisis de Riesgos para Entidades Locales.
Consultado en https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3803-ccn-stic-882-guia-de-analisis-de-riesgos-para-entidades-locales/file.html

[29] Guía de Seguridad de las TIC CCN-STIC-883 Guía de implantación del ENS para Entidades Locales.
Consultado en https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/3758-ccn-stic-883-guia-de-implantacion-del-ens-para-entidades-locales/file.html

[30] CCN-CERT BP/14. Declaración de aplicabilidad en el ENS (Perfil de Cumplimiento). Actualizada en junio 2019.
Consultado en https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/3830-ccn-cert-bp-14-declaracion-de-aplicacibilidad-ens/file.html

[31] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.
Consultado en https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

[32] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos.
Consultado en https://administracionelectronica.gob.es/pae_Home/dam/jcr:5fbe15c3-c797-46a6-acd8-51311f4c2d29/2012_Magerit_v3_libro2_catalogo-de-elementos_es_NIPO_630-12-171-8.pdf

[33] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.

Consultado en https://administracionelectronica.gob.es/pae_Home/dam/jcr:130c633a-ee11-4e17-9cec-1082ceeac38c/2012_Magerit_v3_libro3_guia-de-tecnicas_es_NIPO_630-12-171-8.pdf

APÉNDICE A

Glosario

[A]

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.
Adecuación. Aptitud o idoneidad de una acción o de un curso casual para producir un efecto o un resultado de lesión o de peligro.
Administración electrónica. Acceso electrónico a la Administración.
Amenaza. Delito consistente en intimidar a alguien con el anuncio de la provocación de un mal grave para él o su familia. **Análisis de riesgos.** Estudio para evaluar los peligros potenciales y sus posibles consecuencias en una instalación existente o en un proyecto, con el objeto de establecer medidas de prevención y de protección.
Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.
Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

[C]

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.
Clave criptográfica. Parámetro usado por un algoritmo criptográfico para cifrar y descifrar datos, obtener la firma digital de unos datos, verificar ésta o calcular un código de autenticación de mensajes o una función resumen.
Consultoría. Actividad del consultor
Conformidad. Asenso, aprobación.
Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. **Copyright.** Derecho de autor. **Ciberseguridad.** Conjunto de elementos, medidas y equipos destina-

dos a controlar la seguridad informática de una entidad o espacio virtual.

[D]

Datos personales. Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. **Deontología.** Parte de la ética que trata de los deberes, especialmente de los que rigen una actividad profesional.
Digitalización. Registro de datos en formato digital.
Disposición transitoria. parte de una norma en la que se regulan aspectos temporales, es decir que tienen un carácter no permanente.
Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren

[E]

Eficiente. Que tiene eficiencia.
Eficaz. Que tiene eficacia.
Ética. Conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida

[F]

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

[G]

Gestión del cambio. La gestión del cambio es un enfoque integral, cíclico y estructurado para lograr la transición de individuos, grupos y organizaciones de un estado actual a un estado futuro con los beneficios empresariales previstos.
Gestión de incidentes. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

[I]

Incidente de seguridad. Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.
Información. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.
Infraestructura. Conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de un país, de una ciudad o de una organización cualquiera.
Integridad.
Insuficiencia. Incapacidad total o parcial de un órgano para realizar adecuadamente sus funciones.

Implementación. Acción y efecto de implementar.

[L]

Licitación. Acción y efecto de licitar.

[M]

Marco normativo. Conjunto general de normas, criterios, metodologías, lineamientos y sistemas, que establecen la forma en que deben desarrollarse las acciones para alcanzar los objetivos propuestos en el proceso de programación-Presupuestación.
Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

[O]

Ofimático. Automatización, mediante sistemas electrónicos, de las comunicaciones y procesos administrativos en las oficinas.

[P]

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.
Política de seguridad. Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.
Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado. Proceso de seguridad.
Proyecto. Conjunto de escritos, cálculos y dibujos que se hacen para dar idea de cómo ha de ser y lo que ha de costar una obra de arquitectura o de ingeniería.

[R]

Red. Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden intercambiar información.
Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.
Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

[S]

Seguridad. Cualidad de seguro
Seguridad de las redes y de la información. Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.
Servicio. Prestación que satisface alguna necesidad humana y que no consiste en la producción de bienes materiales.
Sistema de Gestión de la Seguridad de la Información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
Sistema de Información. Aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento.
Software. Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

[T]

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
TIC. Conjunto de técnicas y equipos informáticos que permiten comunicarse a distancia por vía electrónica.

[U]

Usuario. Dicho de una persona: Que tiene derecho de usar de una cosa ajena con cierta limitación.

[V]

Vulnerabilidad. Vulnerabilidad es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes.