Guía general de adecuación al Esquema Nacional de Seguridad.

Producto de la Memoria

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

Estudiante: Francisco Jose Muñoz Torrijos

Nombre del consultor: Ana Maria Chulia Cebolla

Fecha entrega: 11 de Junio de 2018

Índice

1. Introducción

El presente documento tiene por objetivo cumplir con la adaptación al ENS. Es el resultado de extraer la esencia de un trabajo previo o memoria que permite cumplir con la normativa respecto del ENS, y una vez finalizados permiten obtener una idea clara y nítida de su estado de cumplimiento, de las auditorías a realizar y a familiarizarse con el proceso de mejora continua requerido para su mantenimiento, necesario para adaptarse a las nuevas tecnologías futuras y nuevos servicios ofrecidos por la organización, tratando siempre de alcanzar la excelencia en los procesos con las sucesivas iteraciones.

La memoria de la que se extrae el documento es fruto de la lectura de la normativa en relación al ENS, de las guías las guías STIC serie 800 del CCN, de la consulta en internet y del caso de estudio con la finalidad de extraer el conocimiento de un caso práctico, este se ha realizado sobre una universidad ficticia de cierta envergadura ofreciendo los servicios más habituales.

El documento tiene una vocación totalmente práctica, tratando de establecer los pasos mínimos necesarios y suficientes para los fines que persigue de adecuación al ENS.

2. Documentación

La primera tarea a realizar será recomendar la lectura 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 con detenimiento para entender las metas que se persiguen.

Se deberá de seguir con la lectura del Real Decreto 951/2015 de 23 de octubre. Cambios en la regulación del Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

Se completará la tarea de documentación y comprensión del alcance del ENS con la visita a la web del CCN para la revisión de las guías STIC de la Serie 800 creadas para normalizar y ayudar en la realización de las diferentes tareas del ENS.

Para completar el trabajo de adecuación se han desarrollado plantillas de documentos (en su mayoría documentos originales) tratando de crear cierta homogeneidad entre ellos debido a la falta de información disponible. Estos

deberán de ser adaptados a cada organización. Las plantillas se presentan como anexos.

3. Política de seguridad.

El primer paso para la adaptación al ENS es la creación de la Política de Seguridad, es un requisito imprescindible y debe de ser aprobado por el órgano superior competente que corresponda teniendo que estar accesible a todos los miembros de la organización.

La Política de Seguridad de la Información es el documento que definirá todo lo aplicable y relacionado en términos de la seguridad de la información en la organización para su protección y prestación de servicios, adoptando para ello las medidas necesarias.

Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos.

3.1. Objetivos

Establecer un marco de trabajo para unificar la normativa aplicable, las funciones y responsabilidades de las personas, los procesos sobre la información, los servicios, su catalogación y tratamiento, la forma de organizarse, misión y alcance.

3.2. Documento

Se muestra una posible plantilla a rellenar con los datos de la organización en el Anexo I:

3.3. Recursos adicionales.

El CCN ha elaborado una guía STIC 805 sobre la política de seguridad que cumple con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, esta guía puede consultarse como ampliación a lo visto en el siguiente enlace:

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

4. Información que se maneja y valoración

El siguiente paso será valorar la información, esta valoración junto con la valoración de los servicios del siguiente apartado, son clave en el proceso.

4.1. Objetivo.

Se deberá de categorizar el tipo de información manejada, indicando por cada elemento:

- Su nombre, que la identifica unívocamente.
- Su responsable, que establece sus requisitos de seguridad.
- Otras características que se consideren relevantes a efectos operacionales, de asociación de vulnerabilidades, de estimación de riesgos o de auditoría.

4.2. Procedimiento.

Se establecerá el nivel de seguridad de cada elemento en dimensiones o aspectos a tener en cuenta para cada uno de los tipos de información.

Las dimensiones a tener en cuenta son confidencialidad, integridad, autenticidad y trazabilidad, existe una quinta que es la disponibilidad, pero está reservada normalmente a la categorización de los servicios.

El trabajo a realizar consistirá en valorar la afección del tipo de datos ante un incidente de seguridad en distintos niveles (nivel bajo, medio o alto) para cada tipo de datos y cada una de las dimensiones.

4.3. Recursos adicionales

El CCN ofrece una guía que indica las directrices principales para su valoración en el siguiente enlace:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf

5. Servicios que se prestan y valoración

El siguiente paso será valorar los servicios que ofrece la organización.

5.1. Objetivo.

El objetivo es la categorización de igual manera que en el caso de los activos de tipo información, pero en este caso tendremos en cuenta los servicios.

5.2. Procedimiento.

En este caso se trabajará con una nueva dimensión llamada disponibilidad, se evaluarán cada uno de los servicios bajo la perspectiva de un incidente de seguridad, se establecerán de igual manera nivel bajo, medio o alto en función del impacto en la disponibilidad del servicio.

5.3. Recursos adicionales

De igual manera que en el caso anterior, el CCN ofrece una guía que indica las directrices principales para su valoración en el siguiente enlace:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf

6. Datos de carácter personal

Se entenderá como dato personal a cualquier información sobre una persona física identificada o identificable y será considerada persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

6.1. RGPD vs ENS.

El 25 de Mayo de 2018 entra en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como la normativa

nacional que en su momento complemente lo dispuesto en dicha norma europea y por el que se deroga la Directiva 95/46/CE.

En la presente guía únicamente se tendrá en cuenta el tratamiento realizado por el ENS, no siendo el RGPD objeto de análisis, no obstante, en el Documento de Seguridad se deberá de indicar que el tratamiento de los datos de carácter personal se ajustará al Reglamento General de Protección de Datos (RGPD).

7. Categoría del sistema

Una vez tenemos categorizados los servicios y la información, será necesario categorizar el sistema de información.

7.1. Objetivo.

De forma muy simplificada, el objetivo es categorizar toda la información analizada y valorada para dar un nivel global al sistema.

7.2. Procedimiento.

El procedimiento para establecer una referencia con la que trabajar en lo sucesivo será elegir el mayor nivel de los obtenidos en cada uno de los activos del tipo información para cada una de las dimensiones (confidencialidad, integridad, autenticidad y trazabilidad), una vez obtenido el mayor nivel, cogeremos el mayor nivel de nuevo de entre las dimensiones.

Por el lado de los servicios tomaremos el mayor nivel de entre las dimensiones (la mayoría de casos solo habrá sido evaluada la dimensión disponibilidad).

Una vez contamos con los niveles máximos respecto de la Información y servicios, nos quedaremos con el mayor nivel de ellos, siendo esta la valoración del sistema.

7.3. Recursos adicionales

Como en casos anteriores, si se requiere información adicional, el CCN nos ofrece una guía del siguiente enlace:

https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/803-Valoracion_en_el_ENS/803_ENS-valoracion_ene-11.pdf

8. Análisis de riesgos

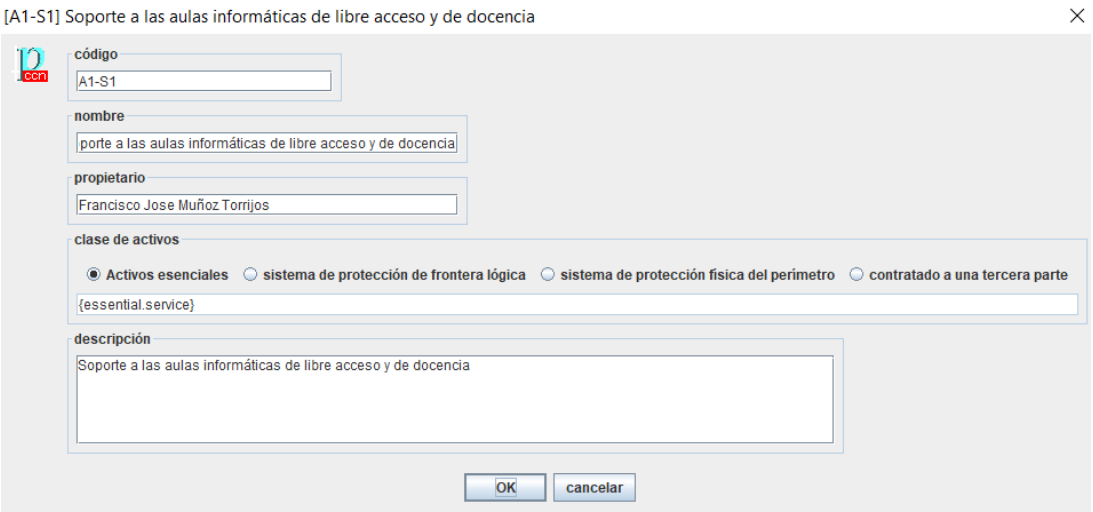
Con el objeto de mejorar la seguridad, se debe de conocer los riesgos a los que se expone el sistema de información, para ello, será necesaria la realización de un análisis de riesgos que ponga de manifiesto el estado actual y las insuficiencias del sistema.

8.1. Procedimiento.

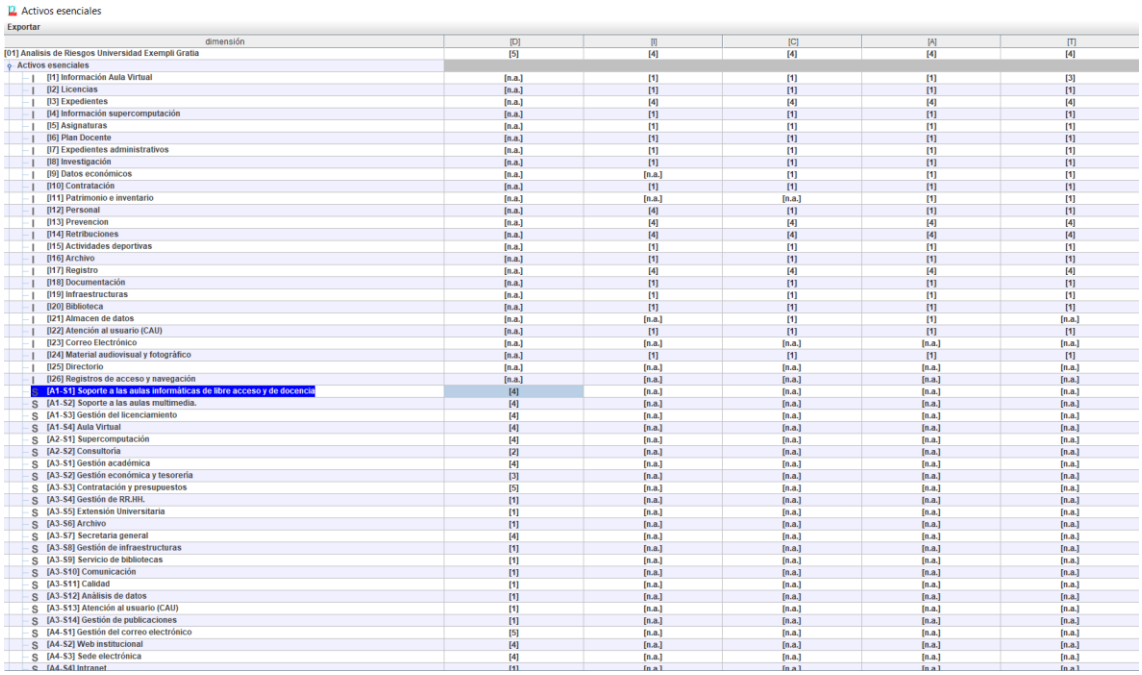
Para realizar el análisis de riesgo será utilizada la metodología Magerit v3, que será utilizada por la herramienta PILAR disponible en la Web del CCN-CERT para las AA.PP.

La herramienta permite realizar el análisis de riesgos introduciendo las valoraciones obtenidas en los apartados anteriores respecto de información y servicios.

Se muestran algunas capturas de pantalla representativas del proceso.



Definición de un servicio en PILAR



Activos esenciales

Exportar

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

Valoraciones de la información y servicios trasladadas a la herramienta PILAR

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

Resultado Análisis de Riesgos en herramienta PILAR

reco...		control	dud...	aplica	com...	current	target	PILAR
		[27002:2013] Código de prácticas para los controles de seguridad de la información						L2-L5
2		[5] Políticas de seguridad de la información						L2
2		[5.1] Directrices de gestión de la seguridad de la información						L2
2		[5.1.1] Políticas para la seguridad de la información						L2
2		[G.3.3] Normas de seguridad						L2
2		[5.1.2] Revisión de las políticas para la seguridad de la información						L2
2		[G.3.3.6] Se revisan regularmente						L2
7		[6] Organización de la seguridad de la información						L2-L4
5		[7] Seguridad relativa a los recursos humanos						L3 (L2-L3)
6		[8] Gestión de activos						L2-L4
7		[9] Control de acceso						L2-L4
8		[10] Criptografía						L3-L5 (L2...
6		[11] Seguridad física y del entorno						L2-L4
8		[12] Seguridad de las operaciones						L2-L5
8		[13] Seguridad de las comunicaciones						L3-L5 (L2...
5		[14] Adquisición, desarrollo y mantenimiento de los sistemas de información						L2-L3
5		[15] Relación con proveedores						L3 (L2-L3)
4		[16] Gestión de incidentes de seguridad de la información						L3 (L2-L3)
5		[17] Aspectos de seguridad de la información para la gestión de la continuidad del negocio						L3 (L2-L3)
4		[18] Cumplimiento						L2-L3

Medidas de seguridad aplicables a Exempli Gratia

8.2. Recursos de la herramienta PILAR

Acceso a la descarga de la herramienta PILAR:

https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar.html

Manual de usuario de la herramienta PILAR:

https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/400-guias-generales/2133-ccn-stic-470-h1-manual-de-la-herramienta-de-analisis-de-riesgos-pilar-6-2/file.html

9. Declaración de aplicabilidad

Se deberá de preparar y aprobar una declaración de aplicabilidad de las 75 medidas del Anexo II del ENS. El objetivo será valorar en cada medida si aplica o no aplica y como será implementada.

9.1. Procedimiento.

En el anexo II se muestra la plantilla que puede ser utilizada en el proceso.

10. Insuficiencias del sistema (gap analysis)

Consiste en estudiar la situación real en la organización de cada una de las medidas de seguridad que determina el Anexo II del ENS (estado ideal vs situación actual). Este informe deberá de ser aprobado por los Responsables de la Información y de los Servicios. Debe recordarse que dichas medidas vendrán determinadas por la categorización de los sistemas realizado previamente.

10.1. Procedimiento.

El procedimiento pasa por adecuar a la organización la plantilla presentada en el Anexo III.

11. Plan de mejora de la seguridad.

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

11.1. Procedimiento.

Adecuar a la organización la plantilla genérica del Anexo IV.

12. Conformidad con el ENS.

Se deberá de publicar un documento que informe del cumplimiento de la organización con el ENS.

12.1. Procedimiento.

Modificar el documento de referencia del Anexo V con los datos de la organización y publicarlo.

13. Herramienta INES

Finalizados los pasos anteriores se debe de notificar el estado de la organización mediante la herramienta INES proporcionada por el Centro Criptológico Nacional.

13.1. Procedimiento.

El responsable de seguridad debe de registrarse y estar autorizado para acceder al portal CCN-CERT (www.ccn-cert.cni.es), el portal es accesible solo para los usuarios registrados.

14. Auditorias

La auditoría es la encargada de la verificación de que los procesos son realizados correctamente.

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

En el caso de contar con una organización de tipo media o alta, se recomienda realizar la tarea a consultores externos especializados, evitando un posible conflicto de intereses. Una vez realizada la tarea los auditores realizaran un resumen del siguiente estilo:

RESULTADOS DE LA AUDITORIA DE SEGURIDAD DE LA "ORGANIZACION"

NO CONFORMIDAD	RECOMENDACION
NC.org.X	Creación de XXX para los procesos YYY.

Y finalizará con un resultado global favorable o desfavorable similar al siguiente:

Opinión del auditor:	**FAVORABLE CON SALVEDADES**

15. Anexo I. Plantilla política de seguridad

Se muestra la plantilla para rellenar con los datos de la organización.

POLITICA DE SEGURIDAD <EL ORGANISMO>

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día <día> de <mes> de <año> por <órgano que la aprueba>.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día <día> de <mes> de <año> por <órgano que lo aprobó>.

2. INTRODUCCIÓN

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

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

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

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

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. PREVENCIÓN

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

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

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

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

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

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de <el organismo> y a todos los miembros de la organización, sin excepciones.

4. MISIÓN

Describir los objetivos de servicio del organismo

5. MARCO NORMATIVO

Listar leyes, reglamentos y otra normativa, nacional o internacional, a la que el organismo este sujeto.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

La guía CCN-STIC 402 puede usarse como modelo.

El Comité de Seguridad TIC estará formado por <…>. Aquí aparecen cargos corporativos y designaciones de departamentos dentro del organismo cuando proceda.

El Secretario del Comité de Seguridad TIC será <…> y tendrá como funciones <…>.

El Comité de Seguridad TIC reportará a <…>.

El Comité de Seguridad TIC tendrá las siguientes funciones: <…>.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

La guía CCN-STIC 801 puede usarse como modelo, en particular concretando las funciones y responsabilidades del Responsable de Seguridad de la Información y su relación con el Comité de Seguridad TIC.

Cuando proceda, se detallará el nombramiento de Responsables Delegados de Seguridad y las funciones que les son delegadas.

Se detallarán igualmente las funciones de los Responsables de Sistemas.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por <órgano que no nombra> a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

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

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por <órgano que la aprueba> y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

<El organismo> trata datos de carácter personal. El <documento de seguridad>, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de <el organismo> se ajustarán al Reglamento General de Protección de Datos (RGPD) para el tratamiento de los datos de carácter personal recogidos en el mencionado <Documento de Seguridad>.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

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

necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de <el organismo> en diferentes materias:

- *Listar referencias a otras políticas en materia de seguridad.*

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet
URL
e impresa en
LOCALIZACIÓN

10. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de <el organismo> atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de <el organismo>, en particular a los de nueva incorporación.

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

11. TERCERAS PARTES

Cuando <el organismo> preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y

coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando <el organismo> utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

16. Anexo II. Declaración de aplicabilidad

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

- Nombre del declarante: <Organización>
- Dirección postal: <Dirección de la organización>
- Dirección electrónica: <Dirección electrónica>

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

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

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

Situación y aplicabilidad de las medidas de seguridad durante el año <actual>.

Marco Organizativo. Org.1	**Proceso de autorización**
Medida de seguridad requerido	XXX
Aplicabilidad de la medida de seguridad	Aplica/No aplica
Motivación de la medida de seguridad	XXX
Implementación de la medida de seguridad	XXX

En <Dirección>, a <Fecha>

Persona que lo firma:	<Persona responsable>
Cargo que ostenta:	Responsable de la seguridad
Firma:	……..

17. Anexo III. Informe de insuficiencias.

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

- Nombre del declarante: <Organización>
- Dirección postal: <Dirección de la organización>
- Dirección electrónica: <Dirección electrónica>

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

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

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

Durante el presente año <Año en curso> han sido detectadas las siguientes insuficiencias:

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

Las insuficiencias no corregidas serán consideradas “riesgo asumible”.

En <Dirección>, a <Fecha>

Responsable de información: <Persona responsable>
Firma: ……..

Responsable del servicio: <Persona responsable>
Firma: ……..

18. Anexo IV. Plan de mejora de la seguridad.

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

- Nombre del declarante: <Organización>
- Dirección postal: <Dirección de la organización>
- Dirección electrónica: <Dirección electrónica>

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

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

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

Durante el presente año <Año en curso> se proponen las siguientes actuaciones con el objetivo de mejorar la seguridad de los sistemas de información:

Mejora 1	**XXX**
Medida de seguridad	XXX
Motivación de la medida de seguridad	XXX
Implementación de la medida de seguridad	2018
Estado	Planificada XXX
Responsable y desarrollo	Definir responsable del proceso y tarea a realizar.
Plazos	3 meses
Recursos	Personal de los servicios afectados

En <Dirección>, a <Fecha>

Responsable de información: <Persona responsable>
Firma: ……..

19. Anexo V. Conformidad con el ENS.

Declaración de conformidad con el Esquema Nacional de Seguridad

- Nombre del declarante: <Organización>
- Dirección postal: <Dirección de la organización>
- Dirección electrónica: <Dirección electrónica>

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

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

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

En <Dirección>, a <Fecha>

Persona que lo firma:	<Persona responsable>
Cargo que ostenta:	Responsable de la seguridad
Firma:	……..