Universitat Oberta de Catalunya

uoc.edu

Desarrollo de procedimientos para cumplimiento de controles aplicables para sistemas de información categorizados como nivel medio según ENS y desarrollo de instrucciones para aplicación de esos procedimientos empleando las herramientas técnicas e instrucciones que proporciona el CCN

Nombre Estudiante:	**Raúl Rodrigo Fernández**
Plan de Estudios:	Máster Universitario en Ciberseguridad y Privacidad
Área del trabajo final	Seguridad empresarial
Nombre Consultor	**Iñaki Moreno Fernández**
Nombre Profesor RA	**Carles Garrigues Olivella**
Fecha Entrega	06/22

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo de procedimientos para cumplimiento de controles aplicables para sistemas de información categorizados como nivel medio según ENS y desarrollo de instrucciones para aplicación de esos procedimientos empleando las herramientas técnicas e instrucciones que proporciona el CCN*
Nombre del autor:	*Raúl Rodrigo Fernández*
Nombre del consultor/a:	*Iñaki Moreno Fernández*
Nombre del PRA:	*Carles Garrigues Olivella*
Fecha de entrega (mm/aaaa):	06/2022
Titulación:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad empresarial*
Idioma del trabajo:	Español
Palabras clave	*ENS, CCN, SGSI*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

El presente trabajo tiene como finalidad plasmar el Plan de Adecuación de una Organización cuyo sistema de información a adecuar está categorizado en nivel medio. Para ello, se contextualiza la normativa aplicable y los cambios más actuales, se continúa realizando una Plan de Implantación del Esquema Nacional de Seguridad presentando como Anexos a este documento todos los entregables que recibiría dicha Organización si se tratase de un caso real (desde la recogida de datos, análisis de riesgos, declaración de aplicabilidad, hasta la normativa redactada que posteriormente tendría que implantar dicho organismo).

Como metodología para llevar a cabo este trabajo, se ha escogido un método práctico de exposición por el cual se narra la teoría y se expone a modo de ejemplo cada documento en formato Anexo.

Abstract (in English, 250 words or less):

The purpose of this work is to capture the Adaptation Plan of an Organization whose information system to be adapted is categorized at the medium level. To that end, the applicable regulations and the most current changes are contextualized, a Plan for the Implementation of the National Security Scheme continues to be carried out, presenting as Annexes to this document all the deliverables that said Organization would receive if it is a real case (from the collection of data, risk analysis, declaration of applicability, up to the drafted regulations that said body will have to implement later).

As a methodology to carry out this work, a practical exposition method has been chosen by which the theory is narrated and each document is presented as an example in Annex format.

Índice

Lista de figuras

1. Introducción

1.1. Contexto y justificación del Trabajo

En años recientes la tecnología ha presentado grandes avances que han facilitado la creación del ciberespacio en multitud de disciplinas. Estos avances han ido ligados al desarrollo de la TIC permitiendo en la actualidad el teletrabajo, la compra online o realizar trámites con la Administración Pública de manera electrónica. Estos avances, no habrían calado en la población mundial si no fueran ligados a unas garantías de seguridad que generen confianza en los cinco pilares básicos de la ciberseguridad, que son: confidencialidad, disponibilidad, integridad, trazabilidad y autenticidad.

En España, la Administración Pública inicio en 2007 el proceso de digitalización de la Administración dando lugar a la Administración Electrónica. El documento que reguló esta creación es la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios, actualmente derogada, donde dentro de su contenido creaba el Esquema Nacional de Seguridad y le asignaba la responsabilidad de generar la normativa y las políticas de modo que se implementase una capa de seguridad que garantizase que los tramites se realizarán con seguridad y confianza.

Hasta este año, el Esquema Nacional de Seguridad estaba regulado principalmente por 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 (modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre y las leyes 39/2015 y 40/2015, de obligado cumplimiento para todo el sector público estatal, lo que significa que es de aplicación en la Administración General del Estado, Administraciones de las comunidades autónomas, Administraciones locales y en el sector público institucional. Durante el desarrollo de este trabajo se ha publicado el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que actualiza el modelo publicado en 2010 para adaptarlo a la nueva realidad y al incremento de las ciberamenzas tanto cuantitativa como cualitativamente. Su actualización constituye una de las medidas del paquete de actuaciones urgentes, acordado por el Gobierno, para reforzar de manera inmediata las capacidades de defensa frente a las

ciberamenazas del sector público y de las entidades privadas que colaboren con este en la prestación de servicios o en el suministro de tecnología. Se eliminan algunas medidas y se añaden otras, como, por ejemplo, las relativas a la protección de los servicios en la nube (hasta ahora, no regulado).

1.2. Objetivos del Trabajo

Este trabajo tiene como objetivo implementar un Sistema de Seguridad de la Información dentro de un órgano de la Administración Pública a través del Esquema Nacional de Seguridad. Como se detalla el título, se ha seleccionado un perfil de seguridad de la información de nivel medio.

Concretamente, se llevarán a cabo las siguientes acciones para conseguir el objetivo fijado:

- Análisis de requerimientos del ENS.
- Análisis de requerimientos legales asociados.
- Análisis y aplicación de controles.
- Desarrollo de procedimientos para la implantación
- Desarrollo de instrucciones para desarrollar los procedimientos.

1.3. Enfoque y método seguido

Dentro de los Sistemas de Gestión de Seguridad de la Información, la normativa más globalizada es la familia 27000 de las normas ISO. Como elementos complementarios, se aplican también la norma ISO 22301 de gestión de la continuidad de negocio y la norma ISO 31000 de Gestión de riesgos, principios y guías.

El Centro Criptológico Nacional, dentro de sus funciones, desarrolla y publica guías entre las que se encuentra la serie CCN-STIC-800 donde se establecen las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad. Estas guías se basan en las familias ISO, pero adaptadas a las necesidades de la Administración Pública.

Por ello, este trabajo se apoyará tanto en las guías CCN-STIC-800 como en las herramientas de ciberseguridad desarrolladas por el CCN con el objetivo de apoyar al ENS.

Dentro del catálogo de las guías CCN-STIC-800, son de especial relevancia para este trabajo las siguientes:

- CCN-STIC-800 Glosario de términos y abreviaturas del ENS
- CCN-STIC-802 Auditoría del ENS
- CCN-STIC-803 Valoración de Sistemas en el ENS
- CCN-STIC-804 ENS. Guía de implantación
- CCN-STIC-806 Plan de Adecuación al ENS
- CCN-STIC-808 Verificación del cumplimiento del ENS
- CCN-STIC-818 Herramientas de Seguridad en el ENS
- CCN-STIC-821 Normas de Seguridad en el ENS
- CCN-STIC-822 Procedimientos de Seguridad
- CCN-STIC-883 Implantación del ENS para Entidades Locales

Dentro del catálogo de herramientas de ciberseguridad, son de especial relevancia para este trabajo las siguientes:

- INES: Informe de Estado de Seguridad en el ENS
- PILAR: Análisis y Gestión de Riesgos
- AMPARO: Implantación de seguridad y conformidad del ENS

Debido a la publicación del RD 311/2022 de 3 de mayo durante el desarrollo de este trabajo, se harán referencias al nuevo ENS, pero las guias publicadas por el CCN y las Instrucciones Técnicas están basadas en el RD 3/2010 de 8 de enero. El corto periodo de tiempo entre la publicación del RD a la entrega de este trabajo ha hecho que la documentación que emana del RD no haya sido actualizada aún. Tras el estudio de los cambios implementa el nuevo ENS y la lectura de las guias y normativas, se ha decidio mantener la referencia a estas ya que siguien siendo de validez prácticamente en su totalidad.

1.4. Planificación del Trabajo

Cod	Nombre de tarea	Duración	Comienzo	Fin
1	**Planificación**	**10 días**	**mie 16/02/22**	**mar 01/03/22**
1.1	Contexto y justificación	3 días	mie 16/02/22	vie 18/02/22
1.2	Objetivos del Trabajo	2 días	sáb 19/02/22	lun 21/02/22
1.3	Enfoque y método seguido	1 día	mar 22/02/22	mar 22/02/22
1.4	Planificación del Trabajo	4 días	mie 23/02/22	sáb 26/02/22
1.5	Breve sumario de productos obtenidos	1 día	dom 27/02/22	dom 27/02/22
1.6	Breve descripción de los otros capítulos de la memoria	1 día	lun 28/02/22	lun 28/02/22
1.7	Entrega PEC1	1 día	mar 01/03/22	mar 01/03/22
2	**Entrega de seguimiento: 1**	**20 días**	**mie 02/03/22**	**mar 29/03/22**
2.1	Análisis Requerimientos ENS	13 días	jue 03/03/22	sáb 19/03/22
2.2	Análisis Requerimientos Legales	5 días	dom 20/03/22	jue 24/03/22
	Entrega PEC2	1 día	mar 29/03/22	mar 29/03/22
3	**Entrega de seguimiento: 2**	**20 días**	**mie 30/03/22**	**mar 26/04/22**
3.1	Implantación de medidas técnicas y organizativas del ENS	12 días	mie 30/03/22	jue 14/04/22
3.2	Redacción de las fases de adecuación al ENS	6 días	vie 15/04/22	vie 22/04/22
	Entrega PEC3	1 día	mar 26/04/22	mar 26/04/22
4	**PEC4: Memoria Final**	**25 días**	**mie 27/04/22**	**mar 31/05/22**
4.1	Desarrollo de procedimientos	12 días	mie 27/04/22	jue 12/05/22
4.2	Desarrollo de Instrucciones	11 días	vie 13/05/22	vie 27/05/22
	Elaborar conclusiones	2 días	sáb 28/05/22	dom 29/05/22
	Revisar Glosario	24 días	lun 30/05/22	jue 30/06/22
	Revisar Biografía	24 días	lun 30/05/22	jue 30/06/22

	Revisar Anexos	22 días	lun 30/05/22	mar 28/06/22
	Entrega PEC 4: Memoria Final	1 día	mar 31/05/22	mar 31/05/22
5	**PEC 5: Presentación**	**5 días**	**mie 01/06/22**	**mar 07/06/22**
6	**PEC 6: Defensa TFM**	**1 día**	**lun 20/06/22**	**lun 20/06/22**

1.5. Breve sumario de productos obtenidos

La relación de productos obtenidos de este trabajo será una guía de aplicación del ENS para un sistema de categoría media en el que se detallarán los procedimientos e instrucciones para su implementación.

1.6. Breve descripción de los otros capítulos de la memoria

El documento está organizado de la siguiente manera:

- Capítulo 1: Se introduce el trabajo exponiendo los motivos por los que se realiza, la normativa aplicable, la metodología llevada a cabo y la planificación del mismo.
- Capítulo 2: A través de la familia de guias CCN-STIC-800 se analizarán los requerimientos que impone a los sistemas de clasificación media, incluidos los requerimientos legales asociados.
- Capítulo 3: Se expondrán las conclusiones de este trabajo.
- Capítulo 4: Se provee de un Glosario
- Capítulo 5: Se referencia la Biografia
- Anexos: Se desarrollará la documentación en relación con lo expuesto en el Capítulo 2.

2. Análisis

2.1 Requerimientos ENS

El objetivo que se persigue por la Administración Pública es brindar a los ciudadanos servicios que sean accesibles por vía electrónica en condiciones tan estables y seguras como las que encuentran cuando acuden en persona a las oficinas públicas. La información y los servicios que se prestan siguen expuestos a amenazas y peligros causados por actividades maliciosas o ilegales, errores o fallos, así como accidentes y catástrofes. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos introduce los principios de estabilidad de la administración electrónica y establece, en su artículo 42, el Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS), establece la política de seguridad de la información a aplicar y se basa en un conjunto de principios básicos y en los requisitos mínimos en relación con la categoría del sistema. El fin de este Real Decreto es garantizar la introducción, la integridad, la accesibilidad, la veracidad, la confidencialidad, la trazabilidad y la conservación de los datos, la información y los servicios utilizados en los medios electrónicos en las interacciones del ciudadano con las siguientes entidades:

- La Administración General del Estado.
- Las Administraciones de las comunidades autónomas.
- Las entidades que integran la Administración local.
- El sector público institucional

Para ello, se definen como objetivos principales:

- Crear las condiciones básicas de confianza en el uso de los medios electrónicos, permitiendo a los ciudadanos y a las autoridades públicas ejercer sus derechos y cumplir sus obligaciones a través de ellos, adoptando medidas para garantizar la estabilidad de la información y los servicios electrónicos.

- Establecer una política de estabilidad para el uso de medios electrónicos, en el marco de la Ley 11/2007, que incluya principios y requisitos mínimos para el correcto almacenamiento de la información.
- Establecer recursos estándar para la gestión de las actividades de la administración pública en el ámbito de la estabilidad informática.
- Proporcionar un lenguaje común para facilitar las relaciones entre las administraciones y comunicar a la industria los requisitos de estabilidad de la información.
- Garantizar un proceso de estabilidad homogéneo para facilitar la cooperación en la prestación de servicios de administración electrónica en la que participen diferentes organizaciones.

Siguiendo el objetivo perseguido por este trabajo, a continuación, se expondrá un Plan de Adecuación al ENS de un órgano de la Administración pública, en el cual se reflejará paso por paso las acciones a llevar a cabo para proteger el sistema de dicho organismo.

Con su elaboración se identificarán, por un lado, las personas u órganos responsables de que la implantación del ENS se lleve a cabo en la entidad y, por otro, las medidas de seguridad que será necesario implantar, con la definición de hitos y la identificación de los recursos necesarios para llevarlas a cabo.

Hay que destacar, que el Responsable de Seguridad es la figura dentro del órgano de la Administración Pública, encargado de llevar a cabo la elaboración del Plan de Adecuación al ENS.

2.1.1 Definir el Alcance del Sistema de Información

En primer lugar, el órgano de la Administración Pública que vaya a ser objeto de adecuación, deberá definir el alcance de su sistema, es decir, tendrá que identificarse hasta donde llegarán las medidas que se van a aplicar, qué abarcará y que no y, sobre todo, se deberá establecer el límite dentro del órgano de lo que encauzará la adecuación al ENS.

La definición del alcance se reflejará en el documento de la Política de Seguridad. La Política de Seguridad es un documento de alto nivel, mediante el cual la entidad define su compromiso respecto a la seguridad de la información

y la de los servicios prestados. En esta Política se describirán los mecanismos implementados para la gestión continuada de la seguridad y se establecerán los responsables de velar por su cumplimiento.

El ENS se refiere en varios puntos a la Política de Seguridad:

- ENS. Artículo 11. Requisitos mínimos de seguridad:

  1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. [1]

  - ENS. Artículo 12. Organización e implantación del proceso de seguridad:

  La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa. [1]

- ENS. Disposición transitoria. Adecuación de sistemas.

  3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo. [1]

- ENS. Anexo II Medidas de Seguridad Marco organizativo [org] Política de seguridad [org.1]: *La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el Artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:*

  a) Los objetivos o misión de la organización.

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

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

d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización. [1]

Las entidades públicas podrán elaborar su propia Política de Seguridad o bien acogerse a la Política de la entidad de orden superior, en el caso de organismos dependientes, para aquellos servicios que son proporcionados por estas. En este caso, el Responsable de Seguridad y el Responsable del Sistema podrán ser los designados por estas. Por el contrario, los Responsables de los Servicios y los Responsables de la Información, serán designados en el Organismo en concreto.

La 'Guía CCN-STIC 806 Política de Seguridad de la Información' ofrece un listado de contenidos mínimos que deberían verse reflejados en este documento:

1. Misión u objetivos del organismo
2. Marco normativo
3. Organización de seguridad
    - Definición de comités (Comité TIC que aprobará todas las decisiones tomadas respecto al ENS) y roles unipersonales
    - Funciones
    - Responsabilidades
    - Mecanismos de coordinación
    - Procedimientos de designación de personas
4. Concienciación y formación
5. Postura para la gestión de riesgos
    - Plan de análisis
    - Criterios de evaluación de riesgos
    - Directrices de tratamiento
    - Proceso de aceptación del riesgo residual
6. Proceso de revisión de la política de seguridad

Para que este trabajo sea más ilustrativo y didáctico, se van a anexar los documentos que la propia adecuación que se está analizando vaya previendo. Por ello, el primer documento es un ejemplo de Política de Seguridad (Anexo I).

2.1.2 Categorización Sistemas de Información

El siguiente paso para comenzar la adecuación es identificar los servicios prestados por la entidad sustentados en los sistemas de información que habrán de ser conformes con el ENS.

Para identificar dichos servicios. la cumplimentación detallada del modelo de Ficha de Servicios que se incluye en el Anexo II de este documento servirá para disponer, ordenadamente, de los datos esenciales de cada servicio prestado, incluyendo los tipos de información tratados y los sistemas de información sobre los que se prestan, así como una valoración inicial del nivel de seguridad de cada una de las dimensiones de seguridad aplicables al servicio/información de que se trate.

La decisión sobre la categoría del sistema se basará en una evaluación del impacto en la organización de un incidente que afecte a la continuidad de la información o los servicios. Se considera que un servicio está afectado si no se cumplen sus objetivos, no se protegen los bienes bajo su responsabilidad, no se cumplen las funciones cotidianas del servicio o no se respetan las leyes aplicables y los derechos de las personas que son usuarias de esa información.

Para identificar el impacto en la organización de un suceso que perturbe la estabilidad de los sistemas y definir la categoría del suceso, deben considerarse las siguientes dimensiones de seguridad:

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

Una o varias variables de la información o del servicio pueden estar comprometidas. A efectos de definir la categoría del sistema de información, se definen 3 categorías: BAJO, MEDIO y ALTO:

- Un sistema de información pertenece al nivel ALTO si alguna de sus variables de seguridad alcanza el nivel ALTO.
- Un sistema de información entra en la categoría MEDIA si alguna de sus medidas de seguridad alcanza el nivel MEDIO y ninguna alcanza el nivel ALTO.
- Un sistema de información pertenece a la categoría BAJA si ninguna de sus variables de seguridad alcanza el nivel ALTO ni MEDIO.

Sobre este método pueden existir variaciones, como la que establece la Federación Española de Municipios y Provincias (en adelante, FEMP) en la normativa de aplicación en ayuntamientos, en la que se definen criterios de valoración relativa para evitar disponer de sistemas de categoría ALTA de forma generalizada, ya que el nivel de exigencia es muy algo y está pensado para sistemas críticos.

	DIMENSIONES				
	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad
SISTEMA	[D]	[I]	[C]	[A]	[T]
Información A	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
Información B	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
… …	…	…	…	…	…
Servicio X	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
Servicio Y	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto	Bajo Medio Alto
… …	…	…	…	…	…

La categoría de aplicación de este trabajo será la MEDIA y según el ENS su criticidad implica que, a raíz del incidente de seguridad, se crea un perjuicio grave a las funciones de la organización, a sus activos o a las personas afectadas.

Se entenderá por perjuicio grave:

- La reducción suficiente de la capacidad de la organización para atender eficientemente a sus compromisos principales, aunque estas sigan realizándose.
- Que los activos de la organización soportaran un daño significativo.
- El incumplimiento material de alguna ley o normativa, o el incumplimiento formal que no tenga carácter de enmendable.
- Causar un perjuicio significativo a algún individuo, de difícil reparación.
- Otros de naturaleza análoga.

La categorización de los sistemas se plasmará en un documento que deberá ser aprobado por el Responsable del Sistema y, para continuar con el ejemplo del Plan de Adecuación, en el Anexo III se presenta una categorización a nivel medio.

2.1.3 Declaración de Aplicabilidad

La Declaración de Aplicabilidad es el documento en el que se formaliza la relación de medidas de seguridad que resultan de aplicación al sistema de información de que se trate, conforme a su categoría, y que se encuentran recogidas en el Anexo II del ENS, que lo regula.

El documento formalizado de Declaración de Aplicabilidad será esencial para la elaboración del plan de adecuación y la posterior implementación de las medidas contempladas, y podrá ser analizado por la entidad certificadora y empleado como documento de apoyo durante el proceso de auditoría para la validación del cumplimiento del ENS.

Una vez categorizado el sistema, corresponde llevar a cabo la Declaración de Aplicabilidad.

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos en el Esquema Nacional de Seguridad, se debe aplicar un conjunto

de medidas de seguridad, que serán proporcionales a las dimensiones de seguridad relevantes en el sistema a proteger y su categoría.

El Anexo II ENS recoge la correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad aplicables. En concreto, por cada medida de seguridad se indica:

- Si se determina su aplicación en función de la categoría del sistema o en función del nivel de seguridad asignado a una o varias dimensiones de seguridad.
- Si es de aplicación o no para un determinado nivel de seguridad. En caso de que la aplicación de la medida no sea necesaria para obtener la adecuación con el ENS, en la tabla del Anexo II se recoge el valor “n.a.”.
- Por otro lado, en caso de sí ser necesaria su aplicación, aparecerá alguno de los siguientes valores: o “aplica”: indica que una medida de seguridad debe ser aplicada a una o varias dimensiones de seguridad en algún nivel.
    - “=”: indica que las exigencias de un nivel son iguales a los del nivel inferior.
    - “+” o ”++”: indica que el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad.

De esta forma, la aplicación o no de las 75 medidas que recoge el Anexo II del ENS tendrían la siguiente distribución:

Dimensiones				**MEDIDAS DE SEGURIDAD**	
Afectadas	**B**	**M**	**A**		
				org	**Marco organizativo**
categoría	aplica	=	=	[org.1]	Política de seguridad
categoría	aplica	=	=	[org.2]	Normativa de seguridad
categoría	aplica	=	=	[org.3]	Procedimientos de seguridad
categoría	aplica	=	=	[org.4]	Proceso de autorización
				op	**Marco operacional**

				[op.pl]	Planificación
categoría	aplica	+	++	[op.pl.1]	Análisis de riesgos
categoría	aplica	+	++	[op.pl.2]	Arquitectura de seguridad
categoría	aplica	=	=	[op.pl.3]	Adquisición de nuevos componentes
D	n.a.	aplica	=	[op.pl.4]	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	[op.pl.5]	Componentes certificados
				[op.acc]	Control de acceso
A T	aplica	=	=	[op.acc.1]	Identificación
I C A T	aplica	=	=	[op.acc.2]	Requisitos de acceso
I C A T	n.a.	aplica	=	[op.acc.3]	Segregación de funciones y tareas
I C A T	aplica	=	=	[op.acc.4]	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	[op.acc.5]	Mecanismo de autenticación
I C A T	aplica	+	++	[op.acc.6]	Acceso local (local logon)
I C A T	aplica	+	=	[op.acc.7]	Acceso remoto (remote login)
				[op.exp]	Explotación
categoría	aplica	=	=	[op.exp.1]	Inventario de activos
categoría	aplica	=	=	[op.exp.2]	Configuración de seguridad
categoría	n.a.	aplica	=	[op.exp.3]	Gestión de la configuración
categoría	aplica	=	=	[op.exp.4]	Mantenimiento
categoría	n.a.	aplica	=	[op.exp.5]	Gestión de cambios
categoría	aplica	=	=	[op.exp.6]	Protección frente a código dañino
categoría	n.a.	aplica	=	[op.exp.7]	Gestión de incidentes
T	aplica	+	++	[op.exp.8]	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	[op.exp.9]	Registro de la gestión de incidentes

T	n.a.	n.a.	aplica	[op.exp.10]	Protección de los registros de actividad
categoría	aplica	+	=	[op.exp.11]	Protección de claves criptográficas
				[op.ext]	Servicios externos
categoría	n.a.	aplica	=	[op.ext.1]	Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	[op.ext.2]	Gestión diaria
D	n.a.	n.a.	aplica	[op.ext.9]	Medios alternativos
				[op.cont]	Continuidad del servicio
D	n.a.	aplica	=	[op.cont.1]	Análisis de impacto
D	n.a.	n.a.	aplica	[op.cont.2]	Plan de continuidad
D	n.a.	n.a.	aplica	[op.cont.3]	Pruebas periódicas
				[op.mon]	Monitorización del sistema
categoría	n.a.	aplica	=	[op.mon.1]	Detección de intrusión
categoría	aplica	+	++	[op.mon.2]	Sistema de métricas
				mp	**Medidas de protección**
				[mp.if]	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	[mp.if.1]	Áreas separadas y con control de acceso
categoría	aplica	=	=	[mp.if.2]	Identificación de las personas
categoría	aplica	=	=	[mp.if.3]	Acondicionamiento de los locales
D	aplica	+	=	[mp.if.4]	Energía eléctrica
D	aplica	=	=	[mp.if.5]	Protección frente a incendios
D	n.a.	aplica	=	[mp.if.6]	Protección frente a inundaciones
categoría	aplica	=	=	[mp.if.7]	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	[mp.if.9]	Instalaciones alternativas
				[mp.per]	Gestión del personal

categoría	n.a.	aplica	=	[mp.per.1]	Caracterización del puesto de trabajo
categoría	aplica	=	=	[mp.per.2]	Deberes y obligaciones
categoría	aplica	=	=	[mp.per.3]	Concienciación
categoría	aplica	=	=	[mp.per.4]	Formación
D	n.a.	n.a.	aplica	[mp.per.9]	Personal alternativo
				[mp.eq]	Protección de los equipos
categoría	aplica	+	=	[mp.eq.1]	Puesto de trabajo despejado
A	n.a.	aplica	+	[mp.eq.2]	Bloqueo de puesto de trabajo
categoría	aplica	=	+	[mp.eq.3]	Protección de equipos portátiles
D	n.a.	aplica	=	[mp.eq.9]	Medios alternativos
				[mp.com]	Protección de las comunicaciones
categoría	aplica	=	+	[mp.com.1]	Perímetro seguro
C	n.a.	aplica	+	[mp.com.2]	Protección de la confidencialidad
I A	aplica	+	++	[mp.com.3]	Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	[mp.com.4]	Segregación de redes
D	n.a.	n.a.	aplica	[mp.com.9]	Medios alternativos
				[mp.si]	Protección de los soportes de información
C	aplica	=	=	[mp.si.1]	Etiquetado
I C	n.a.	aplica	+	[mp.si.2]	Criptografía
categoría	aplica	=	=	[mp.si.3]	Custodia
categoría	aplica	=	=	[mp.si.4]	Transporte
C	aplica	+	=	[mp.si.5]	Borrado y destrucción
				[mp.sw]	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	[mp.sw.1]	Desarrollo

categoría	aplica	+	++	[mp.sw.2]	Aceptación y puesta en servicio
				[mp.info]	Protección de la información
categoría	aplica	=	=	[mp.info.1]	Datos de carácter personal
C	aplica	+	=	[mp.info.2]	Calificación de la información
C	n.a.	n.a.	aplica	[mp.info.3]	Cifrado
I A	aplica	+	++	[mp.info.4]	Firma electrónica
T	n.a.	n.a.	aplica	[mp.info.5]	Sellos de tiempo
C	aplica	=	=	[mp.info.6]	Limpieza de documentos
D	aplica	=	=	[mp.info.9]	Copias de seguridad *(backup)*
				[mp.s]	Protección de los servicios
categoría	aplica	=	=	[mp.s.1]	Protección del correo electrónico
categoría	aplica	=	+	[mp.s.2]	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	[mp.s.8]	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	[mp.s.9]	Medios alternativos

Hecho lo anterior, la categoría de seguridad del sistema de información será la resultante de la valoración de los servicios analizados y de la información tratada por cada uno de ellos. En base a ello, podremos obtener una Declaración de Aplicabilidad (relación de medidas aplicables del Anexo II del ENS) provisional.

2.1.4 Análisis de Riesgos

El análisis de riesgos se desarrollará conforme a lo dispuesto en el artículo 13 y Anexo II (sección [op.pl.1]) del ENS, para la categoría establecida para el sistema.

Para su realización, el CCN se recomienda utilizar la metodología MAGERIT, metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, que parte de la base de que el uso de las tecnologías de la información da lugar a ciertos riesgos que deben minimizarse mediante la adopción de medidas técnicas y organizativas de seguridad. Con

MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA (ENISA es la agencia de ciberseguridad de la Unión Europea). Por otro lado, como se verá más adelante, PILAR es la aplicación, que sirve de herramienta para aplicar la metodología MAGERIT (los organismos de la administración pública española pueden solicitar una licencia libre de cargos al CCN).

La metodología MAGERIT, documentalmente se desarrolla en base a tres libros:

Libro I – Método

- Describe cómo aplicar la metodología

Libro II - Catálogo de Elementos

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas que considerar para proteger sistemas de información

Libro III - Guía de Técnicas

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

MAGERIT divide el proceso de gestión de riesgos en dos grupos de actividades:

a) Análisis de riesgo: “que permite determinar qué tiene el Organismo y estimar lo que podría pasar”.

b) Tratamiento de los riesgos: selección de los controles que modifican el riesgo, hasta el nivel de riesgo residual que la organización decide asumir

Por lo que respecta al análisis de riesgos, la metodología MAGERIT establece una secuencia de actividades que deben llevarse a cabo:

1. Determinar e identificar los activos relevantes para el Organismo, es decir los elementos del sistema de información que permiten a la organización lograr sus objetivos
2. Determinar a qué amenazas están expuestos los activos y que por la tanto pueden perjudicar la organización
3. Determinar qué salvaguardas hay previstas (es decir, identificar los controles/medidas de protección implementadas) y su eficacia en términos de riesgo
4. Estimar el impacto, definido como el daño sobre el activo, como consecuencia de la amenaza
5. Estimar el riesgo, "expectativa de materialización" de la amenaza (probabilidad)

El siguiente esquema representa gráficamente la actividad de análisis de riesgos:

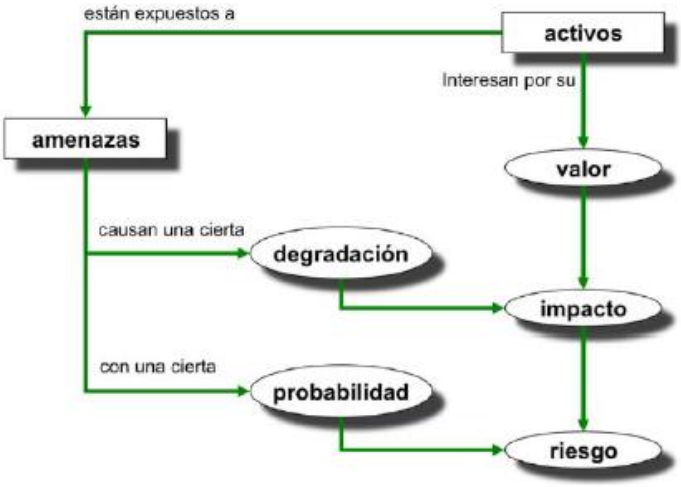


Ilustración 1 Método Análisis de Riesgos

Un aspecto importante de cualquier metodología de gestión de riesgos para la seguridad de la información es la identificación de los activos que quieren protegerse

de las potenciales amenazas que puedan afectarles. En este sentido MAGERIT prevé dos tipos de activos.

Por un lado, los denominados activos esenciales, constituidos por:

- La información que se maneja
- Los servicios que se prestan

Y, por otro, los activos de soporte en los que se apoyan los activos esenciales:

- Las aplicaciones informáticas *(software)* que permiten manejar los datos.
- Los equipos informáticos *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Por lo que respecta las amenazas, MAGERIT aporta un conjunto de amenazas comunes, que pueden afectar a los activos, y las clasifica según lo reflejado en la siguiente tabla (el número entre paréntesis indica el número de amenazas de cada tipo que propone MAGERIT):

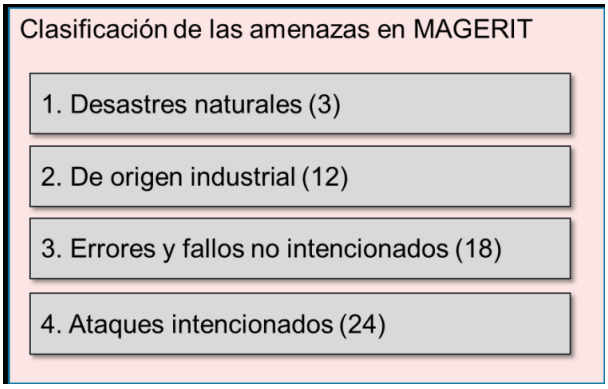
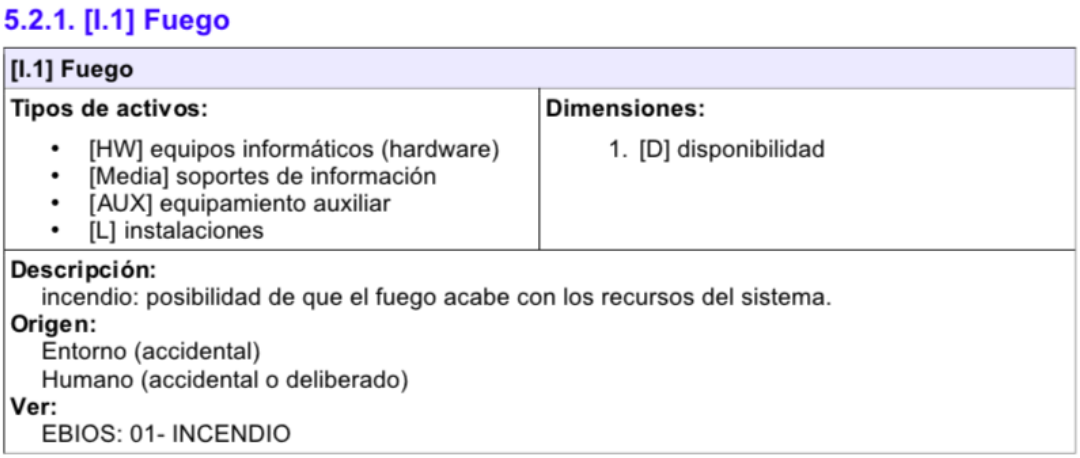


Ilustración 2 Amenazas en Magerit

Por cada amenaza, MAGEIRT propone un cuadro ilustrativo que contiene la siguiente información:

- Tipos de activos que se pueden ver afectados por la amenaza
- Dimensiones de seguridad que pueden verse afectadas por la amenaza
- Descripción de la amenaza indicando lo que puede ocurrir a los activos

Por ejemplo:



5.2.1. [I.1] Fuego

[I.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: incendio: posibilidad de que el fuego acabe con los recursos del sistema. **Origen:** Entorno (accidental) Humano (accidental o deliberado) **Ver:** EBIOS: 01- INCENDIO	

Ilustración 3 Ejemplo Amenazas Magerit

También en este caso, la información facilitada por MAGERIT simplifica la actividad de determinar a qué amenazas están expuestos los activos identificados.

Por lo que respecta las medidas o controles para reducir el riesgo MAGERIT aporta un listado de salvaguardas a aplicar, concretamente en el capítulo 6 del "Catálogo de Elementos" (libro 2):

- Protecciones generales u horizontales
- Protección de los datos / información
- Protección de las claves criptográficas
- Protección de los servicios
- Protección de las aplicaciones (software)
- Protección de los equipos (hardware)
- Protección de las comunicaciones
- Protección en los puntos de interconexión con otros sistemas
- Protección de los soportes de información
- Protección de los elementos auxiliares
- Seguridad física
- Protección de las instalaciones
- Salvaguardas relativas al personal
- Salvaguardas de tipo organizativo

- Continuidad de operaciones
- Externalización
- Adquisición y desarrollo

Además, los controles se distinguen según el tipo de protección que ofrecen ante las amenazas: preventivas (que reducen la probabilidad); las que limitan la degradación; y un tercer grupo que refuerzan los efectos del resto (monitorización, detección, concienciación y de carácter administrativo).

Finalmente hay que añadir que, en lo que respecta a la toma de decisiones, resulta relevante destacar que para MAGERIT el análisis de riesgos es solo eso, un análisis, y que lo importante es que debe facilitar la posterior toma de decisiones, que es en definitiva lo que se pretende, es decir, la aplicación de salvaguardas que protejan los activos de las amenazas a que están expuestos.

El proceso de gestión de riesgos implica la realización de una serie de actividades muy sistemáticas, y el uso de diferentes tipos de informaciones que a veces pueden tener un cierto volumen, a lo que además se une la necesidad de efectuar cálculos, y de consolidar toda esa información. Por ello, disponer de herramientas que automaticen el conjunto del proceso de gestión de riesgos resulta una buena opción para optimizar el tiempo que debe emplearse a la evaluación y tratamiento de riesgos.

Los entornos de análisis de riesgos permiten clasificar e incorporar a una aplicación la información necesaria para evaluar los riesgos, y para seleccionar las medidas que permitan mitigarlos en base a la disponibilidad de catálogos específicos de amenazas y controles (medidas).

Para realizar el análisis de riesgos se puede utilizar la herramienta de referencia PILAR, que implementa la metodología MAGERIT, en cualquiera de sus versiones (PILAR, PILAR Basic, µPILAR y online a través de la plataforma INÉS).

Las Guías CCN-STIC-470 PILAR, proporcionan manuales de uso en sus diferentes versiones.

A modo de ejemplo y siguiendo con la implantación del ENS, se ha llevado a cabo un Análisis de Riesgos con la herramienta de PILAR Basic y se adjunta el informe obtenido en el Anexo IV.

2.1.5 Validación y Declaración de Aplicabilidad Definitiva

Atendiendo a los resultados del anterior análisis de riesgos, en el que se habrán tenido en cuenta las exigencias derivadas de la normativa de protección de datos, el Responsable de Seguridad elaborará una relación de las medidas del ENS que son de aplicación al sistema (o a cada sub-sistema, si se ha recurrido a una segregación de sistemas), de acuerdo a los valores máximos de seguridad obtenidos en cada una de las dimensiones de seguridad y/o de acuerdo a la categoría del sistema, y las medidas de seguridad adicionales resultante del análisis de riesgos.

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

La inaplicabilidad de una medida requerida por el Anexo II, en función de la valoración del sistema, deberá estar motivada.

Cuando se recurra a medidas compensatorias, se indicará el motivo, así como las medidas que sustituye, tal y como se recoge en la Guía CCN-STIC 819 Medidas Compensatorias.

Las medidas se complementarán con aquellas que sean pertinentes a la vista del análisis de riesgos realizado. Téngase en cuenta que, tanto el ENS como la reglamentación de protección de datos de carácter personal, establecen una serie de medidas mínimas que deben ampliarse cuando sea prudente hacerlo.

La Declaración de Aplicabilidad se plasmará en un documento que debe ser aprobado formalmente por el Responsable de Seguridad. Este documento puede ser el elaborado de manera provisional que, una vez contrastado con el resultado obtenido en el Análisis de Riesgos, pasa a ser definitivo.

2.2 Datos de Carácter Personal

Casi todas las interacciones con la Administración implican un intercambio de datos de índole personal. Uno solo de esos datos puede no ser suficiente para identificar a un individuo. Sin embargo, cuando se recopilan varios juntos, pueden permitir la acotación entre la población, habilitando la identificación de

una persona en particular y, por lo tanto, constituyen datos personales. Es por eso que a menudo se la conoce como información de identificación personal.

Estos datos personales pueden ser tratados en un proceso de privacidad que los convierte en anónimos y ya no sería posible identificar al individuo. Para que los datos sean efectivamente anónimos, este proceso de verificación debe ser irreversible. Los datos que tras el proceso de encriptado o des identificado, pueden usarse identificar a una persona, siguen siendo datos personales.

Para dar amparo al tratamiento de los datos de carácter personal, se creó el Reglamento General de Protección de Datos (RGPD) que permite proteger los datos personales de una manera integral, independientemente de la tecnología utilizada, y se aplica tanto al procesamiento manual como al automatizado. Dentro del ámbito de aplicación de esta norma, también se tiene en cuenta la información almacenada, trasmitida y procesada.

2.2.1 El RGPD y los datos personales

El RGPD se crea con la intención de proporcionar un conjunto de leyes de privacidad en el marco de la UE, para posteriormente ser aplicada en la normativa interna de cada país miembro.

El Reglamento proporciona pautas tanto para organizaciones como para empresas con respecto a cómo manejan la información que se relaciona con las personas con las que interactúan. Esto es importante porque la tecnología tiene una naturaleza cambiante, y los datos personales están evolucionando con ella.

Actualmente la naturaleza de la información personal que compartimos con los sistemas de información se ha incrementado dando cabida a datos biométricos, datos de ubicación o direcciones IP. Por esta razón, nuestra información personal es más vulnerable que nunca y debe ser protegida por los Estados.

2.2.2 La definición de datos personales

Los datos personales son fundamentales para el espíritu del RGPD. Para evitar ser una definición que quede obsoleta en un corto periodo de tiempo, se ha buscado que sea lo más amplia y genérica posible.

La definición básica de datos personales es cualquier información relacionada con una persona física identificada o identificable (sujeto de datos). [2]

Además, según el RGPD serán datos de carácter personal los que permitan identificar a un individuo de manera directa o indirectamente, a través de identificadores en línea como su nombre, un número de identificación, direcciones IP o sus datos de ubicación.

En algunas circunstancias, incluso la información relacionada con el trabajo, el color del cabello o las opiniones políticas de una persona podría clasificarse como datos personales. Por lo general, esto se reduce al contexto en el que se recopilaron los datos y si un sujeto de datos podría ser directa o indirectamente identificable.

- **Ejemplos de información personal**

La definición de datos personales es cualquier información relacionada con una *"persona física identificada o identificable".* Los datos personales cubren una gama de identificadores.

- Nombre y apellidos.
- Dirección de correo electrónico.
- Número de teléfono.
- Domicilio.
- Fecha de nacimiento.
- Raza.
- Género.
- Opiniones políticas.
- Números de tarjetas de crédito.
- Datos en poder de un hospital o médico.
- Fotografía donde un individuo es identificable.
- Número de tarjeta de identificación.
- Un ID de cookie.

- Dirección de protocolo de Internet (IP)
- Datos de ubicación (por ejemplo, los datos de ubicación de un teléfono móvil).
- El identificador de publicidad de su teléfono.
- Los datos personales relacionados con el RGPD no cubren:
- Información sobre alguien que ha fallecido.
- Datos debidamente anonimizados.
- Información sobre administraciones públicas y empresas.

- **Datos confidenciales**

Aunque los términos "datos personales" y "datos sensibles" se utilizan a menudo para describir lo mismo, el RGPD hace una clara distinción entre estos dos términos. Según el reglamento, los datos sensibles son un conjunto de categorías especiales que deben manejarse con mayor seguridad. Estas categorías especiales son:

- Origen étnico o racial.
- Opiniones políticas.
- Identidad cultural o social.
- creencias filosóficas o religiosas;
- Afiliaciones sindicales.
- Datos genéticos.
- Datos biométricos (que se pueden utilizar para identificar de forma única a alguien).

- **Violaciones de datos personales**

El RGPD establece pautas muy estrictas con respecto a los datos personales y cómo se utilizan. Si cualquier información relacionada con otra persona se pierde, altera, divulga, destruye o accede accidental o ilegalmente, esto se clasifica como una violación de datos.

Los datos personales son un aspecto clave de la identidad en línea, pero desafortunadamente, pueden ser explotados. Algunas personas pueden alterar los datos personales con fines ilícitos, como crear documentos falsos o usar la información de contacto de las personas para acosarlas.

Incluso se puede dar el delito de robo de identidad financiera, que generalmente implica que los detalles de la tarjeta de crédito y la cuenta bancaria sean robados para ser utilizados o vendidos. En otros casos, los datos personales que han sido violados se utilizan para crear identidades falsas en línea, como perfiles falsos en las redes sociales.

2.2.3 La relación ENS y el RGPD

- **Empresa pública**

Con la aprobación de la Ley Orgánica nº 3/2018, de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales (en adelante LOPDGDD), los operadores a los que se refiere el artículo 77 de la citada ley son los siguientes:

Autoridades constitucionales u órganos de relevancia constitucional y sus homólogos en las comunidades autónomas, órganos jurisdiccionales, administraciones públicas generales, administraciones de las comunidades autónomas y órganos constitutivos de las administraciones locales; autoridades públicas y organismos públicos vinculados o dependientes de la administración pública; administraciones públicas independientes; el Banco de España; empresas públicas, en la medida en que los fines del tratamiento estén relacionados con el ejercicio del poder público; las fundaciones del sector público; las universidades públicas; los consorcios y los grupos parlamentarios de las Cortes Generales y de las legislaturas autonómicas, así como los grupos políticos de las sociedades locales, están obligados a aplicar las medidas de seguridad adecuadas establecidas en el RGPD cuando traten datos personales y a promover un cierto grado de implantación de medidas equivalentes en sus empresas vinculadas o en las fundaciones sujetas al derecho privado.

Para que sea eficaz, la aplicación del ENS debe llevarse a cabo con vistas a la integración con las obligaciones derivadas del RGPD. Es importante señalar que la Agencia Española de Protección de Datos ha establecido claramente en sus

directrices para las autoridades públicas que el cumplimiento de la ENS se considera parte del cumplimiento del artículo 32 del RGPD. La realización de la evaluación de riesgos de la ENS y la aplicación de las medidas de seguridad adecuadas constituyen el cumplimiento del RGPD.

Está claro que ambas normas deben cumplirse simultáneamente, incluyendo la auditoría proactiva, la notificación de infracciones y otros solapamientos.

- **Empresa privada**

Como se ha indicado previamente, el ENS está regulado en el ENS y su objeto es “el establecimiento de los principios y requisitos de una política de estabilidad en la implementación de medios electrónicos que posibilite la idónea defensa de la información” y sigue “fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información según con sus especificaciones funcionales, sin interrupciones o modificaciones descontrolado, y sin que la información logre llegar al entendimiento de individuos no autorizadas”.

El ámbito principal de aplicación del ENS son las Administraciones Públicas para “asegurar la entrada, totalidad, disponibilidad, veracidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios usados en medios electrónicos que gestionen en el ejercicio de sus competencias”. Sin embargo, se contemplan casos donde se aplicará a empresas del sector privado.

Los principios de este supuesto, se ubican en el último párrafo de la Disposición Adicional 1ª de la LOPDGDD. Esa Ley Orgánica instituye en su artículo 1.a) que su objeto es “adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679”, o sea, al Reglamento Gral. de Defensa de Datos.

Por ello, es importante mencionar que el párrafo final de la DA 1ª refiere una circunstancia que hace que la aplicabilidad del ENS sea, al menos potencialmente, universal.

> *“En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad*

se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad."

Este párrafo quiere decir que, en que toda entidad que preste o quiera prestar servicios a una Administración Pública ha de cumplir también con las medidas de seguridad que, en virtud del ENS, sean de aplicación a dicha administración de referencia.

Como consecuencia de dicho precepto, cada vez es más común, que las empresas privadas que se presentan a licitaciones del sector público encuentren reflejados en los pliegos la exigencia inexcusable de que cumplan con el Esquema Nacional de Seguridad y que hayan superado un proceso de certificación por una entidad debidamente acreditada.

2.3 Implantación de las medidas técnicas y organizativas del ENS

Una vez que se ha determinado el Plan de Adecuación y se ha definido que el sistema a evaluar se adecuará a una categoría media, el siguiente paso es llevar a cabo la implantación de las medidas técnicas y organizativas del ENS.

En la implementación de las medidas de seguridad, el Responsable de Seguridad cuenta con el apoyo de herramientas y guías publicadas por el CCN-CERT. El propio ENS en su artículo 29 señala la utilidad de las Guías CCN-STIC. En concreto, establece: "*Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones*."

Estas guías CCN-STIC no establecen un criterio que debe implementarse de forma obligada, sino que nos encontramos ante una serie de recomendaciones y directrices que permiten con su uso, la correcta implementación y cumplimiento del contenido en la normativa sobre el ENS. Entre las guías publicadas, las más representativas para la elaboración de este documento son las siguientes:

- CCN-STIC-800 Glosario de términos y abreviaturas del ENS
- CCN-STIC-803 Valoración de Sistemas en el ENS. El anexo II establece una serie de medidas de seguridad en función del nivel de seguridad de cada extensión y de la evaluación de la categoría de los sistemas de

información en cuestión. La categoría del sistema se calcula entonces en función del nivel de seguridad de cada dimensión. Esta guía proporciona directrices generales aplicables a diferentes tipos, dimensiones y sensibilidades de estructuras y no cubre casos específicos.

- CCN-STIC-804 ENS. Guía de implantación
- CCN-STIC-806 Plan de Adecuación al ENS. Los sistemas que ya se encontraban en uso a la entrada en vigor del Real Decreto 3/2010, de 8 de enero, tienen que adaptarse al Esquema Nacional de Seguridad de forma que permitan el acatamiento de lo determinado en la disposición final tercera de la Ley 11/2007, de 22 de junio. Esta guía refiere unos modelos de carácter general que son adaptables a entidades de diferente naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.
- CCN-STIC-818 Herramientas de Seguridad en el ENS. Persigue el doble objetivo de representar y catalogar las diferentes herramientas de seguridad efectivas, así como instituir las exigencias relativas a la selección, conformidad, ejecución, uso y sostenimiento de dichas herramientas de seguridad en los Sistemas.
- CCN-STIC-821 Normas de Seguridad en el ENS
- CCN-STIC-822 Procedimientos de Seguridad

2.3.1 Hoja de Ruta

Resulta útil cuadrar una hoja de ruta para crear un mapa de aquellas medidas que se han determinado a través de la Declaración de Aplicabilidad que serán aplicables. Además, si se sigue esta hoja de ruta se podrán implantar aquellas herramientas o soluciones necesarias para cumplir con las medidas que el ENS nos exige, de manera paulatina y organizada.

Como se ha repetido durante este trabajo, el Sistema analizado responde a una adecuación de categoría media, por lo tanto, las medidas aplicables a dicha adecuación serían 63 de las 75 que recoge el Anexo II del ENS y son las las siguientes:

org	Marco organizativo
[org.1]	Política de seguridad
[org.2]	Normativa de seguridad
[org.3]	Procedimientos de seguridad
[org.4]	Proceso de autorización
op	**Marco operacional**
[op.pl]	Planificación
[op.pl.1]	Análisis de riesgos
[op.pl.2]	Arquitectura de seguridad
[op.pl.3]	Adquisición de nuevos componentes
[op.pl.4]	Dimensionamiento / Gestión de capacidades
[op.acc]	Control de acceso
[op.acc.1]	Identificación
[op.acc.2]	Requisitos de acceso
[op.acc.3]	Segregación de funciones y tareas
[op.acc.4]	Proceso de gestión de derechos de acceso
[op.acc.5]	Mecanismo de autenticación
[op.acc.6]	Acceso local (local logon)
[op.acc.7]	Acceso remoto (remote login)
[op.exp]	Explotación
[op.exp.1]	Inventario de activos
[op.exp.2]	Configuración de seguridad
[op.exp.3]	Gestión de la configuración
[op.exp.4]	Mantenimiento

[op.exp.5]	Gestión de cambios
[op.exp.6]	Protección frente a código dañino
[op.exp.7]	Gestión de incidentes
[op.exp.8]	Registro de la actividad de los usuarios
[op.exp.9]	Registro de la gestión de incidentes
[op.exp.11]	Protección de claves criptográficas
[op.ext]	Servicios externos
[op.ext.1]	Contratación y acuerdos de nivel de servicio
[op.ext.2]	Gestión diaria
[op.cont]	Continuidad del servicio
[op.cont.1]	Análisis de impacto
[op.mon]	Monitorización del sistema
[op.mon.1]	Detección de intrusión
[op.mon.2]	Sistema de métricas
mp	**Medidas de protección**
[mp.if]	Protección de las instalaciones e infraestructuras
[mp.if.1]	Áreas separadas y con control de acceso
[mp.if.2]	Identificación de las personas
[mp.if.3]	Acondicionamiento de los locales
[mp.if.4]	Energía eléctrica
[mp.if.5]	Protección frente a incendios
[mp.if.6]	Protección frente a inundaciones
[mp.if.7]	Registro de entrada y salida de equipamiento
[mp.per]	Gestión del personal

[mp.per.1]	Caracterización del puesto de trabajo
[mp.per.2]	Deberes y obligaciones
[mp.per.3]	Concienciación
[mp.per.4]	Formación
[mp.eq]	Protección de los equipos
[mp.eq.1]	Puesto de trabajo despejado
[mp.eq.2]	Bloqueo de puesto de trabajo
[mp.eq.3]	Protección de equipos portátiles
[mp.eq.9]	Medios alternativos
[mp.com]	Protección de las comunicaciones
[mp.com.1]	Perímetro seguro
[mp.com.2]	Protección de la confidencialidad
[mp.com.3]	Protección de la autenticidad y de la integridad
[mp.si]	Protección de los soportes de información
[mp.si.1]	Etiquetado
[mp.si.2]	Criptografía
[mp.si.3]	Custodia
[mp.si.4]	Transporte
[mp.si.5]	Borrado y destrucción
[mp.sw]	Protección de las aplicaciones informáticas
[mp.sw.1]	Desarrollo
[mp.sw.2]	Aceptación y puesta en servicio
[mp.info]	Protección de la información
[mp.info.1]	Datos de carácter personal

[mp.info.2]	Calificación de la información
[mp.info.4]	Firma electrónica
[mp.info.6]	Limpieza de documentos
[mp.info.9]	Copias de seguridad *(backup)*
[mp.s]	Protección de los servicios
[mp.s.1]	Protección del correo electrónico
[mp.s.2]	Protección de servicios y aplicaciones web
[mp.s.8]	Protección frente a la denegación de servicio

Muchas de estas medidas pertenecen al mismo ámbito y están relacionadas entre sí, por lo que su agrupación a la hora de elaborar las guías, procedimientos y normativas, ayuda y simplifica el proceso. Por ello, como hoja de ruta se propone la siguiente agrupación de medidas por nombre de documento:

Medidas organizativas generales	**Medida ENS**
Política de seguridad	org.1
Normativa interna de uso de medios electrónicos	org.2; mp.per.2
Procedimientos de seguridad	org.3
Normativa de gestión del proceso de autorizaciones	org.4
Marco operacoinal	**Medida ENS**
Metodología de Gestión de Riesgos	op.pl.1
Procedimiento de Arquitectura de Seguridad	op.pl.2; mp.com.2; mp.com.3
Procedimiento para la adquisición de nuevos componentes	op.pl.3
Norma para el correcto dimensionamiento de los Sistemas de Información	op.pl.4;
Medidas de control de acceso	**Medida ENS**
Normativa de Control de Acceso Lógico	op.acc.1; op.acc.2; op.acc.4; op.acc.5; op.acc.6; op.acc.7
Procedimiento de Gestión de Usuarios	
Procedimiento de segregación de funciones	op.acc.3
Medidas de explotación	**Medida ENS**
Inventario de activos	op.exp.1
Procedimiento de Control de Seguridad en la Operativa	op.exp.2; op.exp.3; op.exp.6
Procedimiento de Gestión del Mantenimiento	op.exp.4; op.ext.2
Procedimiento de Gestión del Cambio	op.exp.5

Normativa de Gestión de Incidencias	op.exp.7; op.exp.9
Normativa de elaboración y protección de registros de actividad de los usuarios	op.exp.8
Procedimiento de Gestión de Claves Criptográficas	op.exp.11
Medidas de gestión de servicios externos	**Medida ENS**
Procedimiento de Contratación y seguimiento de Servicios Externos	op.ext.1
Medidas de continuidad del servicio	**Medida ENS**
Norma para la realización de Análisis de Impacto	op.cont.1
Medidas de monitorización del sistema	**Medida ENS**
Procedimiento de detección de intrusión	op.mon.1
Procedimiento de Métricas e indicadores	op.mon.2
Medidas de protección	**Medida ENS**
Normativa de Seguridad Física	mp.if.1; mp.if.2; mp.if.3; mp.if.4; mp.if.5; mp.if.6
Normativa de Control de Acceso Físico	
Registro de entrada y salida de equipamiento	mp.if.7
Medidas de gestión de personal	**Medida ENS**
Normativa competencias y perfiles de puesto	mp.per.1
Procedimiento de formación y concienciación	mp.per.3; mp.per.4
Medidas de protección de equipos	**Medida ENS**
Normativa de puesto despejado	mp.eq.1; mp.eq.2
Normativa de seguridad de los equipos	mp.eq.3; mp.eq.9
Medidas de protección de las comunicaciones	**Medida ENS**
Procedimiento de protección perimetral	mp.com.1;
Medidas de protección de los soportes de información	**Medida ENS**
Procedimiento de gestión de soportes etiquetado de soportes	mp.si.1; mp.si.2; mp.si.3; mp.si.4; mp.si.5
Medidas de protección de aplicaciones informáticas	**Medida ENS**
Normativa para el desarrollo seguro de aplicaciones y su paso a producción	mp.sw.1
Normativa Plan de Pruebas	mp.sw.2
Medidas de protección de la información	**Medida ENS**
Procedimiento para la protección de los datos de carácter general	mp.info.1
Procedimiento de Clasificación y Gestión Segura de la Información	mp.info.2
Política de firma electrónica	mp.info.4
Procedimiento sobre control y borrado de Metadatos	mp.info.6
Procedimiento de Respaldo y Recuperación	mp.info.9
Medidas de protección de los servicios	**Medida ENS**
Procedimiento de protección del correo electrónico	mp.s.1
Protección de servicios y aplicaciones WEB	mp.s.2; mp.s.8

2.3.2 Normativa y procedimientos de seguridad

Las medidas de seguridad que se han de aplicar se dividen en tres grupos:

- Marco organizativo (org). Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
- Marco operacional (op). Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
- Medidas de protección (mp). Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

Para llevar a cabo esta fase de la implantación, se elaborará un modelo de los documentos que formarían parte de esta Adecuación al ENS (Anexo V), concretamente la Normativa General que debe ser conocedora por todos los usuarios y empleados del organismo en el que se realice la implantación y que forma parte de todo el repositorio documental del Plan de Adecuación. Este documento presentará el formato y los apartados que compartirán en común todos los documentos. El objeto de cada uno de dichos documentos, es el siguiente:

- Normativa interna de uso de medios electrónicos: Este documento establece las normas de uso de los dispositivos asignados al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como al acceso y tratamiento de datos de carácter personal, en soporte electrónico y en papel.
- Procedimientos de seguridad: Este documento establece una presentación de las normas, procedimientos y guías que aplicarán los requisitos de seguridad previamente definidos, los procedimientos operativos a seguir y las responsabilidades del personal, así como la estructura y el contenido de estos documentos.
- Normativa de gestión del proceso de autorizaciones: Este documento establecerá las pautas que deben seguir los usuarios del organismo para

solicitar autorización de acceso a todos aquellos recursos que lo necesiten.

- Metodología de gestión de riesgos: Este documento expondrá la metodología utilizada para llevar a cabo el Análisis de Riesgos y contendrá una guía de utilización de la herramienta asignada.
- Procedimiento de arquitectura de seguridad: Este procedimiento fundamenta y describe la arquitectura de seguridad de sistemas actualizada con la que cuenta el organismo dentro del alcance señalado en el ENS.
- Procedimiento para la adquisición de nuevos componentes: Este documento narra el proceso que debe seguir la organización a la hora de adquirir nuevos componentes, los requisitos de seguridad que deben tener los mismos y las características mínimas.
- Norma para el correcto dimensionamiento de los Sistemas de Información: Esta norma describirá cuales son las necesidades de dimensionamiento con las que debe contar el sistema a la hora de adquirir o poner en explotación un recurso.
- Norma de control de acceso lógico: Esta norma será de aplicación a los usuarios del organismo y describirá los requisitos que se deben cumplir a la hora de solicitar acceso a un recurso.
- Procedimiento de gestión de usuarios: Este documento establece el procedimiento que deberá seguir el personal TIC a la hora de dar de alta un usuario, modificar o dar de baja el mismo.
- Procedimiento de segregación de funciones: Este documento plasma un esquema de funciones y tareas en el que se contemplan las que son incompatibles en una misma persona.
- Inventario de activos: Este documento registrará los activos con los que cuente la organización siguiendo los mínimos recomendados por el ENS.
- Procedimiento de Control de Seguridad en la Operativa: Este documento recogerá los controles que se deben llevar a cabo por parte del personal TIC en el día a día de su actividad.

- Procedimiento de Gestión del Mantenimiento: Este documento expondrá los planes de mantenimiento continuos que deben llevarse a cabo.
- Procedimiento de Gestión del Cambio: Este documento establece el proceso y mecanismo de autorización y ejecución de cambios dentro del sistema del organismo.
- Normativa de Gestión de Incidencias: Este documento establece el mecanismo de gestión de incidencias y su registro.
- Normativa de elaboración y protección de registros de actividad de los usuarios: Este documento expondrá la metodología que se seguirá para proceder proteger los registros de la actividad de los usuarios.
- Procedimiento de Gestión de Claves Criptográficas: Este documento tiene por objeto establecer un mecanismo común a todo el organismo de gestión de las claves criptográficas.
- Procedimiento de Contratación y seguimiento de Servicios Externos: Documento en el que se expone el proceso de contratación de servicios externos y los requisitos mínimos que éstos deben cumplir.
- Norma para la realización de Análisis de Impacto: Este documento expone la metodología a seguir para llevar a cabo un análisis de impacto.
- Procedimiento de detección de intrusión: Este procedimiento establece las medidas de detección de intrusos con las que cuenta el organismo.
- Procedimiento de Métricas e indicadores: Este procedimiento describirá las métricas predictivas con las que debe contar el organismo que anuncian posibles incidentes antes de que estos se produzcan.
- Normativa de Seguridad Física: Este documento expondrá las medidas con las que tiene que contar el organismo en su entorno físico (instalaciones y CPD).
- Normativa de Control de Acceso Físico: Este documento narra las medidas que deben cumplirse para acceder a las instalaciones del organismo.

- Registro de entrada y salida de equipamiento: Se trata de un documento donde se debe registrar toda entrada y salida de equipamiento de las instalaciones siguiendo los mínimos establecidos por el ENS.
- Normativa competencias y perfiles de puesto: Este documento refleja la relación de los puestos de trabajo de los usuarios que forman parte del organismo.
- Procedimiento de formación y concienciación: Este documento refleja el plan de formación y concienciación anual que debe seguir el organismo.
- Normativa de puesto despejado: Este documento está dirigido a los usuarios para que mantengan su puesto de trabajo despejado según las normas del ENS.
- Normativa de seguridad de los equipos: Este documento, dirigido a los usuarios, expone las medidas que deben seguirse para proteger los equipos de posibles vulnerabilidades.
- Procedimiento de protección perimetral: Este procedimiento establece los requisitos mínimos que deben seguirse para proteger el perímetro lógico del sistema de información.
- Procedimiento de gestión de soportes: Este procedimiento expone el mecanismo de etiquetado, manejo, custodia, borrado, destrucción, transporte y uso de los elementos criptográficos de los soportes del organismo.
- Normativa para el desarrollo seguro de aplicaciones y su paso a producción: Este documento establece el procedimiento de desarrollo seguro y el paso a producción que debe seguir el personal TIC.
- Normativa Plan de Pruebas: Este proceso establece las pruebas y los mecanismos de restauración que debe seguir el organismo de manera periódica.
- Procedimiento para la protección de los datos de carácter general: Este procedimiento está ligado directamente a las instrucciones que el Delegado de Protección de Datos indique al respecto.

- Procedimiento de Clasificación y Gestión Segura de la Información: Este procedimiento tiene por objeto establecer las normas de clasificación de la información que se maneja dentro del organismo para evitar posibles fugas,
- Política de firma electrónica: Este documento reflejará la política a la que esté adherida el organismo respecto a la firma electrónica.
- Procedimiento sobre control y borrado de Metadatos: El objeto de este documento es establecer el mecanismo de limpieza de documentos antes de que éstos sean publicados o compartidos fuera del organismo.
- Procedimiento de Respaldo y Recuperación: Este documento establece el proceso de copias de seguridad que debe cumplir el organismo.
- Procedimiento de protección del correo electrónico: Este procedimiento establece la configuración con la que debe contar el servidor de correo electrónico que utilice el organismo.
- Protección de servicios y aplicaciones WEB: El objeto del documento es establecer las directrices de protección de los sistemas dedicados a la publicación frente a los ataques, amenazas o denegaciones de servicios que pueda sufrir el organismo.

2.3.3 Auditoría y certificación

El articulo 34 y el anexo III del ENS define que los sistemas de categoría media tienen la obligatoriedad de realizar una auditoria regular ordinaria cada dos años.

El objeto de una auditoria es verificar el cumplimiento de los establecido en el ENS, tanto en sus principios básicos como en los requisitos de seguridad y emitir una opinión independiente, objetiva, integra, profesional y confidencial siempre basada en la evidencia del cumplimiento o no de las medidas de seguridad.

El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado sobre el nivel de seguridad implantado; tanto internamente como frente a terceros, que pudieran estar relacionados, es decir, calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida. Además, se obtendrá la certificación que acredite que

el sistema de información del organismo cumple con el ENS y está adecuado a una categoría media.

Como toda auditoría de sistemas de las tecnologías de la información, que incluye normalmente, los aspectos de seguridad de los sistemas, ésta debe realizarse de una forma metodológica que permita identificar claramente:

- El Alcance y Objetivo de la Auditoría.
- Los recursos necesarios y apropiados para realizar la auditoría (equipo auditor), según lo establecido en los Anexos A y B de esta guía.
- Las debidas comunicaciones con los responsables de la organización que soliciten la auditoría.
- La planificación preliminar o requisitos de información previos al desarrollo del plan de auditoría, y a la ejecución de las pruebas que se consideren necesarias.
- El establecimiento de un plan de auditoría detallado con las actividades, revisiones y pruebas de auditoría previstas.
- La presentación, de los resultados individuales de las pruebas, a las personas involucradas con estos resultados, para su confirmación sin valoraciones con respecto a los resultados finales.
- La evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del RD 3/2010.
- La confección, presentación y emisión formal del Informe de Auditoría.

La metodología aplicada debe permitir comprobar, a través de los registros y evidencias de auditoría, la consecución de estos pasos, las limitaciones que se hayan podido producir en el desarrollo de las tareas, y las actividades realizadas.

Para una consecución eficaz de la auditoría, el equipo auditor verificará que las medidas de seguridad para el sistema auditado se ajustan a los principios básicos del RD 3/2010 (artículo 4), y satisfacen los requisitos mínimos de seguridad (artículo 11). La ‘Guía CCN-STIC 808 de Verificación del cumplimiento del ENS’ resulta muy útil para preparar la auditoría, puesto que establece todos los parámetros que tendrá en cuenta el auditor.

Una vez que se ha planificado y llevado a cabo la auditoría, El dictamen final del Informe de Auditoría será uno de los tres siguientes:

- “FAVORABLE”: Cuando no se evidencie ninguna “No Conformidad Mayor” o “No Conformidad Menor”.
- “FAVORABLE CON NO CONFORMIDADES”: Cuando se evidencien “No Conformidades Menores”. y/o “No Conformidades Mayores”. En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un Plan de Acciones Correctivas (PAC) sobre tales desviaciones a la entidad certificadora para su evaluación.
- “DESFAVORABLE”: Cuando exista un número significativo de No Conformidades Mayores cuya solución no pueda evidenciarse a través de un Plan de Acciones Correctivas y requiere la comprobación in-situ de su correcta implantación a través de una auditoría extraordinaria.

La Certificación de Conformidad con el ENS únicamente podrá expedirse si el dictamen fuera “FAVORABLE” o, si habiendo sido “FAVORABLE CON NO CONFORMIDADES”, el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve las desviaciones evidenciadas, a criterio de la entidad certificadora.

Ante un dictamen “DESFAVORABLE”, la entidad titular del sistema de información auditado, en un plazo no superior a seis meses desde la fecha de emisión del Informe de Auditoría, deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre las desviaciones evidenciadas que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.

3. Conclusiones

Las conclusiones al trabajo llevado a cabo son las siguientes:

- En primer lugar, el objetivo fijado en este Trabajo de Fin de Máster está asociado directamente con el cumplimiento del ENS. Para ello, se ha creado ‘Organismo X’ a modo de ejemplo, a través del cual se han ido implantando las medidas del Anexo II del ENS y para el que se han desarrollado los documentos que resultarían de aplicación.

  A través del desarrollo de las medidas y los documentos que han justificado el Plan de Adecuación al ENS, se ha podido observar que este Real Decreto asume al completo la misión para la que fue encomendado, es decir, la protección de la seguridad de las Administraciones Públicas y sus sistemas.

- Para comenzar y, siguiendo las guías que ha elaborado el CCN, se ha creado un Plan de Adecuación por el cual el ‘Organismo X’ pasará a cumplir con el ENS. Se identificó el sistema a través de las Fichas de Servicio, en las que se recopilan todos los datos necesarios para conocer el sistema de información del Organismo. A continuación, con la categorización del sistema, se pudo comprobar a qué nivel sería adecuado este Organismo y, por tanto, las medidas del Anexo II del ENS que, a priori, serían aplicables.

  Posteriormente, se llevó a cabo un análisis de riesgos, con el objetivo de determinar en qué situación se encuentra el Organismo antes de implantar el ENS y conseguir así una foto de la seguridad actual del mismo. Además, con este Análisis de Riesgos se confirma la categoría del Sistema de información del ‘Organismo X’, pudiendo pasar así a validar la Declaración de Aplicabilidad y comenzar con la implantación de las medidas. Cabe destacar que se realizó el Análisis de Riesgos con la herramienta PILAR, cuya metodología de análisis es MAGERIT.

  Una vez determinada la categoría del Sistema, se ha procedido a elaborar un mapa de ruta a través del cual se ve reflejado el número de documentos que se irán implantando en el Organismo. Este mapa de ruta

permite simplificar el proceso de implantación, aunando varias medidas que pertenecen al mismo ámbito de aplicación en un solo documento, facilitando así su interpretación y su cumplimiento.

Se ha proporcionado un ejemplo de documentación con la que el 'Organismo X' contaría y mediante la cual implantaría las medidas del ENS. Para corroborar que las mismas se están cumpliendo, el último paso debe ser siempre la auditoría, puesto que, de esta forma, una entidad ajena al organismo y al proceso de Adecuación al ENS revisa y verifica el cumplimiento de todas las pautas implantadas, consiguiendo así la certificación del ENS y cumpliendo con la obligación legal que el Real Decreto impone.

- Una vez llevado a cabo todo este proceso, cabe concluir que se han cumplido los objetivos fijados inicialmente. Considero que el ENS permite crear una hoja de ruta bastante intuitiva y lógica que consigue que la Adecuación al mismo no resulte dificultosa. Como toda normativa, el ENS es interpretable, por lo que las Guías que proporciona el CCN resultan de especial ayuda para despejar las dudas que puedan ir surgiendo y para trazar ese mapa que se ha nombrado anteriormente. Sin duda, el trabajo que hay detrás de las mismas, hechas por expertos, no deja lugar a las dudas y sirve para conseguir el objetivo fijado.
- Respecto a la metodología seguida para llevar a cabo este trabajo, considero que ha sido de gran ayuda establecer un método de entregas parciales pues, de esta forma, he conseguido llegar a las metas de manera desahogada y con las correcciones necesarias para conseguir el objetivo final que es entregar un trabajo de calidad y a tiempo.
- Como objetivo a futuro, aunque se ha tenido en cuenta el Real Decreto 311/2022, de 3 de mayo en la elaboración de este documento, quedaría estudiar como se va implementando realmente y las desviaciones que van apareciendo. Merece la pena ver la evolución del mismo y el grado de implementación en el ámbito público y observar como los cambios que ha introducido actualizan la seguridad de los Sistemas de Información de las Administraciones Públicas.

4. Glosario

A	Autenticidad
C	Confidencialidad
CCN	Centro Criptológico Nacional
D	Disponibilidad
DA	Declaración Adicional
ENS	Esquema Nacional de Seguridad
FEMP	Federación Española de Municipios y Provincias
I	Integridad
IP	Protocolo de Internet
LOPDGDD	Ley Orgánica de Protección de Datos y Garantías de Derechos Digitales
mp	Medidas de Protección
n.a.	No Aplica
op	Medidas operacionales
org	Medidas organizacionales
RGPD	Reglamento (UE) General de Protección de Datos
T	Trazabilidad
UE	Unión Europea

5. Bibliografía

- **Bibliografía y guías**:

ALVAREZ HERNANDO, J., Guía práctica sobre Protección de Datos: cuestiones y formularios, LEX NOVA, 2011.

CCN-STIC-800 Glosario de términos y abreviaturas del ENS, 2011. Disponible 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

CCN-STIC-802 Auditoría del ENS, 2017. Disponible 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

CCN-STIC-803 Valoración de Sistemas en el ENS, 2020. Disponible 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

CCN-STIC-804 ENS. Guía de implantación, 2017. Disponible 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

CCN-STIC-806 Plan de Adecuación al ENS, 2020. Disponible 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

CCN-STIC-808 Verificación del cumplimiento del ENS, 2017. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2404-ccn-stic-808-anexo-iii-verificacion-del-cumplimiento-del-ens.html

CCN-STIC-818 Herramientas de Seguridad en el ENS, 2012. Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/527-ccn-stic-818-herramientas-de-seguridad-en-el-ens/file.html

CCN-STIC-821 Normas de Seguridad en el ENS, 2018. Disponible 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

CCN-STIC-822 Procedimientos de Seguridad, 2012. Disponible 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

CCN-STIC-883 Implantación del ENS para Entidades Locales, 2020. Disponible 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

FERNÁNDEZ RIVERO, P.P., Cómo implantar un SGSI según UNE-ISO/IEC 27001: 2014 y su aplicación en el Esquema Nacional de Seguridad. 2015.

FERRO VEIGA, J.M., Normativa de Seguridad Nacional, 2019

FUNDACION TELEFONICA, universidad 2020: Papel de las TIC en el nuevo entorno socioeconómico, Ariel, 2012

GALÁN PASCUAL, C., ciberseguridad, Lefebvre, 2021.

MOLINA MATEOS, J.M., Esquema Nacional de Seguridad. 2010.

- **Normativa:**

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, *BOE núm 150 de 23 de junio de 2007.*

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, *BOE núm. 25 de 29 de enero de 2010*.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, *BOE núm. 236 de 2 de enero de 2015.*

Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales, *BOE núm. 294 de 6 de diciembre de 2018.*

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, *BOE núm. 106 de 4 de mayo de 2022.*

6. Anexos

6.1 Anexo I: Política de Seguridad de la Información

1. INTRODUCCIÓN

El Organismo ‘X’ 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. MISIÓN DEL ORGANISMO ‘X’

El Organismo ‘X’ tiene como misión y objetivo proporcionar sus servicios a través de la Sede Electrónica.

3. ALCANCE

Esta Política se aplicará a los sistemas de información del Organismo ‘X’ que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

4. MARCO NORMATIVO

El marco normativo que afecta al desarrollo de las actividades y competencias del Organismo ‘X’ está constituido por normas jurídicas estatales orientadas a la administración electrónica, a la seguridad de la información y los servicios que la manejan, así como a la protección de datos de naturaleza personal.

Las normas que constituyen dicho marco, se encuentran recogidas en un registro al efecto, el cual se mantiene actualizado según señala el correspondiente procedimiento de gestión de requisitos legales.

También podrán formar parte del referido marco, aquellas normas aplicables a la Administración Electrónica del Organismo ‘X’, que sean desarrollo de las anteriores o estén relacionadas, pudiendo ser adicionalmente publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

5. CUMPLIMIENTO DE ARTÍCULOS

El Organismo ‘X’ para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Organismo 'X' estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

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

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 2)

El Organismo 'X' ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma

rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 14) y profesionalidad (artículo 15)

Todos los miembros del Organismo 'X' dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, 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.

Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos cada una vez al año.
- Cuando cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)

El Organismo ‘X’ ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, el Organismo ‘X’ implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

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

El Organismo ‘X’ establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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).

- Para garantizar la disponibilidad de los servicios, el Organismo ‘X’ dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)

El Organismo ‘X’ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)

El Organismo ‘X’ ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “ORGANIZACIÓN DE LA SEGURIDAD” del presente documento.

Autorización y control de los accesos (artículo 16)

El Organismo ‘X’ ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 17)

El Organismo ‘X’ ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)

Para la adquisición de productos, el Organismo ‘X’ tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen, a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)

El Organismo ‘X’ ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de las competencias del Organismo ‘X’. De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 23)

El Organismo ‘X’ ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en

cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

6. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la Seguridad de la Información en el Organismo 'X' se establece en la forma que se indica a continuación.

6.1. Roles o perfiles de seguridad

Para garantizar el cumplimiento y la adaptación de las medidas exigidas reglamentariamente, se han creado roles o perfiles de seguridad y se han designado los cargos u órganos que los ocuparán, del siguiente modo:

- Delegado de Protección de Datos (DPD): _____
- Responsable/s de Información: _____
- Responsable/s de los Servicios: _____
- Responsable de Seguridad: _____
- Responsable del Sistema: _____

6.2. Comité de Seguridad de la Información

El Organismo 'X' ha constituido un Comité de Seguridad de la Información, como órgano colegiado, y está formado por los siguientes miembros:

- Presidente: _____
- Secretario/a: _____
- Miembros:
    - Responsable/s de la Información. <opcional>
    - Responsable/s de los Servicios. <opcional>
    - Delegado de Protección de Datos.
    - Responsable de Seguridad.

- Responsable del Sistema.

Los Responsables de la Información y de los Servicios serán convocados en función de los asuntos a tratar.

El Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación, se hará constar siempre en acta la opinión del Delegado de Protección de Datos.

Con carácter opcional, otros miembros del Organismo 'X' podrán incorporarse a las labores del Comité, incluidos grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias del Organismo 'X' con periodicidad semestral, previa convocatoria al efecto realizada por el Presidente de dicho Comité.

6.3. Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada una de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios

- Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta al Responsable de Seguridad ENS, y/o Comité de Seguridad de la Información
- Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.

- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema

Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

Elaborar los procedimientos operativos necesarios.

Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

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

Prestar al Responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.

Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

Llevar a cabo las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

6.4 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

6.5. Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta Política ha sido realizada por Organismo 'X' y comunicada a las partes afectadas vía electrónica.

Los miembros del Comité, así como los roles de seguridad serán revisados cada cuatro años o con ocasión de vacante.

6.6. Resolución de conflictos

El Comité de Seguridad de la Información, se encargará de la resolución de los conflictos y/o diferencias de opiniones, que pudieran surgir entre los roles de seguridad.

7. DATOS DE CARÁCTER PERSONAL

El Organismo ‘X’ solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se han ido adaptando las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo.

9. TERCERAS PARTES

Cuando una tercera parte preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Organismo 'X' definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Organismo 'X' lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Organismo 'X' utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad. De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogidas en el artículo 29 "Instrucciones técnicas de seguridad y guías de seguridad" del Real Decreto 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 modificado por el Real Decreto 951/2015 de 23 de octubre, y en consideración a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS 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.

6.2 Anexo II: Ficha de Servicio

Nombre del Servicio	
Código[1]	**Denominación**

Descripción del Servicio

Datos (información) que trata					
Datos personales				**Datos no-personales**	
Dato	**¿Categorías especiales de datos? (S/N)**[2]	**Origen del Dato**	**Destinatarios previstos**	**Dato**	**Origen del Dato**

Tipo de Servicio (Formulario web, aplicaciones, servicio externo, …)

[1] El código usado será: {SF/SI}nn, siendo SF (Servicio Finalista: descrito en las funciones del organismo), SI (Servicio Instrumental: de apoyo a la consecución de los Servicios Finalistas), nn (desde el 00 al 99)

[2] Datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física. (Art. 9 RGPD)

Componentes del servicio

Componentes del Servicio (servidores virtuales, servidor web, servidores externos,…)	**Ubicación** (CPD, …)

Arquitectura técnica de prestación del Servicio

Dependencias entre Servicios	
¿Depende de otro(s) Servicio(s)?	
Cód. – Nombre del Servicio	**Descripción de la dependencia**

¿Dependen otro(s) Servicio(s) de éste?	
Cód. – Nombre del Servicio	**Descripción de la dependencia**

Responsables
Responsible funcional del Servicio

Aproximación inicial a la valoración de los Niveles de Seguridad				
DISPONIBILIDAD (D)	**INTEGRIDAD (I)**	**CONFIDENCIALIDAD (C)**	**AUTENTICIDAD (A)**	**TRAZABILIDAD (T)**

(D): Tiempo máximo de interrupción del servicio: B-Baja (24 horas) / M-Media (Entre 4 y 24 horas) / A-Alta (Menos de 4 horas)

6.3 Anexo III: Categorización del Sistema

A) Identificación de los servicios esenciales:

Por activos esenciales se entenderán aquellos que constituyen la esencia y razón de ser de un sistema de información, es decir, los servicios que presta y la información que maneja.

La determinación de la categoría de un sistema de información se fundamenta en la valoración de los activos esenciales, a saber:

- Los Servicios, entendidos como toda función o prestación desempeñada por alguna entidad, órgano o unidad administrativa, destinados a cuidar intereses o satisfacer necesidades de los ciudadanos.

  También se pueden considerar los procedimientos internos de los citados organismos como accesorios para la prestación del servicio.

  No se consideran activos esenciales aquellos servicios internos o auxiliares, tales como correo electrónico, ficheros en red, servicios de directorio, de impresión, de copias de respaldo, etc.

- La Información, entendida como los datos en los que se apoyan los servicios para la realización de dichas funciones o actividades, ya sea que los utilice directamente, o de forma accesoria, es decir, siempre será necesaria la existencia de un Servicio o función que la utilice.

  No se consideran activos esenciales los datos auxiliares que no son objeto directo del servicio y sólo aparecen como instrumentales para la prestación de los servicios. Por ejemplo, servicios de directorio, claves de acceso, etc.

Para la identificación de los activos esenciales de un sistema, puede resultar de utilidad consultar las fuentes que se citan a continuación:

- Documentación técnica de aplicaciones que componen el sistema (guías o manuales de usuario, manuales de despliegue, de explotación o de mantenimiento, esquemas de red, etc.).
- Registro de Actividades de Tratamiento (obligatorio en virtud de lo dispuesto en los artículos 30 del RGPD y 31 de la LOPDGDD).

Por otra parte, puede darse la circunstancia de diferentes activos de un mismo sistema de información sometidos a requisitos diferentes, en virtud de que atiendan a distintos tipos de información o servicios. Lo anterior exigirá la descomposición del sistema de información en subsistemas de información o a asumir para todo el conjunto el máximo nivel al que están sometidos sus dimensiones de seguridad.

Se han identificado los siguientes activos:

ACTIVOS ESENCIALES	
Servicios Finalistas	[SF_01] Servicio a usuarios
	[SF_02] Servicio a externos
	[SF_03] Servicio a ciudadanos
Servicios instrumentales	[SI_01] Servicio nóminas a usuarios
	[SI_02] Servicio de buzón electrónico

B) Valoración de los activos:

Acorde al artículo 43 ENS, la categoría de un sistema de información, en materia de seguridad, busca el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad.

El citado artículo y el Anexo I indican que la determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los sistemas, con repercusión en la capacidad organizativa para alcanzar sus objetivos, proteger los activos a su cargo, cumplir sus obligaciones diarias de servicio, respetar la legalidad vigente y los derechos de las personas.

En este sentido el presente procedimiento permitirá a los Responsables de la Información y del Servicio justificar la valoración otorgada a los activos a su cargo, en función de las consecuencias que tendría un incidente de seguridad que afectara a cada una de las dimensiones de seguridad.

- **Dimensiones de seguridad**

La determinación de la categoría se efectuará de acuerdo con la valoración del impacto que tendría un incidente que afectará a la seguridad de la información o de los servicios con perjuicio para alguna de las dimensiones de seguridad, a saber:

- **Disponibilidad** [D]. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

  El nivel de seguridad requerido en el aspecto de disponibilidad se establecerá en función de las consecuencias que tendría el que una persona autorizada no pudiera acceder a la información cuando la necesita.

- **Autenticidad** [A]. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

  El nivel de seguridad requerido en el aspecto de autenticidad se establecerá en función de las consecuencias que tendría el hecho de que la información no fuera auténtica.

- **Integridad** [I]. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

  El nivel de seguridad requerido en el aspecto de integridad se establecerá en función de las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

- **Confidencialidad** [C]. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

  El nivel de seguridad requerido en el aspecto de confidencialidad se establecerá en función de las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

- **Trazabilidad** [T]. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

  El nivel de seguridad requerido en el aspecto de trazabilidad se establecerá en función de las consecuencias que tendría el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.

La selección de las medidas de seguridad, indicadas en el Anexo II del ENS, en consecuencia, vendrá determinada por la valoración del nivel de seguridad en cada dimensión, y, en definitiva, por la determinación de la categoría del sistema de información de que se trate. A su vez, la categoría de un sistema de información se establecerá a partir del nivel de seguridad más alto de las dimensiones valoradas.

- **Valoración de las dimensiones de seguridad de los activos**

La categorización de un sistema de información, en materia de seguridad, consistirá en la valoración de los activos esenciales, y de las dimensiones de seguridad en las que el impacto de un incidente sea mayor, obviando aquellas combinaciones en las que el impacto sea despreciable o irrelevante.

Se comenzará la valoración de los activos de tipo información, valorando en este orden: confidencialidad, integridad, autenticidad, trazabilidad y, si fuera relevante, disponibilidad.

Se seguirá con la valoración de los activos de tipo servicio, valorando para los mismos la disponibilidad. Los requisitos en materia de confidencialidad, integridad, autenticidad y trazabilidad suelen venir impuestos por los tipos de información que maneja el servicio, asumiendo los establecidos anteriormente.

Una información o un servicio, por otra parte, pueden verse afectados en una o más de sus dimensiones de seguridad. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

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

Cada una de las dimensiones de seguridad afectadas se adscribirá a uno de los siguientes niveles:

- **Nivel BAJO:** Cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones, obligaciones, responsabilidades y reputación de la organización, sobre sus activos o sobre los derechos de los individuos afectados.

  Se entenderá por perjuicio limitado:

  - La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque sigan desempeñándose.
  - El sufrimiento de un daño menor por los activos de la organización.
  - El incumplimiento formal de alguna Ley o regulación, que tenga carácter de subsanable.
  - Causar un perjuicio menor a algún individuo, que aun siendo molesto pueda ser fácilmente reparable.
  - Otros de naturaleza análoga.
- **Nivel MEDIO**: Cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones, obligaciones, responsabilidades y reputación de la organización, sobre sus activos o sobre los derechos de los individuos afectados.

  Se entenderá por perjuicio grave:

  - La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque sigan desempeñándose.
  - El sufrimiento de un daño significativo por los activos de la organización.
  - El incumplimiento material de alguna Ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
  - Causar un perjuicio significativo a algún individuo, de difícil reparación.

- Otros de naturaleza análoga.

- **Nivel ALTO:** Cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones, obligaciones, responsabilidades y reputación de la organización, sobre sus activos o sobre los derechos de los individuos afectados.

  Se entenderá por perjuicio muy grave:

  - La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
  - El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
  - El incumplimiento grave de alguna Ley o regulación.
  - Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
  - Otros de naturaleza análoga.

Se ha llevado a cabo la siguiente valoración:

Activos esenciales	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	AUTENTICIDAD	TRAZABILIDAD
[SF_01]	BAJA	MEDIA	BAJA	BAJA	BAJA
[SF_02]	BAJA	MEDIA	BAJA	BAJA	BAJA
[SF_03]	BAJA	BAJA	MEDIA	BAJA	BAJA
[SI_01]	BAJA	BAJA	BAJA	BAJA	BAJA
[SI_02]	BAJA	BAJA	BAJA	BAJA	BAJA

C) Resultado de la categorización

Una vez valorados los diferentes tipos de servicios e información que se manejan en un sistema de información, será el Responsable de Seguridad el encargado de formular y documentar la categoría del sistema, de acuerdo a los niveles máximos de cada dimensión de seguridad.

El ENS establece tres categorías para los sistemas: BÁSICA, MEDIA y ALTA, a saber:

- Un sistema de información será **de categoría ALTA** si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- Un sistema de información será de **categoría MEDIA** si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO y ninguna alcanza un nivel superior.
- Un sistema de información será de **categoría BÁSICA** si alguna de sus dimensiones de seguridad alcanza el nivel BAJO y ninguna alcanza un nivel superior.

Por lo tanto, el resultado de la categorización llevada a cabo es la siguiente:

Resultado categorización
CATEGORÍA MEDIA

6.4 Anexo IV: Análisis de Riesgos

A) Objeto

El propósito del presente informe es documentar el análisis de riesgos que se ha realizado a la sede electrónica del Organismo ‘X’

La funcionalidad principal de esta solución web, es la de permitir realizar por vía electrónica la presentación y seguimiento de solicitudes relacionadas con los procedimientos administrativos de la sede electrónica.

B) Alcance

El alcance de este análisis de riesgos consiste en la evaluación del uso de recursos y controles del Sistema (implementados o no) para eliminar y gestionar las vulnerabilidades explotables por amenazas, tanto internas como externas a los sistemas que componen la sede electrónica.

En el caso de que estas vulnerabilidades llegaran a explotarse, podrían tener las siguientes consecuencias:

- Divulgación no autorizada de información.
- Modificaciones no autorizadas en el sistema, de la información o ambas.
- Impacto en la reputación de la organización.
- Denegación de servicio, acceso a datos o a usuarios autorizados.

En este sentido, el presente informe evalúa las dimensiones de Confidencialidad (protección contra la divulgación no autorizada de información), Integridad (protección de modificaciones inadecuadas de la información), Disponibilidad (perdida de acceso al sistema), Autenticidad (identificación inequívoca de los usuarios con acceso al sistema) y Trazabilidad (registro detallado de la totalidad de las acciones acontecidas en el sistema).

Para la ejecución del análisis de riesgos, se ha utilizado la herramienta PILAR basic (Procedimiento Informático Lógico de Análisis de Riesgos) y se ha seguido la metodología Magerit.

Magerit es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada en su momento por el Consejo Superior de Administración Electrónica (sustituido en la actualidad por la Comisión de

Estrategia TIC de la Administración General del Estado) para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información en la Administración Pública Española, pero que puede emplearse por entidades fuera de este ámbito, ya sean corporaciones privadas españolas o extranjeras o por entes públicos de terceros países.

C) Enfoque del análisis de riesgos

Esta metodología de análisis de riesgos se realiza utilizando las directrices de la legislación nacional principalmente el ENS.

Este análisis recomienda medidas de seguridad adecuadas, permitiendo a los administradores tomar decisiones, desde el conocimiento, sobre las iniciativas de seguridad. La metodología aborda los siguientes tipos de controles:

- **Controles de administración**: Gestión del sistema de seguridad de tecnología de la información, y la gestión y la aceptación del riesgo.
- **Controles operacionales**: Métodos de seguridad centrados en mecanismos implementados y ejecutados principalmente por personas, incluyendo todos los aspectos de seguridad física, seguridad de medios de comunicación y controles de inventario.
- **Controles técnicos**: Controles de hardware y software que proporcionan protección automatizada para el sistema o aplicaciones.

D) Análisis de riesgos

Identificación de activos

La primera tarea a realizar a la hora de acometer un análisis de riesgos es la de identificar los activos más importantes que guardan relación con el sistema objeto del estudio.

Entendemos por Activos a los recursos del sistema Sede Electrónica o relacionados con éste, que son necesarios para realizar la función encomendada.

A continuación, se detallan los activos de la información implicados en Sede Electrónica ISFAS, presentados de forma jerárquica y divididos en Activos Esenciales y Activos de la Información.

Activos Esenciales

En un sistema como el de la Sede Electrónica del Organismo 'X', existe información esencial y servicios esenciales que debemos proteger, estos se denominan Activos Esenciales y son los que marcan, en última instancia, las necesidades del sistema de información en materia de seguridad. Estos elementos se constituyen como los más importantes y que por su tipología tienen unos requisitos de seguridad propios, a diferencia de otros elementos cuyos requisitos de seguridad derivan de la información y los servicios que soportan.

En este caso, se describen 5 activos esenciales:

[SF_01] Servicio a usuarios

[SF_02] Servicio a externos

[SF_03] Servicio a ciudadanos

[SI_01] Servicio nóminas a usuarios

[SI_02] Servicio de buzón electrónico

Activos de información

A continuación, se detallan los activos de la información que son titularidad de CAST y que son empleados para la prestación del servicio Sede Electrónica. Estos se han agrupado con la finalidad de reducir la complejidad del análisis.

Esta agrupación se ha realizado siguiendo unos criterios como el de ubicación en la misma instalación, que se encuentre sujetos a las mismas condiciones de operación y funcionamiento, lo que los hace expuestos a las mismas amenazas.

El listado definitivo tras el proceso de agrupación ha quedado recogido en el cuadro que se expone a continuación.

- [E] Equipamiento
  - [SW] Aplicaciones
    - [SW-01] Sede electrónica
  - [HW] Equipos
    - [HW-01] Servidor web
    - [HW-02] Servidor de aplicaciones y componentes
    - [HW-03] Servidor de bases de datos
- [L] Instalaciones
  - [Sala técnica] CPD
- [P] Personal
  - [PE-01] Personal laboral contratado
  - [PE-02] Proveedores

Cada uno de estos tratamientos, considerados como activos o servicios principales se evaluarán con la ayuda de la herramienta PILAR y en ella se establecerán las dependencias de cada activo siguiendo el criterio de la metodología Magerit. Para hacer la valoración se tienen en cuenta las dimensiones de la seguridad de la información, estas son Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad.

A continuación, pasamos a definirlas y a explicarlas pormenorizadamente:

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
¿Qué importancia tendría que el activo no estuviera disponible?
Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves. Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño. La disponibilidad es una característica que afecta a todo tipo de activos. A menudo la disponibilidad requiere un tratamiento por escalones pues el coste de la indisponibilidad aumenta de forma no lineal con la duración de la interrupción, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
¿Qué importancia tendría que los datos fueran modificados fuera de control?
Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

[A] 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. [UNE 71504:2008]
¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio. Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización. Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.
¿Qué importancia tendría que los datos no fueran realmente imputables a quien se cree?
Los datos reciben una elevada valoración desde el punto de vista de autenticidad del origen cuando un defecto de imputación causaría graves quebrantos a la organización. Típicamente, se habilita la oportunidad de repudio. Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante**.**

[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

Abriría las puertas al fraude, incapacitaría a el Organismo para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.
¿Qué importancia tendría que no quedara constancia del acceso a los datos?
Abriría las puertas al fraude, incapacitaría a el Organismo para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

A continuación, se recoge la valoración realizada sobre total de activos, es decir los activos esenciales y los del sistema de información:

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[AARR] Análisis de Riesgos					
[essential] Activos esenciales	[M]	[M]	[M]	[B]	[B]
S [SF-01] Servicio a usuarios	[B]	[M]	[B]	[B]	[B]
S [SF-02] Servicio a externos	[B]	[M]	[B]	[B]	[B]
is [SF-03] Servicio a ciudadanos	[B]	[B]	[M]	[B]	[B]
S [SI-01] Servicio nóminas a usuarios	[B]	[B]	[B]	[B]	[B]
S [SI-02] Servicio de buzón electrónico	[B]	[B]	[B]	[B]	[B]
A [SW-01] Sede electrónica	[B]	[B]	[B]	[B]	[B]
A [HW-01] Servidor web	[B]	[B]	[B]	[B]	[B]
A [HW-02] Servidor de aplicaciones y componentes	[B]	[B]	[B]	[B]	[B]
A [HW-03] Servidor de bases de datos	[B]	[B]	[B]	[B]	[B]
A [Sala técnica] CPD	[M]	[B]	[B]	[B]	[B]
A [PE-01] Personal laboral contratado	[B]	[B]	[B]	[B]	[B]
A [PE-02] Proveedores	[B]	[B]	[B]	[B]	[B]

E) Análisis de Salvaguardas

En este apartado se analizan las salvaguardas aplicadas sobre los activos de la información ya definidos en puntos anteriores. Mediante el análisis de salvaguardas se establecen las medidas de seguridad existentes y su nivel de madurez, así como su nivel de madurez y la previsión de cumplimiento del ENS para cada una de las salvaguardas existentes.

El análisis de las mismas determina el riesgo final existente.

Los niveles de madurez contemplado para cada salvaguarda son:

- **L0-** Inexistente
- **L1-** Inicial/ad hoc
- **L2-** Reproducible, pero intuitivo
- **L3-** Proceso definido
- **L4-** Gestionado y medible
- **L5-** Optimizado

- **Evaluación**

Para entender las siguientes tablas, es necesario entender previamente la leyenda de cada una de las columnas:

- Salvaguarda: Elemento de análisis de cada medida evaluada en el análisis de riesgo.
- R: Un valor en el rango **[null.10]** estimado por PILAR teniendo en cuenta los activos declarados, la valoración en cada dimensión de seguridad y el nivel de riesgo afrontado por esta medida o control.
    a. **(o)-** PILAR considera que es excesivo ("*overkill"*)
    b. **(u)-** PILAR considera que es insuficiente ("*underkill"*)
- **[Actual]**: Situación actual de la madurez de la salvaguarda.
- **[PILAR/ENS]**: Objetivo para el cumplimiento del ENS en cada una de sus salvaguardas.

En este supuesto, todas las salvaguardas se han evaluado en un nivel L1 por encontrarse en una fase inicial.

Análisis de Riesgos

Teniendo en consideración los activos, amenazas y salvaguardas, es posible obtener el riesgo de los sistemas de la información, con las salvaguardas actualmente aplicadas y las que deberían existir una vez aplicadas las salvaguardas recomendadas para el ENS.

F) Leyenda de riesgos

Para entender los siguientes cuadros es necesario conocer los niveles de criticidad proporcionados por la herramienta de análisis de riesgos.

- Riesgo potencial

Este tipo de riesgo determina la criticidad que presentaría el sistema en caso de que no existiera ningún tipo de salvaguarda aplicada.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{3,7}	{3,9}	{3,7}	{1,5}	{2,2}
S [SF-01] Servicio a usuarios	{1,9}	{3,9}	{1,9}	{1,5}	{2,2}
S [SF-02] Servicio a externos	{1,9}	{3,9}	{1,9}	{1,5}	{2,2}
is [SF-03] Servicio a ciudadanos	{1,9}	{2,2}	{3,7}	{1,5}	{2,2}
S [SI-01] Servicio nóminas a usuarios	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
S [SI-02] Servicio de buzón electrónico	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [SW-01] Sede electrónica	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [HW-01] Servidor web	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [HW-02] Servidor de aplicaciones y componentes	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [HW-03] Servidor de bases de datos	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [Sala técnica] CPD	{3,7}	{2,2}	{1,9}	{1,5}	{2,2}
A [PE-01] Personal laboral contratado	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}
A [PE-02] Proveedores	{1,9}	{2,2}	{1,9}	{1,5}	{2,2}

- Riesgo actual

Este riesgo determina el riesgo actual que presenta el sistema, con las salvaguardas aplicadas.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{3,1}	{3,4}	{3,1}	{1,0}	{1,6}
S [SF-01] Servicio a usuarios	{1,4}	{3,4}	{1,4}	{1,0}	{1,6}
S [SF-02] Servicio a externos	{1,4}	{3,4}	{1,4}	{1,0}	{1,6}
is [SF-03] Servicio a ciudadanos	{1,4}	{1,7}	{3,1}	{1,0}	{1,6}
S [SI-01] Servicio nóminas a usuarios	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
S [SI-02] Servicio de buzón electrónico	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [SW-01] Sede electrónica	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [HW-01] Servidor web	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [HW-02] Servidor de aplicaciones y componentes	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [HW-03] Servidor de bases de datos	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [Sala técnica] CPD	{3,1}	{1,7}	{1,4}	{1,0}	{1,6}
A [PE-01] Personal laboral contratado	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}
A [PE-02] Proveedores	{1,4}	{1,7}	{1,4}	{1,0}	{1,6}

- Riesgo objetivo/ENS

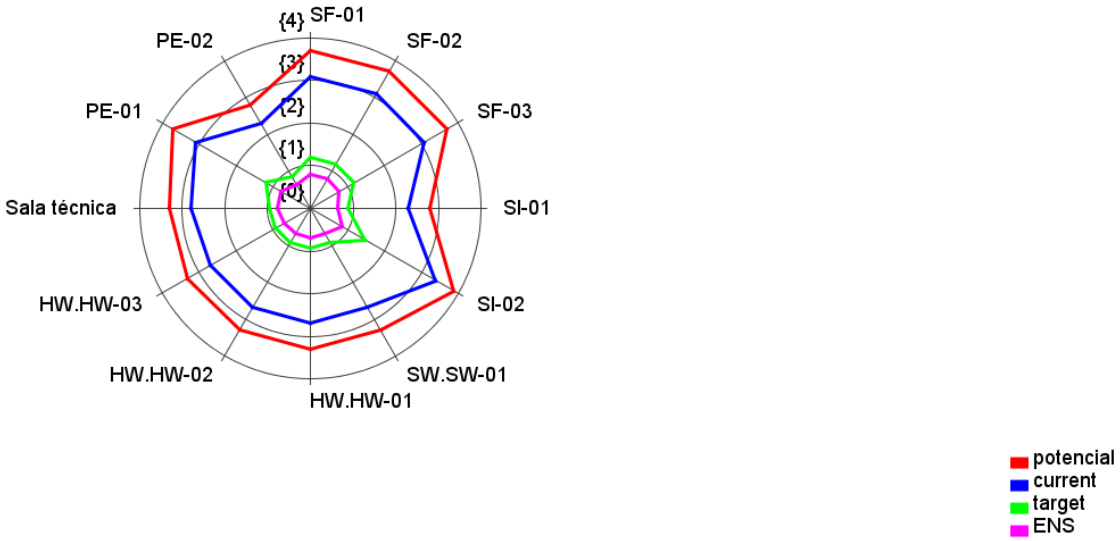
Este riesgo determina la evolución del riesgo teniendo en consideración la aplicación de las salvaguardas que debieran aplicarse dentro del proceso de maduración en materia de seguridad IT de el Organismo, tanto en lo referente a procedimientos, implementaciones técnicas, personal e instalaciones. Se

establece este riesgo en consonancia a lo requerido para el cumplimiento del ENS.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{0,81}	{0,88}	{0,80}	{0,39}	{0,50}
S [SF-01] Servicio a usuarios	{0,45}	{0,88}	{0,45}	{0,39}	{0,50}
S [SF-02] Servicio a externos	{0,45}	{0,88}	{0,45}	{0,39}	{0,50}
is [SF-03] Servicio a ciudadanos	{0,45}	{0,52}	{0,80}	{0,39}	{0,50}
S [SI-01] Servicio nóminas a usuarios	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
S [SI-02] Servicio de buzón electrónico	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [SW-01] Sede electrónica	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [HW-01] Servidor web	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [HW-02] Servidor de aplicaciones y componentes	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [HW-03] Servidor de bases de datos	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [Sala técnica] CPD	{0,81}	{0,52}	{0,45}	{0,39}	{0,50}
A [PE-01] Personal laboral contratado	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}
A [PE-02] Proveedores	{0,45}	{0,52}	{0,45}	{0,39}	{0,50}

- Diagrama de riesgo

El siguiente diagrama muestra la representación del riesgo de forma visual, teniendo en consideración los valores expuestos en los apartados anteriores.



G) Conclusiones

Para concluir el informe procederemos a aclarar e interpretar los resultados obtenidos del análisis.

Cabe destacar que, los resultados obtenidos en el apartado Riesgo Actual muestran una situación preocupante respecto al riesgo del sistema. La mayoría de los valores se encuentran en un valor bajo, medio y alto, lo que revela que el sistema, de por sí, no es seguro si no se le aplica ningún tipo de medida.

El apartado del Riesgo Potencial, nos indica que, actualmente con las medidas que el Sistema tiene implantadas, seguimos encontrándonos bajo un nivel

preocupante de seguridad. Algunos servicios cuentan con un riesgo medio en algunas dimensiones que, tal y como vemos con el apartado de Riesgo Objetivo/ENS se ven prácticamente eliminados con la aplicación de las medidas que el ENS indica.

Por todo ello, puede deducirse que el Sistema de la Sede Electrónica del Organismo ‘X’, actualmente no cuenta con la seguridad necesarias que exige el ENS pero que, aplicando las medidas que éste estipula para un sistema de Categoría Media, se verá suprimido dicho riesgo.

6.5 Anexo V: Normativa interna de uso de medios electrónicos

Normativa interna de uso de medios electrónicos del Organismo ‘X’

Versión	Fecha	Elaborado por:
1.0	31/05/2022	Responsible de Seguridad
Revisado por:	Aprobado por:	Responsable del Proceso
Comité de Seguridad	Comité de Seguridad	Responsible de Seguridad

Control de cambios

Versión	Fecha	Resumen de los cambios producidos
1.0	31/05/2022	Versión inicial

1. OBJETO

El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en el Organismo ‘X’ (en adelante, el Organismo), dentro del alcance señalado en el Esquema Nacional de Seguridad.

La seguridad siempre ha sido un concepto presente en todos los sistemas de gestión de la información. Su implementación no es sencilla, dado que abarca todos los eslabones de la cadena de gestión de la información y requiere de un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende además de que exista en todos los niveles una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el usuario final del sistema (informático y papel), debido en gran parte al desconocimiento de la importancia que tiene la seguridad de la información.

El usuario final necesita, por tanto, ser concienciado y culturizado en materia de seguridad de la información y, al mismo tiempo, debe disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos a su alcance, así como soportes o documentos en papel y, con especial relevancia, en cuanto a preservar la confidencialidad de la información de carácter personal que esté siendo tratada en cumplimiento de la legislación vigente.

El presente documento establece las normas de uso de los dispositivos asignados al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como al acceso y tratamiento de datos de carácter personal, en soporte electrónico y en papel.

Es fundamental que todos los empleados del Organismo que utilizan equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas sean conocedores de esta norma.

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de el Organismo, que resultan de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 331/2022, de 3 de mayo, por el que se regula el

Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS):

- Marco Organizativo- Normativa de Seguridad [org.2];
- Medidas de Protección- Gestión del personal- Deberes y Obligaciones [mp.per.2];
- Medidas de Protección- Protección de los Servicios- Protección del correo electrónico [mp.s.1]

2. ALCANCE

Esta Normativa de Uso de los Sistemas es de aplicación a todo el ámbito de actuación del Organismo, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad del Organismo.

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Organismo, especialmente, el Responsable de Seguridad, los responsables de Sistemas de Información y los propios usuarios internos, como actores todos ellos, en sus respectivas competencias, de la especificación de la normativa de control de acceso, de la implantación técnica de dicha normativa, y del cumplimiento de la misma, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información del Organismo.

3. LEGISLACIÓN Y NORMATIVA APLICABLE

Serán aplicables:

- Real Decreto 311/2022, de 3 de mayo, 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, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), que deroga la anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y posterior reglamento de desarrollo mediante Real Decreto 1720/2007, de 21 de diciembre.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- CCN-STIC-821 Normas de seguridad en el ENS" y el Anexo I de la Guía "CCN-STIC-822" – Procedimientos de seguridad en el ENS".

4. ROLES Y RESPONSABILIDADES

Responsable de la Seguridad	• Elaborar la normativa de uso de los sistemas de información.
Comité de Seguridad	• Aprobar la normativa de uso de los sistemas de información.
Usuarios	• Cumplir con la normativa de uso de los sistemas de información.

5. NORMATIVA INTERNA DE USO DE LOS MEDIOS ELECTRÓNICOS

Obligaciones de la organización

El Organismo facilita a los usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo. Este equipamiento pasará por un proceso de bastionado previo a su entrega.

Dentro de este tipo de equipamiento se encuentran tanto aquellos dispositivos propiedad del Organismo como, excepcionalmente, aquellos otros que ésta haya autorizado para ser utilizados en su infraestructura informática y de comunicaciones.

En el primer caso, los dispositivos son propiedad del Organismo y por tanto no están destinados a un uso personal. Como consecuencia de esto, el Organismo se reserva el derecho de revisar, sin previo aviso, los equipos y el uso de Internet y del teléfono corporativo que esté haciendo cada Usuario, en caso de que existieren indicios de que se está llevando a cabo una utilización indebida. De esta forma el usuario queda informado de que el resultado de los controles efectuados puede ser utilizado para llevar a cabo, en su caso, las actuaciones disciplinarias previstas por la normativa vigente.

Uso de los dispositivos informáticos

Los Usuarios deben cumplir las siguientes medidas de seguridad para el uso del equipamiento informático que se les haya proporcionado para las tareas relacionadas con su puesto de trabajo:

Conexión de otros dispositivos	• No está permitido conectar dispositivos que no estén autorizados a la red del Organismo. • Tampoco se pueden conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente.
Ubicación del dispositivo	• No está permitido variar la ubicación física de los dispositivos asignados a una ubicación.

Configuración del dispositivo	• No está permitido alterar la configuración física, configuración de seguridad ni el software de los dispositivos.
Uso de dispositivos y de la red	• Los dispositivos, así como la red de información que el Organismo pone a disposición de los usuarios están destinados a permitir el desempeño de las funciones y tareas profesionales que estos tienen encomendadas, estando prohibido el uso para otras finalidades de carácter personal, o bien para la realización de actos desleales o que pudieran ser considerados ilícitos.
Antivirus	• El Usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario deberá notificarlo como una incidencia de seguridad.
Uso de la información	• Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otro distinto del servicio al que está destinada. • El Usuario se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de este Organismo en ordenador propio, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de la Seguridad y se adopten las medidas de seguridad correspondiente. Asimismo, los datos contenidos en este tipo de soportes deben ser suprimidos una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte

	informático externo, se deberá restringir el acceso y uso de la información que obra en los mismos. • El Usuario deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de el Organismo y dispuesto a razón única de las funciones o tareas desempeñadas en la misma. Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.
Identificación y autenticación	• Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por el Organismo son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Por cuestiones de seguridad no están permitidas prácticas como: • Emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red de el Organismo. • Intentar modificar o acceder al registro de accesos. • Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros.

Uso de la red corporativa

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los usuarios internos del Organismo a la Intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas

corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Los Usuarios deben cumplir las siguientes medidas para el uso de la red corporativa:

Uso de internet	• La utilización de Internet por parte de los Usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. • El Organismo podrá controlar el uso de acceso a Internet proporcionado. Para ello seguirá un sistema basado en un control de las páginas visitadas, lo que podrá suponer el almacenamiento y control de las cookies que se generen. • La normativa completa sobre el uso de Internet puede consultarse en el • • *Anexo* 2. Normas de uso **de internet** del presente documento.
Uso del correo electrónico	• Se considera el correo electrónico como un instrumento básico de trabajo. • El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones. • Los envíos masivos de información, así como lo correos que se destinen a gran número de usuarios serán solo los estrictamente necesarios que puedan provocar un colapso del sistema de correo.

	• No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. • El Organismo se reserva el derecho de que el Responsable de Seguridad o el Responsable del Sistema pueda revisar y controlar el uso correcto del correo electrónico corporativo. • En caso de ausencia, baja temporal o definitiva, el *Responsable del Departamento* correspondiente podrá consultar su buzón de correo o redireccionar su cuenta con la finalidad de continuar con el normal desarrollo de la actividad de el Organismo. • La normativa completa sobre el uso del correo electrónico puede consultarse en el epígrafe Anexo 1. Normas de uso del correo electrónico del presente documento.
Compartición de contenidos	• Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

Acceso a aplicaciones y servicios

Tanto el equipamiento informático como todos los recursos facilitados al usuario para la realización de las tareas relacionadas con su puesto de trabajo (tales como teléfonos móviles, aplicaciones, servicios, etc.) son propiedad del Organismo, o son propiedad del usuario, pero han sido autorizados para dichos usos, por lo que deberá hacerse un uso diligente de los mismos. En este sentido, podrá revisarse la utilización que cada usuario esté haciendo de los teléfonos móviles facilitados para el desempeño de su puesto de trabajo. En caso de que existieran indicios acerca del uso indebido de los mismos, podrá realizarse un control de la actividad que se considere sospechosa o fraudulenta, así como de la facturación, y de los destinatarios de las llamadas realizadas.

Gran parte de los procedimientos administrativos se gestionan en la actualidad accediendo desde ordenadores personales a aplicaciones que residen en servidores conectados a la red corporativa.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por el Organismo para el uso de aplicaciones y servicios corporativos:

Identificación y autenticación	• Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante *Usuario* y *contraseña*, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
Custodia de las contraseñas	• La custodia de la contraseña es responsabilidad del Usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona. • Las contraseñas no deben anotarse, deben recordarse.
Renovación de las contraseñas	• Las contraseñas deben cambiarse periódicamente. Los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.
Incidencias con las contraseñas	• Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al Responsable de Seguridad, a través de correo electrónico.
Soportes informáticos (*pendrives* y discos duros externos USB, CDs, DVDs, disquetes, etc.)	• La salida de soportes que contengan datos de nivel Medio o Alto fuera de los locales de el Organismo debe ser expresamente autorizada por el Responsable del Tratamiento. Toda salida de soportes deberá además quedar registrada de acuerdo con el PRO-190 Procedimiento de

	transporte y entrada y salida de soportes en el Organismo. • La entrada de soportes que contengan datos personales deberá quedar registrada de acuerdo con el PRO-190 Procedimiento de transporte y entrada y salida de soportes en el Organismo. Asimismo, el soporte deberá ser dado de alta en el inventario de soportes de acuerdo con procedimiento establecido en el Organismo. • Debe evitarse el uso de unidades de almacenamiento de la información externas para uso privado como por ejemplo disquetes, pendrives, discos duros externos, CD-R, DVD-R, etc. • En caso de necesitar desechar un soporte que contenga datos personales, se destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior. El Departamento de Informática cuenta con el equipamiento necesario para destruir la información de forma segura e irreversible. Asimismo, el soporte deberá ser dato de baja del correspondiente inventario.

Ficheros en formato no digital. En relación con los ficheros en soporte o documento papel, el usuario deberá observar las siguientes diligencias indicadas anteriormente con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones del Organismo.

Archivadores o dependencias	• Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros

	elementos que contenga soportes o documentos en papel con datos de carácter personal. • En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada de trabajo o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
Almacenamiento de documentos	• El archivo de la documentación se realizará siguiendo los criterios establecidos por el Organismo, para garantizar su correcta conservación. • Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de el Organismo. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información. • Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de estos. • No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.
Custodia de documentos	• Cuando los documentos en soporte papel no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso. • Guardar todos los soportes o documentos que contengan información de carácter personal en un

	lugar seguro, cuando éstos no sean usados, particularmente, fuera de la jornada de trabajo. • Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes. • Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en las mesas de trabajo, mostradores u otro mobiliario.
Traslado	• En los procesos de traslado de documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubiere datos de carácter personal. • En caso de cambiar de dependencia, en el proceso de traslado de los documentos en soporte papel, se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal. • Si se envían a terceros ajenos al Organismo categorías especiales de datos o datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial, étnico, etc.) contenidos en soporte papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.

	Su envío debe estar autorizado por el Responsable del Tratamiento.
Destrucción	• No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. • A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio que disponga el Organismo.
Registro de accesos	• Se debe mantener un registro de accesos a la documentación con datos de las categorías especiales (Ej: datos sindicales, salud, etc.,) siempre y cuando vayan a ser utilizados por varios usuarios.
Incidencias	• Comunicar con la mayor diligencia posible al Responsable de Seguridad a través de correo electrónico, las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales. • Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel**,** los sucesos siguientes: • Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal. • Uso indebido de las llaves de acceso. • Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal. • Pérdida de soportes o documentos en papel, con datos de carácter personal.

	• Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

Proceso disciplinario

Todos los usuarios de los sistemas de información y de los recursos informáticos del Organismo están obligados a cumplir lo prescrito en la presente Norma Interna de Uso de Medios Electrónicos.

Cualquier incumplimiento de lo indicado en la presente Norma, ya sea de forma intencionada o por una utilización negligente, puede dar lugar a la suspensión temporal o definitiva del uso de los recursos y servicios asignados al usuario, sin perjuicio de la revisión de los hechos concretos en el ámbito de la normativa disciplinaria en el caso de los empleados públicos y, de manera general, de las responsabilidades a que, en su caso, hubiere lugar en materia penal y/o civil.

La valoración de las consecuencias del incumplimiento para el infractor, y las medidas a adoptar serán tomadas de conformidad con las normas que regulan la relación de servicio, funcionarial o laboral entre el Organismo y el Usuario.

6. Anexo 1. Normas de uso del correo electrónico

Objetivo

El objetivo del presente epígrafe es regular el acceso y utilización del correo electrónico (e-mail) por parte de los usuarios de los Sistemas de Información de el Organismo, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de el Organismo, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Organismo, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de el Organismo.

Normas de uso del correo electrónico

Concepto. El correo electrónico es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de el Organismo para el envío y recepción de las comunicaciones mediante el uso de cuentas de correo corporativas. Junto con los mensajes también pueden ser enviados ficheros adjuntos.

Caracteres. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

Especificaciones. El Organismo, consciente de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes especificaciones:

Responsabilidad	• Los usuarios serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por el Organismo. • Los usuarios deberán ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por el Organismo. • Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la correspondiente autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial. • Los mensajes de correo transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.
Uso aceptable	• Como norma general, no se utilizará la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades que cada usuario tiene encomendadas en el Organismo. • La forma y contenidos de los correos enviados por el usuario estarán alineados con las normas éticas y de cortesía marcadas por el Organismo, y en ningún caso se enviarán correos ofensivos, amenazantes o de mal gusto. • El usuario debe mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados, y todos los archivos adjuntos

	almacenados en el equipo o unidad de disco habilitada.
Usos no permitidos que implican un riesgo para la seguridad	• La instalación y uso de cualquier otra aplicación de correo electrónico, así como de una versión diferente de la aplicación homologada que no haya sido autorizada e instalada por el personal técnico autorizado o por el sistema automático de distribución de software oficial a través de Radia o utilidad análoga. • La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva. • El uso no autorizado de servidores propiedad de el Organismo para el envío de correo personal. • El envío masivo de correos publicitarios o de cualquier otro tipo que no guarde relación alguna con las necesidades de negocio de el Organismo. Este hecho, además, puede llegar a ser interpretado como “spamming”. • La divulgación, independientemente del formato en que se encuentren, de correos que revelen datos del directorio o de usuarios pertenecientes a el Organismo, fuera de los límites laborales establecidos por la misma. • En el caso de se requiera enviar un mensaje de correo electrónico a varios destinatarios, se utilizará preferentemente el campo CCO (copia oculta) para introducir las direcciones de correo de los destinatarios, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación

	de todos los destinatarios para confirmar que han sido informados.
Diligencia	• Los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos o de dudosa procedencia no serán abiertos, y menos aún los archivos adjuntos que contengan. Su eliminación debe ser inmediata. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.). • No emplear el correo electrónico como medio de comunicación para enviar o recibir información confidencial o que contenga datos que correspondan a categorías especiales según el RGPD (datos de salud, opiniones políticas, afiliación sindical, religión, convicciones religiosas, origen racial o étnico, vida sexual, datos genéticos o biométricos, orientación sexual). Únicamente, y en aquellos casos en los que sea estrictamente necesario, se utilizará este medio, en cuyo caso, se enviará con las medidas de seguridad apropiadas para cada tipo concreto de información mediante la utilización de un software de cifrado, previa autorización expresa del Responsable del Tratamiento. • En la medida de lo posible, desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos. Del mismo modo, limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.

	• Los navegadores utilizados para acceder al correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados. • Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada. • Desactivar las características de recordar contraseñas para el navegador. • Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
Incidencias	• Los usuarios, con la mayor diligencia posible, deberán comunicar al Responsable de Seguridad y a sus responsables directos sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus.
Monitorización	• El Organismo se reserva el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a el Organismo como responsable civil subsidiario.

7. Anexo 2. Normas de uso de internet

Objetivo

El objetivo de la presente Norma es regular el uso de internet por parte de los usuarios de el Organismo, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de el Organismo, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Organismo, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de el Organismo.

Normas de uso de internet

Con carácter general, los usuarios de el Organismo disponen de acceso corporativo a Internet como herramienta de productividad, conocimiento, apoyo al desempeño y mejora de los sistemas de trabajo y búsqueda de información. Esta herramienta es propiedad de el Organismo, la cual se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

- Seguridad: debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- Volumen del tráfico externo de datos: garantizando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de el Organismo.

- Volumen del tráfico interno de datos: como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- Ética: es ineludible el compromiso que el Organismo debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

Responsabilidad	• Internet es un servicio que el Organismo pone a disposición de su personal para uso estrictamente profesional. • Los usuarios son los únicos responsables de las sesiones iniciadas en Internet con sus credenciales de acceso, y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente Normativa. • El acceso a Internet el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios propiedad de el Organismo, así como a monitorizar y registrar los accesos realizados desde los mismos. En caso de que un usuario considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable directo para que éste gestione el acceso correspondiente.
Usos no permitidos que implican un riesgo para la seguridad	• En ningún caso se modificarán las configuraciones de los navegadores (opciones de Internet) de los equipos ni la activación de servidores o puertos sin la autorización expresa. Todos los equipos que así lo estima el Organismo, ya están configurados para su acceso a Internet.

	• Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de el Organismo. • No se permite el almacenamiento en los equipos de archivos y contenidos personales descargados vía Internet, especialmente aquellos que violen la legislación vigente relativa a Propiedad Intelectual. Los usuarios deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos o de red de el Organismo. • Se prohíbe el uso de Internet mediante los recursos informáticos o de red de la empresa con fines recreativos, así como para obtener o distribuir material violento o pornográfico, o para obtener o distribuir material incompatible con los valores de el Organismo. • El uso de chats o programas de conversación en tiempo real no está permitido. • La descarga de software ejecutable desde internet.
Incidencias	• Cualquier incidente de seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al responsable directo oportuno y al Responsable de Seguridad.

8. MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios de los recursos informáticos y/o sistemas de información de el Organismo deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de Uso de Interno de Medios Electrónicos.

Para su aceptación se ha elaborado el presente modelo de aceptación de la Normativa de uso de medios electrónicos:

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*empleado de el Organismo* _____ *],* como usuario de recursos informáticos y sistemas de información de el Organismo, declara haber leído y comprendido la Normativa de Usos de medios electrónicos del Consorcio Asturiano de Servicios Tecnológicos (*versión x*), y aceptar los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, atender a las modificaciones del documento que le hayan sido debidamente comunicadas, comprometiéndose, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Organización:	Organismo ‘X’
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	