


1

Política de Seguridad de la Información


ORG.01-01 v2.0

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 2 de 67	

Seguridad de la Información


CONTROL DE VERSIONES	
Ámbito de difusión:	Uso público / Todo el personal de la empresa
Responsable	COMITÉ EJECUTIVO

Versión		Autor	Resumen de modificaciones	Revisado	Aprobado
Nº	Fecha				
1.0	20/09/2021	CSI	Creación del documento	CSC	CE
1.1	14/DIC/2021	CSI	Adaptación ART. 11	CSC	CE
2.0	06/MAR/23	CSI	Revisión periódica, adaptación al ENS 2022, Marco legal y objetivos corporativos.	CSC	CE

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 3 de 67	

1 Índice

1	ÍNDICE	3
2	APROBACIÓN Y ENTRADA EN VIGOR	4
3	PROCESO DE DESARROLLO Y APROBACIÓN	5
4	INTRODUCCIÓN	6
4.1	Prevención	9
4.2	Detección	10
4.3	Respuesta	10
4.4	Conservación	11
4.5	Recuperación	11
5	ALCANCE	12
6	MISIÓN Y OBJETIVOS	13
7	MARCO LEGAL	14
8	PROCESO DE IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD	15
9	ORGANIZACIÓN DE SEGURIDAD	17
10	PROCEDIMIENTO DE DESIGNACIÓN	18
11	RESOLUCIÓN DE CONFLICTOS	19
12	SEGREGACIÓN DE FUNCIONES	20
13	CATEGORIZACIÓN DE SISTEMAS	21
14	CATEGORIZACIÓN DE LA INFORMACIÓN	22
15	DATOS DE CARÁCTER PERSONAL	23
16	AUTORIZACIÓN Y CONTROL DE ACCESOS	24
17	PROTECCIÓN DE LAS INSTALACIONES	25
18	MÍNIMO PRIVILEGIO	26
19	INTEGRIDAD Y ACTUALIZACIÓN DE LOS SISTEMAS	27
20	PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO	28
21	PREVENCIÓN ANTE LOS SISTEMAS DE INFORMACIÓN INTERCONECTADOS	29
22	REGISTRO DE ACTIVIDAD Y CÓDIGO DAÑINO	30
23	GESTIÓN DE INCIDENTES DE SEGURIDAD	31
24	CONTINUIDAD DE LA ACTIVIDAD	32
25	MEJORA CONTINUA DEL PROCESO DE SEGURIDAD	33
26	GESTIÓN DEL PERSONAL Y PROFESIONALIDAD	34
27	CONCIENCIACIÓN, FORMACIÓN Y ADIESTRAMIENTO EN CIBERSEGURIDAD	35
28	ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y NUEVOS COMPONENTES	36
29	SEGURIDAD POR DISEÑO Y POR DEFECTO	38
30	ANÁLISIS Y GESTIÓN DE RIESGO	39
31	OBLIGACIONES Y COMPROMISO DE LOS USUARIOS	41
32	TERCERAS PARTES	42
33	ANEXO 1: VALORES CORPORATIVOS	43
34	ANEXO 2: ESTRUCTURA DE SEGURIDAD	45
35	ANEXO 3: GLOSARIO	62
36	ANEXO 4: ABREVIATURAS	67


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 4 de 67	

2 Aprobación y entrada en vigor

Esta política se ha aprobado el día 06/MAR/2023 por el Comité Ejecutivo del Grupo OESIA, para adaptar la Política de Seguridad de la Información a los requisitos del ENS y al manejo de información Clasificada.

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

Este texto anula a la anterior Política que fue aprobada el día 20/12/2021 por el Comité Ejecutivo del grupo Oesía.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 5 de 67	



3 Proceso de desarrollo y aprobación

La Política de Seguridad de la Información será elaborada por el Comité de Seguridad de la Información y revisada por el Comité de Seguridad Corporativa, que será el que la elevará al Comité Ejecutivo para su aprobación formal y posterior difusión a todas las partes afectadas.

La Política de Seguridad de la Información es un documento vivo que estará sujeto a una actualización permanente y a su revisión periódica para ver si se adapta a las necesidades y a la orgánica específica del grupo Oesía.

Será misión del Comité de Seguridad TIC la revisión anual o cuando exista un cambio de impacto de esta Política de Seguridad de la Información, así como la propuesta de revisión o mantenimiento de esta, de forma que se garantice la oportunidad, idoneidad, completitud y precisión de lo que la Política establece.

La Política de Seguridad de la Información deberá estar permanentemente adaptada a las circunstancias técnicas y organizativas del Grupo OESÍA.

Las Políticas de Seguridad de la Información y las Normas de Seguridad serán de uso Público y estarán a disposición de todos los miembros del Grupo OESÍA y externamente a través de la Página WEB del grupo.

Los Procedimientos de Seguridad estarán disponibles para todo el personal al que les afecte y en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Los responsables de cada área del Grupo OESÍA velarán por el cumplimiento de las Políticas, Normas y Procedimientos por parte del personal a su cargo.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 6 de 67	

4 Introducción

El Grupo OESIA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos de negocio. Por lo que la compañía es consciente de que 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.

En este sentido, el Grupo OESÍA ha decidido implantar un Sistema de Gestión de la Seguridad de la Información basado en el Sistema de Gestión de la Seguridad de la Información ISO 27001/27002, y que sea conforme con lo establecido para el cumplimiento del Esquema Nacional de Seguridad (Nivel Medio), que, de forma integral, permita garantizar los siguientes objetivos:

- a) Garantizar la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de la información, tanto en los productos y servicios ofrecidos a los clientes, como en la gestión interna.
- b) Cumplir los requisitos legales, reglamentarios y de los clientes en lo que se refiere a seguridad de la información y como valor añadido en la entrega de productos y servicios, atendiendo estas necesidades de seguridad de la información durante todo su ciclo de vida.
- c) Transmitir confianza a todos los organismos y personas que tienen relación con el Grupo OESÍA.
- d) Establecer las distintas responsabilidades en el cumplimiento de los distintos cometidos y obligaciones relacionadas con la seguridad de la información.
- e) Seguir un proceso de mejora continua.
- e) Atender, desde el punto de vista de la seguridad, a la necesidad de cumplimiento de normas, leyes y estándares, prestando una especial atención a la Seguridad, Protección de Datos, Derechos Laborales y Propiedad Intelectual.

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 fuentes de riesgo para la seguridad.

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 prontitud a los incidentes de seguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 7 de 67	

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución que afecten a la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios.

Para defenderse de estas amenazas, se requiere una estrategia de seguridad 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 marco legal aplicable, 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.

En materia de seguridad de la información todo el Grupo Oesía deberá tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.

b) Gestión de la seguridad basada en los riesgos.

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

c) Prevención, detección, respuesta, conservación y recuperación.

La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección, respuesta y recuperación, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.


Las medidas de prevención deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información y mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

Asimismo, se tomarán las medidas necesarias para garantizar la recuperación en un tiempo razonablemente corto en caso de necesidad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 8 de 67	

d) Existencia de líneas de defensa.

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, que permita desarrollar una reacción adecuada, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

e) Vigilancia continua.

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

f) Reevaluación periódica.


Las medidas de seguridad se reevaluarán y actualizarán periódicamente

g) Diferenciación de responsabilidades.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información. La presente política establece las responsabilidades y los cometidos de las distintas autoridades relacionadas con la Seguridad de la Información del Grupo Oesía.

La presente política materializa el compromiso de la Alta Dirección del Grupo Oesía en materia de seguridad de la información y lo que en ella se expone, es de obligado cumplimiento para toda la organización y se orienta al cumplimiento de los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 9 de 67	

o) Mejora continua del proceso de seguridad.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, producto o servicio del Grupo Oesía, 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 por los distintos departamentos, e incluidos en la planificación de recursos, en las ofertas, y en pliegos de licitación para proyectos del Grupo Oesía.

La ciberseguridad en el Grupo Oesía se articula en las siguientes actividades:

4.1 Prevención

Las áreas del Grupo OESIA deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el marco legal, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la Política de Seguridad de la Información, las distintas Áreas y Responsables del Grupo OESÍA deben:

- Autorizar los sistemas antes de entrar en operación y retirarlos del servicio cuando ya no sean necesarios.
- Asegurarse de que los usuarios entienden y aplican las normas de seguridad y que atienden de forma inmediata y preferente las indicaciones, instrucciones y alertas de ciberseguridad.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Mantener los sistemas permanentemente actualizados y bajo soporte del fabricante.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 10 de 67	

Los sistemas han de disponer de una estrategia de protección en líneas de defensa, constituida por múltiples capas de seguridad dispuestas de forma que cuando una de las capas falle, permita:

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

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

4.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.


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

4.3 Respuesta

Las áreas del Grupo OESIA deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar puntos de contacto para las comunicaciones con respecto a los incidentes de seguridad detectados internamente o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con incidentes. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Incidentes del Grupo Oesía y con los clientes y proveedores cuando corresponda.

Cuando se detecten incidentes o eventos de seguridad se analizarán y se notificará a los usuarios implicados y a sus responsables, para reducir el impacto o la ocurrencia de incidentes similares en el futuro. En el caso de incidentes siempre se elaborará un informe y un documento de lecciones aprendidas para el proceso de mejora continua.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 11 de 67	

4.4 Conservación

Se atenderá con especial cuidado la conservación de la información y los datos durante todo su ciclo de vida.


Es responsabilidad del que la genera o gestiona la información, su adecuada categorización y protección, usando para ello, los mecanismos y procedimientos establecidos.

El ciclo de vida de la información en el Grupo Oesía es el siguiente:

- a) Creación, recepción o captura de la información.
- b) Almacenamiento.
- c) Uso o proceso.
- d) Archivo.
- e) Destrucción.

4.5 Recuperación

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

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 12 de 67	

5 Alcance

Esta Política de seguridad TIC es de aplicación, con carácter obligatorio, sobre todos los sistemas TIC responsabilidad del Grupo OESIA, servicios y procesos de negocio, activos de información y sus dependencias, órganos directivos del Grupo OESIA, personal interno o externo que tenga acceso información o sistemas del Grupo OESIA (con independencia de que exista o no una relación de carácter laboral), empresas que formen o puedan formar parte del Grupo OESIA y, cualquier otra entidad involucrada con el Grupo OESIA en la utilización de su información y sus sistemas.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 13 de 67	

6 Misión y objetivos


La misión del Grupo OESÍA es acompañar a nuestros clientes en su operativa diaria, así como en los procesos de transformación de sus negocios, cumpliendo con sus expectativas y aportándoles valor a través de soluciones tecnológicamente innovadoras en los campos de la ingeniería digital e industrial.

El Grupo OESIA tiene como objetivo su consolidación en el mercado como uno de los grandes impulsores globales de innovación, con una visión de futuro vinculada a sus clientes, a sus profesionales y a la Sociedad. Por ello, ofrece a sus clientes una ventaja competitiva a través de las nuevas tecnologías y de un equipo altamente cualificado. Contribuyendo a que los avances tecnológicos sirvan para construir una sociedad mejor, más justa y segura, mediante el desarrollo de grandes proyectos socialmente responsables.

Una parte integral de esa ventaja competitiva es la ciberseguridad, que, además, se debe prestar como valor un añadido y un elemento diferenciador en todos los productos y servicios que se prestan a los clientes.

A la consecución de estos fines contribuyen los cinco valores desarrollados en el Anexo 1, que imprimen el carácter del Grupo Oesía:

- 1) Confiabilidad.
- 2) Compromiso.
- 3) Aprendizaje continuo.
- 4) Excelencia.
- 5) Innovación

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 14 de 67	

7 Marco legal

El marco legal se revisará cuando sea necesario por la Asesoría Jurídica, o al menos, una vez al año y en caso necesario, se adaptarán los documentos de Sistema de Gestión de Seguridad de la Información conforme a los cambios legislativos aplicables por los departamentos, autoridades o comisiones que correspondan.

La legislación de referencia se mantendrá actualizada en un documento denominado **ORG-01 Marco Normativo**.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 15 de 67	

8 Proceso de implantación del sistema de seguridad

El proceso de implantación de la política se establece a tres niveles mediante, políticas, normas y procedimientos operativos de seguridad que afronten aspectos específicos según el marco legal y regulatorio vigente:

- a) Políticas que son elaboradas por el Comité de Seguridad de Información, revisadas por el Comité de Seguridad Corporativa y son aprobadas por el Comité Ejecutivo.
- b) Las Normas que son elaboradas por el Comité de Seguridad de la Información y son aprobadas por el Comité de Seguridad Corporativa.


Las Normas son documentos que sirven para indicar cómo se debe actuar de manera adecuada, especialmente en el caso de que una cierta circunstancia no esté recogida en un procedimiento específico.

Son el conjunto de regulaciones que desarrollan la política de seguridad y privacidad y tratan de su aplicación. Cada norma deberá:

1. Centrarse en los objetivos que se desean alcanzar, antes que en la forma de lograrlo. Las normas ayudan a tomar la decisión correcta en caso de duda.
2. Describir lo que se considera uso correcto, así como lo que se considera uso incorrecto.
3. Indicar la forma de localizar los procedimientos de seguridad y privacidad que se han desarrollado en la materia tratada.
4. Ser concisa, motivada y descriptiva, y definir puntos de contacto para su interpretación correcta.
5. Explicar cómo actuar ante situaciones anómalas y no previstas.
6. Describir la responsabilidad del personal con respecto al cumplimiento o violación de la norma: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Existe una Normativa general de uso de los sistemas. Esta normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet y en los escritorios de todos los usuarios.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 16 de 67	

c) Los Procedimientos Operativos de Seguridad, que son elaboradas por los Responsables de los Sistemas, con la colaboración del Responsable de Seguridad (CISO) y son aprobadas por el Comité de Seguridad de la Información. Y son el conjunto de documentos que describen explícitamente y paso a paso como realizar una cierta actividad, según las directrices de carácter técnico o procedimental que se deben observar.


Cada procedimiento Operativo de Seguridad debe detallar:

1. En qué condiciones debe aplicarse.
2. Quiénes son las personas que deben llevarlo a cabo.
3. Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada.
4. Cómo se miden y evalúan sus resultados.
5. Cómo se reportan posibles mejoras y deficiencias en los procedimientos.

Además de los documentos citados, la documentación de seguridad y privacidad podrá contar con otros adicionales, como son: alertas, recomendaciones, buenas prácticas, informes, lecciones aprendidas, registros, evidencias electrónicas, etc.

La Política de Seguridad de la Información y de Desarrollo Seguro serán de Uso Público y estará publicada en la Intranet y en la Web del Grupo Oesía.

Tanto las Políticas, como las Normas y los Procedimientos Operativos de Seguridad, son de obligado cumplimiento y deben ser conocidos y estar disponibles para su consulta por aquellas personas que los tienen que aplicar.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 17 de 67	


9 Organización de seguridad

Toda la organización tiene responsabilidades en materia de Seguridad de la Información, con independencia de las figuras y responsables detallados en este apartado.

La organización de seguridad se articula en:

- 1) Comité de Seguridad Corporativa.
- 2) Comité de Seguridad de la Información.
- 3) Responsable de Seguridad Corporativa.
- 4) Responsable de Seguridad de la Información.
- 5) Responsable del Sistema.
- 6) Administrador de Seguridad del Sistema.
- 7) Oficina de Seguridad (OSEG).
- 8) ERI/SOC


Las responsabilidades y funciones de la organización de seguridad se detallan en el Anexo 2.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 18 de 67	

10 Procedimiento de designación


- El responsable de Seguridad Global (CSO) será nombrado por el Comité Ejecutivo.
- El Responsable de Seguridad de la Información (CISO) será nombrado por el Comité Ejecutivo.
- El Responsable de los Sistemas Corporativos (RSIS/AOSTIC) será nombrado por el Comité Ejecutivo.

La Dirección de Operaciones, para el caso de cualquier servicio o producto que se preste electrónicamente y no esté incluido entre los corporativos, designará, cuando se considere necesario, un Responsable del Sistema (RSIS/AOSTIC), o un Responsable de Seguridad de Producto o Servicio, según sea el caso, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política de seguridad de la Información.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 19 de 67	


11 Resolución de conflictos

En caso de tener que solucionar conflictos en lo que se establece en la presente Política, la decisión será tomada por el superior o superiores jerárquicos, que podrán solicitar asesoramiento previo del Comité de Seguridad de la Información.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 20 de 67	

12 Segregación de funciones

En el Grupo Oesía se seguirá el principio de Segregación de funciones, es decir, el responsable de la supervisión de la ciberseguridad debe ser distinto del responsable de la operación del sistema y nadie puede autorizarse a sí mismo, por lo que los roles, perfiles, permisos y privilegios, deben estar bien definidos y delimitados para cada puesto de trabajo.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 21 de 67	

13 Categorización de sistemas

Todos los sistemas del Grupo OESÍA tendrán una categorización (sistemas que manejan información no clasificada), adecuada a la información y servicios que proporcionan. 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:

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Cumplir sus obligaciones diarias de servicio.
- d) Respetar la legalidad vigente.
- e) Respetar los derechos de las personas.

La categorización de los sistemas de información será responsabilidad del Comité de Seguridad de la Información, como órgano colegiado con las competencias del Responsable del Servicio y Responsable de la Información, en base a las dimensiones de confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de la información que manejan.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 22 de 67	


14 Categorización de la Información

La información generada en el Grupo OESÍA, se categorizará por la persona que la genera y siempre se realizará en base a las siguientes categorías y criterios establecidos por el Responsable de la Información, es decir, el Comité de Seguridad de la Información del Grupo OESÍA.

Para el caso de los sistemas de información, la categorización de la información será responsabilidad del Comité de Seguridad de la Información, como órgano colegiado que tiene las competencias de Responsable de la Información, para lo que establecerá unos criterios de categorización.


Toda información en soporte papel y en soportes informáticos se etiquetarán adecuadamente en base a su categorización para facilitar su uso, manipulación y protección.

Del resultado de la categorización en base a las dimensiones de confidencialidad, integridad y disponibilidad, trazabilidad y autenticidad de la información, se calculará su nivel de criticidad, que será BAJO, MEDIO o ALTO.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 23 de 67	

15 Datos de carácter personal

El Grupo OESIA trata datos de carácter personal. El Registro de Actividades de Tratamiento (RAT), al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información del Grupo OESIA se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado RAT.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 24 de 67	

16 Autorización y control de accesos

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Para ello, todo el personal que acceda a las instalaciones del Grupo OESÍA deberá estar debidamente autorizado, identificado y registrado.

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 25 de 67	

17 Protección de las instalaciones

Los sistemas se instalarán en áreas separadas (CPD y clientes), y estarán dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Además, los CPD contarán con las medidas de protección contra inundación, alimentación, contra la intrusión, de control ambiental, control de emisiones radioeléctricas o contra incendios, que garanticen la continuidad de negocio y adecuadas a la información a manejar.

Las zonas de trabajo se clasificarán adecuadamente en función de la información a manejar en las mismas y contarán con las medidas de protección adecuadas a la información a manejar.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 26 de 67	

18 Mínimo privilegio

Los usuarios y administradores contarán con los mínimos privilegios que sean necesarios para hacer su trabajo. En caso de que un usuario necesite un mayor privilegio, de forma temporal o permanente, lo solicitará mediante CAU para su estudio o autorización si procede. En cuanto dejen de ser necesarios los privilegios serán retirados a la mayor brevedad.

Hay que tener en cuenta, que un mayor nivel de privilegio también requiere una mayor responsabilidad y conocimientos por parte de la persona que lo solicita.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, atendiendo especialmente lo siguiente:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. 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.
- d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 27 de 67	

19 Integridad y actualización de los sistemas

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema, lo que se materializará en un CAU.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación con 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 este. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Todo el software y el hardware deberá estar actualizado con los últimos parches de seguridad, debidamente licenciado y con soporte del fabricante. Se mantendrá un adecuado control y gestión de la obsolescencia, para lo que las distintas áreas del Grupo OESÍA establecerán en sus presupuestos las necesidades de mantenimiento de licencias de software y de mantenimiento y sustitución de hardware.

En el caso de tener que mantenerse obsolescencia por requisitos del servicio, cliente o del producto, se tomarán las medidas compensatorias que se consideren más adecuadas. En todo caso se valorará el coste y los riesgos de mantener la obsolescencia en los sistemas y siempre que sea posible, se llevarán a cabo planes de gestión o de eliminación de esta.

La gestión de la obsolescencia es especialmente crítica en los entornos de desarrollo, para lo que se elaborará una Política de Desarrollo Seguro y se formará al personal que lo requiera en las buenas prácticas y en el desarrollo seguro.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 28 de 67	

20 Protección de la información almacenada y en tránsito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles o móviles, los asistentes personales (PDA), los dispositivos periféricos, los soportes de información y comunicaciones sobre redes abiertas o con cifrado débil, que deberán analizarse especialmente para lograr una adecuada protección de la información. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las administraciones públicas en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el Real Decreto del ENS, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de éstos.


Se establecerá un procedimiento de sanitización y destrucción de soportes de información conforme a la normativa aplicable y guías del CCN en función de los distintos tipos de información. También se elaborará un procedimiento de categorización de la información, para permitir el tratamiento adecuado de la misma por parte de todos los miembros de la organización.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 29 de 67	

21 Prevención ante los sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el Art. 13 de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones. 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.

Se elaborará un modelo de interconexión compatible con el ENS, para la conexión de los sistemas con otros sistemas de clientes o proveedores y con otras sedes o socios. Dicho modelo tendrá en cuenta la conectividad mínima necesaria, los mecanismos de cifrado, el aislamiento, la segmentación y la anonimización de redes, así como los mecanismos de monitorización y de protección perimetral que sean necesarios. En la medida de lo posible, se aplicarán criterios de ZeroTrust o alternativamente, de mínimos privilegios.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 30 de 67	

22 Registro de actividad y código dañino

Con la finalidad exclusiva de lograr el cumplimiento del ENS y sobre la base de un interés legítimo y proporcionado, 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, se registrarán las actividades 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.

Todos los sistemas del Grupo Oesía, sean físicos o virtuales, estarán protegidos contra el código dañino mediante las aplicaciones y sistemas de seguridad que sean necesarios.

Todos los archivos de procedencia externa serán revisados antes de ser usados.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 31 de 67	

23 Gestión de incidentes de seguridad

Se establecerá un sistema de detección, monitorización y reacción frente a código dañino 24/7.

Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán 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.

Dicha gestión de incidentes será acorde con la documentación aplicable del CCN y la Guía Nacional de Notificación y Gestión de Ciberincidentes.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 32 de 67	

24 Continuidad de la actividad

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 elaborará un procedimiento de gestión de copias de seguridad y un plan de continuidad de negocio.

Asimismo, para los servicios críticos, se considerará tanto la necesaria redundancia como la deseable resiliencia, entendiendo como tal la posibilidad de seguir operando en un entorno degradado. Como mínimo en los sistemas críticos se considerará la alta disponibilidad y comunicaciones redundantes.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 33 de 67	

25 Mejora continua del proceso de seguridad

En este sentido, el Grupo OESÍA deberá reevaluar y actualizar las medidas de seguridad periódicamente, adecuando su eficacia a la evolución de los riesgos y sistemas de protección, bien por la aparición o incremento de los riesgos o bien en cumplimiento de la normativa vigente sobre un modelo de mejora continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Este proceso se basará en el conocimiento de la amenaza, de las debilidades observadas y en el análisis y lecciones aprendidas obtenidas de eventos e incidentes de seguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 34 de 67	

26 Gestión del personal y profesionalidad

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

Se llevará a cabo una adecuada caracterización del puesto de trabajo, teniendo en cuenta las obligaciones, los perfiles y la adecuada verificación de antecedentes en la contratación.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Se dispondrá de un procedimiento sancionador orientado al incumplimiento de las medidas de seguridad, que será conforme a la legislación aplicable, convenio colectivo en vigor y Estatuto de los Trabajadores, que deberá ser conocido por todo el personal de la empresa.

También se dispondrá de una normativa de puesto de trabajo despejado, así de los medios necesarios para que sea llevada a cabo.

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Grupo OESÍA.

Se exigirá, de manera objetiva y no discriminatoria, el disponer de profesionales cualificados para prestar los servicios relacionados con el ENS en el Grupo OESÍA, con unos niveles idóneos de gestión y madurez, atendiendo especialmente a los que se prestan a administraciones públicas.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 35 de 67	

27 Concienciación, formación y adiestramiento en ciberseguridad

Todo el personal del Grupo OESÍA seguirá un plan anual obligatorio de concienciación, formación y adiestramiento en ciberseguridad, sobre un esquema de formación continua y mejora de la ciberseguridad.

Se entiende como:

- a) Concienciación, la sensibilización al problema de la ciberseguridad. Está orientada a la organización.
- b) Formación, la adquisición de habilidades básicas de ciberseguridad para el desarrollo de sus competencias profesionales. Está orientada al puesto de trabajo y a los cometidos de la persona que lo ocupa.
- c) Adiestramiento, la puesta a prueba y valoración de las habilidades básicas de ciberseguridad mediante simulacros, ejercicios o supuestos prácticos. Está orientada a la organización o a grupos de usuarios dentro de la misma.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 36 de 67	

28 Adquisición de productos de seguridad y nuevos componentes

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por el Grupo OESÍA se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que 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 (CISO).

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema sujetos al ENS, mediante Acuerdos Operacionales de Servicio (OLA) con el Área de Compras. Proceso que:


- a) Atenderá a las conclusiones del análisis de riesgos.
- b) Será acorde a la arquitectura de seguridad escogida.
- c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Para la contratación de servicios de ciberseguridad se estará a lo dispuesto en los apartados anteriores y lo relativo a la profesionalidad del personal.

Se elaborará una norma de Gestión de Riesgos de Proveedores y un Anexo de Seguridad de la Información para los contratos. Los contratos se valorarán también por el nivel de seguridad del proveedor y se podrán establecer Sistemas de Gestión de la Seguridad de la Información y de mejora continua de la ciberseguridad con los proveedores críticos para la continuidad del negocio o que se conecten a la infraestructura del Grupo OESÍA.

Cuando proceda, se establecerán SLA en los contratos y los destinatarios del servicio comprobarán que se están cumpliendo dichos SLA y si fuera necesario por la criticidad del servicio, se comprobará mediante simulaciones o pruebas, que dichos SLA son los adecuados y se pueden cumplir.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 37 de 67	

En la adquisición de nuevos componentes debe:

- a) Tener en cuenta el análisis de riesgos.
- b) Ajustarse a la arquitectura de seguridad.
- c) Prever los recursos necesarios, esfuerzo y medios económicos y humanos para:
 - a. La implantación inicial.
 - b. El mantenimiento a lo largo de su vida útil.
 - c. Atender a la evolución de la tecnología.
 - d. En todo momento se atenderá tanto a las necesidades técnicas como a la necesaria concienciación y formación de las personas que van a trabajar con los componentes.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 38 de 67	

29 Seguridad por diseño y por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por diseño y por defecto y para que faciliten la gestión de ésta durante todo su ciclo de vida.

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

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, máquinas de salto y puntos de acceso o equipos facultados.

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, en especialmente las de desarrollo.

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.

Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 39 de 67	

30 Análisis y Gestión de riesgo

Cada área del Grupo OESÍA que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propio análisis y gestión de riesgos.

Todos los sistemas sujetos a esta Política de Seguridad de la Información deberán disponer de su correspondiente Análisis de Riesgos, evaluando las amenazas y los riesgos a los que están expuestos, como base para la adecuada selección de las salvaguardas necesarias, optimizando así, el coste beneficio.

Este análisis se revisará regularmente:


- Al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambie la arquitectura de la red o los servicios prestados.
- Cuando cambien de forma sustancial los procesos internos.
- Cuando se actualicen las herramientas de análisis de riesgo.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, se empleará alguna metodología reconocida internacionalmente.

La gestión de riesgos en el Grupo Oesía se realizará mediante la metodología Magerit y todas las decisiones en relación con configuración, tecnologías y salvaguardas de seguridad, se basarán en el resultado del análisis de riesgo (no formal, semiformal o formal, según corresponda) y al cumplimiento efectivo de los controles de seguridad del ENS.


Las medidas adoptadas para mitigar o suprimir los riesgos, deberán estar debidamente justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejada y los diferentes servicios prestados.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 40 de 67	

El Comité de Seguridad de la Información dinamizará las necesidades de recursos trasladadas por los RSIS/AOSTIC de todos los sistemas para atender a las necesidades de seguridad de éstos, promoviendo las inversiones de carácter horizontal.

En la implementación de salvaguardas se considerará la aplicación de tecnología, la implantación de Procedimientos Operativos de Seguridad, la aceptación de riesgos de baja ocurrencia y bajo impacto o la externalización de los riesgos, según proceda y los recursos disponibles. Por lo general ante los riesgos muy altos o altos siempre se debe aplicar tecnología para evitar el impacto del fallo humano, en los riesgos medios y bajos se puede considerar la aplicación de Procedimientos Operativos de Seguridad o la externalización de éstos. En ningún caso, la externalización se podrá considerar como sustituto de otras salvaguardas y siempre como un complemento a éstas

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 41 de 67	

31 Obligaciones y compromiso de los usuarios


Todos los miembros del Grupo OESÍA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, Normativa y Procedimientos de Seguridad que le afecten, siendo responsabilidad del Comité de Seguridad Corporativa el disponer de los medios necesarios para que la información llegue a los afectados y de sus responsables, y que el personal a su cargo los conozca y apliquen adecuadamente.

Todos los miembros del Grupo OESÍA tienen la obligación de atender de forma prioritaria y diligente las alertas de seguridad y las instrucciones que reciban de los responsables de seguridad de la organización.

Todos los miembros del Grupo OESÍA recibirán concienciación y/o formación de forma anual y llevarán a cabo ejercicios de adiestramiento para comprobar que la concienciación y formación ha sido asimilada adecuadamente. Se establecerá un programa anual de formación continua en ciberseguridad que será obligatoria para todos los miembros de la organización.

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 la responsabilidad de dicho puesto, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Todos los correos de alertas de ciberseguridad son prioritarios y sus indicaciones de obligado cumplimiento a la mayor brevedad por parte de todo el personal de la empresa, por lo que los responsables con personal a su cargo deben velar por el conocimiento y cumplimiento inmediato de las medidas y recomendaciones contempladas en dichos mensajes, por parte de todo el personal que dependa de ellos. Los usuarios asumirán las responsabilidades del incumplimiento ante cualquier medida urgente que tenga impacto en la ciberseguridad, en el caso de materializarse un incidente por el incumplimiento de ésta.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 42 de 67	

32 Terceras partes

Cuando el Grupo OESIA preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para informe y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

La seguridad y la calidad de los productos y servicios es prioritaria.

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

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

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 43 de 67	

33 ANEXO 1: VALORES CORPORATIVOS

A la consecución de los objetivos corporativos contribuyen los cinco valores que imprimen el carácter del Grupo Oesía:

Confiabilidad

“Todo lo que diga una persona del Grupo, se cumple”.

Si estamos proporcionando productos y servicios de Tecnologías de la Información y las Comunicaciones, que requieren el cumplimiento de normativas y compromisos diversos en el área de ciberseguridad, es obligación de todo el personal del Grupo Oesía, que el cumplimiento de esas normativas y compromisos con los clientes sea una realidad demostrable y se mantenga adecuadamente en el tiempo.

Compromiso

“Todas las acciones del Grupo Oesía se realicen dando lo mejor de las personas”.

Para que una organización sea cibersegura, es necesario que todas las personas de la organización se impliquen y realicen su trabajo diario teniendo en cuenta los procedimientos y normativas de ciberseguridad ya que usan la tecnología para realizar su trabajo diario, o para el desarrollo de productos y servicios para los clientes.

Debe ser compromiso de todo el personal del Grupo Oesía el evitar errores, aumentar los conocimientos en ciberseguridad, interesarse por las buenas prácticas de ciberseguridad y conocer los riesgos a los que nos enfrentamos en el ciberespacio.

Aprendizaje continuo

“Todas las personas del Grupo Oesía y toda la organización, tengan un conocimiento constantemente actualizado de su especialidad”.

El conocimiento de ciberseguridad, al nivel que nos corresponda en la organización, es una necesidad transversal para la organización ya que todo el personal usa la tecnología para llevar a cabo su trabajo diario. La rápida evolución de las ciberamenazas y de las tácticas, técnicas y procedimientos de los atacantes, hace necesario y vital para la supervivencia de la organización y el mantenimiento de sus beneficios, el desarrollo de un proceso de aprendizaje continuo en ciberseguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 44 de 67	

Excelencia

“Que todo lo que se hace en el Grupo Oesía alcance la máxima calidad en todas las vertientes.”

No cabe duda, que cuanto mayor sea nuestro conocimiento y excelencia a la hora de tratar los temas relacionados con la ciberseguridad, mucho más complicado le estamos poniendo a un posible adversario el poder realizar un ataque con éxito a nuestra organización.

Muchas veces, los pequeños detalles, la mejora continua en las configuraciones de seguridad, la diligencia en las actualizaciones de los sistemas, o el exacto cumplimiento de los cometidos y responsabilidades en materia de ciberseguridad, permiten tener un elevado grado de excelencia en ciberseguridad como elemento diferenciador y de valor añadido para todos los productos y servicios del Grupo Oesía.

Innovación

“Todos los productos y servicios del Grupo Oesía, serán concebidos para marcar la última frontera del desarrollo en sus respectivos sectores.”

A todo el personal que trabaja con la tecnología, no se le es ajeno que, con la evolución de la tecnología y las amenazas en el mundo cibernético, hay un enorme campo para la innovación en productos y servicios orientados a la ciberseguridad y al uso seguro de las tecnologías de la información y telecomunicaciones.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 45 de 67	

34 ANEXO 2: ESTRUCTURA DE SEGURIDAD

Comité de Seguridad Corporativa

Composición:

Presidente:

- ASTIC de OESÍA (Dirección Corporativa de Finanzas y Control).

Secretario:

- CSO.

Vocales:

- OSI
- CISO
- DPO
- Director de Seguridad Física.
- Director Oficina Técnica COO.
- Director de Infraestructura.
- Director de Fabricación.
- Director de Talento.
- Director Jurídico.
- Director de Calidad.

Adicionalmente, se podrá convocar por el Secretario al personal que se considere necesario en función de los temas a tratar.


Se reunirán al menos una vez cada 6 meses, revisando al principio de la reunión los temas pendientes de reuniones anteriores.

El Secretario levantará acta de la reunión y de las acciones acordadas indicando los responsables de su ejecución y la fecha límite para su ejecución, si procede.


También se reunirán cuando las circunstancias así lo aconsejen, o a petición de cualquiera de sus miembros.

Cometidos:

- Coordinar todas las funciones de seguridad de la Organización en las áreas de SEGINFOSIT, SEGINFOPER, SEGINFODOC, SEGINFOINS, SEGINFOEMP.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Coordinar los planes de continuidad de las diferentes áreas para asegurar una actuación sin fisuras en el caso de que deban ser activados.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 46 de 67	

- Revisar la Política de Seguridad Corporativa elaborada, y elevarla para su aprobación por la Alta Dirección.
- Elaborar las Normas de Seguridad de obligado cumplimiento.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los Responsables de Seguridad (física y lógica) se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Atender a las inquietudes de la Alta Dirección y transmitírselas a los Responsables de Seguridad.
- Recabar respuestas y soluciones de los Responsables de Seguridad que, una vez coordinadas, serán notificadas a la Alta Dirección.
- Recabar de los Responsables de Seguridad informes regulares del estado de la seguridad de la Organización y de los posibles incidentes. Estos informes se consolidarán y resumirán para la Alta Dirección.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad de las distintas Áreas.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de funciones.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 47 de 67	

Comité de Seguridad de la Información

Composición:

Presidente:

- CSO

Secretario:

- CISO

Vocales:

- DPO
- Director de Arquitectura y Medios.
- Director de Proyectos TIC.
- Director de proyecto del Plan Permanente de Seguridad y/o responsable de la Oficina Técnica de Seguridad.
- Jefe del SOC.
- AOSTIC's (RSIS) de los sistemas.

Adicionalmente, se podrá convocar por el Secretario al personal que se considere necesario en función de los temas a tratar.

Se reunirán al menos una vez cada 6 meses, revisando al principio de la reunión los temas pendientes de reuniones anteriores.


El Secretario levantará acta de la reunión y de las acciones acordadas indicando los responsables de su ejecución y la fecha límite para su ejecución, si procede.

También se reunirán cuando las circunstancias así lo aconsejen, o a petición de cualquiera de sus miembros.

El Comité de Seguridad de la Información informará al Comité de Seguridad Corporativa mediante el envío de las Actas correspondientes al Secretario del mismo.


Cometidos:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos trasladadas por la ASTIC o el CSO.
- Informar regularmente del estado de la seguridad de la información a la ASTIC.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Colaborar con el Comité de Seguridad Corporativa en la elaboración y evolución de la Organización en lo que respecta a seguridad de la información.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 48 de 67	

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para elevarla al Comité de Seguridad Corporativa.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Proponer para su aprobación por el Comité de Seguridad Corporativa las Normas de Seguridad que sean necesarias.
- Aprobar los Procedimientos Operativos de Seguridad.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar la propuesta de planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar 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 TIC 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Definir el alcance y las necesidades del Plan de Seguridad Corporativa, para solicitar los recursos necesarios al Comité Ejecutivo.
- Este Comité, como órgano colegiado, asumirá las funciones de Responsable de la Información y Responsable del Servicio en el marco del ENS.

Como Responsable de la Información, el Comité de Seguridad de la Información, tendrá la potestad de determinar los niveles de seguridad de la información y para ello recabará la opinión del CISO y


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 49 de 67	

del Responsable del Sistema. Asimismo, como "information owner", el Comité de Seguridad de la Información, tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

Como Responsable del Servicio, el Comité de Seguridad de la Información tiene la potestad de establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los distintos servicios y para ello, recabará la opinión del CISO y del Responsable del Sistema.

El Comité de Seguridad de la Información, es responsable de la determinación de los tipos de información que se van a manejar y de la clasificación de los servicios que se van a prestar (Categorización del Sistema).

Definidos los tipos de información y los servicios, el Comité de Seguridad también establecerá los niveles de seguridad recomendados para cada uno de los tipos de información y servicios. La valoración puede ser propuesta por el Responsable del Sistema, o por el Responsable de Seguridad y será aprobada por Comité de Seguridad de la Información, como Responsable de la Información y del Servicio, si se considera adecuada dicha valoración.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 50 de 67	

Responsable de Seguridad Corporativa (CSO)


Este rol lo asume el Director de Seguridad Global (CSO) del Grupo OESÍA.

Responsabilidades:

- Actúa como Secretario del Comité de Seguridad Corporativa.
- Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.
- Escucha las inquietudes de la Alta Dirección y de los responsables de seguridad y las incorpora al orden del día para su discusión en las reuniones del Comité de Seguridad Corporativa.
- Es responsable, junto con los diferentes Responsables de Seguridad, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad Corporativa y proponiendo las medidas oportunas de adecuación al nuevo marco.
- Es el responsable de la toma de decisiones del día a día entre las reuniones del Comité de Seguridad Corporativa. Estas decisiones serán respuesta a propuestas de los responsables de seguridad, velando por la unidad de acción y la coordinación de actuaciones, en general y en especial en caso de incidencias que tengan repercusión fuera de la Organización y en caso de desastres.
- En caso de desastre se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización.

Tareas:

- Tener una visión de negocio que comprenda los riesgos que afronta el Grupo OESÍA y cómo tratarlos.
- Entender la misión y los objetivos de negocio y asegurarse de que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos.
- Comprender las necesidades normativas, la gestión de la reputación del Grupo OESÍA y las expectativas de los clientes.
- Coordinar todas las funciones de seguridad del Grupo OESÍA.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos del Grupo OESÍA.
- Coordinar los planes de continuidad de las diferentes áreas de la compañía, para asegurar una actuación sin fallos en caso de que deban ser activados
- Coordinar y elevar las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose de gestionar, controlar y presentar regularmente el progreso de

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 51 de 67	

los proyectos y anuncio de las posibles desviaciones al Comité de Seguridad Corporativa. Recibir las inquietudes en materia de seguridad de la Alta Dirección del grupo OESÍA y transmitir las a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, se comunicaran a la Alta Dirección.


- Recabar del Responsable de Seguridad de la Información (CISO) informes regulares del estado de la seguridad de la organización y de los posibles incidentes, a fin de comunicarlos al Comité de Seguridad Corporativa.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 52 de 67	


Responsable de Seguridad de la Información (RSEG/CISO)

Responsabilidades:

- Actuar como Secretario del Comité de Seguridad de la Información del Grupo OESÍA.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Definir la estrategia de seguridad y orientar los objetivos en relación con la consecución de los objetivos de la organización.
- Solicitar la acreditación de cada sistema que maneje información clasificada y, en su caso, su renovación.
- Garantizar que la seguridad sea parte del proceso de planificación de la información y un requisito más del negocio.
- Desarrollar el Plan Anual de Seguridad en coordinación con las distintas áreas y responsables del Grupo.
- Asegurar el desarrollo y la aplicación de la política de seguridad global, normas, directrices y procedimientos para garantizar el mantenimiento continuo de la seguridad de la información y la protección de activos.
- Formular y conducir la elaboración de los documentos normativos de gestión para el ordenamiento y mejora de las acciones a desarrollar por el resto de las áreas.
- Definir la arquitectura de seguridad de red, acceso a la red y las políticas de monitorización.
- Formular el presupuesto anual de la unidad y evaluar su ejecución
- Dirigir el Proceso de desarrollo de Políticas y Normativas de Uso y de Servicios.
- Establecer, revisar, aprobar y mantener actualizada, junto con el Comité de Seguridad Corporativa, y el Comité de Seguridad de la Información, la Política de Seguridad de la Información de la organización y las responsabilidades generales en materia de seguridad de la información en cada área de la organización.
- Estar a cargo de la planificación de respuesta de incidentes.
- Supervisar los incidentes relativos a la seguridad.
- Supervisar los cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes.
- Investigar y/o valorar y aprobar las principales iniciativas para el incremento del nivel de seguridad de la información.
- Evaluar la pertinencia y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Trabajar con el resto del personal ejecutivo para dar prioridad a las iniciativas de seguridad y el gasto sobre la base de la gestión del riesgo apropiadas.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 53 de 67	

- Dirigir y supervisar permanentemente las actividades de la unidad con el objeto de establecer medidas de mejora continua.
- Colaborar con el personal consultor externo según corresponda respecto a las Auditorías de Seguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 54 de 67	

Tareas:

- Dirigir y priorizar las tareas de la oficina de seguridad (OSEG).
- Dirigir la actividad del Centro de Operaciones de Ciberseguridad (CoCS) en lo referente a los servicios corporativos.
- Marcar las directrices funcionales del equipo de Respuesta a Incidentes de Seguridad (ERI).
- Aprobar, en coordinación con los Responsables de los Sistemas (RSIS/AOSTIC), el Concepto de Operación (CO) de cada sistema en sus aspectos de Seguridad de las TIC.
- Verificar que las medidas de seguridad establecidas en la documentación de seguridad sean adecuadas para la protección de la información que se va a manejar en el sistema, satisfaciendo, además, los requisitos de protección establecidos por la normativa vigente.
- Revisar la documentación relacionada con la seguridad del sistema: Declaración de Aplicabilidad (DA), Procedimientos Operativos de Seguridad (POS), Análisis de Riesgos y Seguridad Criptológica.
- Verificar la implementación de los Procedimientos Operativos de Seguridad (POS) y de las funciones de seguridad de los sistemas, mediante la realización de verificaciones de seguridad periódicas.
- Realizar el seguimiento, en conjunción con el Centro de Operaciones de Ciberseguridad (CoCS), del estado de seguridad de los sistemas proporcionado por las herramientas de monitorización, gestión de eventos de seguridad y otros posibles mecanismos de vigilancia implementados en el sistema.
- Diseñar en coordinación con el Centro de Operaciones de Seguridad (CoCS) los planes de respuesta ante incidentes de seguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 55 de 67	

Responsable de Seguridad Física (RSF)

Este rol asume la responsabilidad sobre la seguridad física de la organización, pudiendo designarse más de uno en organizaciones con Zonas de Acceso Restringido (ZAR) en emplazamientos distribuidos geográficamente; en ese caso, se nombrará un coordinador de entre todos ellos.

Funciones

Las funciones del Responsable de Seguridad Física (RSF) podrán ser las siguientes:

- a) Supervisar los emplazamientos y especialmente de las Zonas de Acceso Restringido (ZAR), en lo que respecta a sus medidas de seguridad física y al control de acceso de personas y equipamiento.
- b) Mantenimiento actualizado de la lista de usuarios autorizados a acceder a las diferentes áreas y verificación de su adecuación comparándola con el registro de entradas y salidas de personas.
- c) Comprobar regularmente el estado de seguridad en dependencias, emplazamientos y especialmente Zonas de Acceso Restringido (ZAR).
- d) Supervisión de todas las acciones que se lleven a cabo sobre el equipamiento del área (instalación, modificación, retirada, destrucción, etc.), junto al control y registro de sus entradas y salidas. Se comprobará previamente que las acciones están autorizadas y que, durante el desarrollo de estas, la seguridad del sistema no se vea comprometida.
- e) Atender a las relaciones con las Fuerzas y Cuerpos de Seguridad del Estado, en el ámbito de su competencia.
- f) Colaborar con el CISO y CSO en la investigación de incidentes en los que es relevante el factor humano (insider, sabotaje, espionaje industrial, etc).
- g) Elaborar el Plan de Seguridad física de las instalaciones.
- h) Coordinar con la Dirección de Servicios Generales y los Jefes de Seguridad, las necesidades de seguridad física de las instalaciones.


	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 56 de 67	

Responsable del Sistema (RSIS/AOSTIC)

El Director de Infraestructura y Sistemas TIC del Grupo OESÍA es el RSIS de todos los sistemas corporativos, mientras que para los proyectos para los que se considere necesario por su entidad, normativa a cumplir o seguridad requerida por el cliente, los RSIS serán nombrados por la DA Operaciones. Hay que señalar que el RSIS es un cargo operativo no técnico que se encargará de todo lo relacionado con la gestión necesaria para mantener la seguridad del sistema o del proyecto.

Responsabilidades:

- Identificar y valorar las necesidades relacionadas con la seguridad del sistema o proyecto.
- Coordinar con el resto de las áreas del Grupo OESÍA, los apoyos y la financiación necesaria para mantener la seguridad del sistema o proyecto, las certificaciones de seguridad y los requisitos de seguridad requeridos por los clientes. Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, establecer sus especificaciones para el cumplimiento los objetivos y la verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del sistema, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de nuevos equipos y usuarios en el sistema.
- Decidir las medidas de seguridad que aplicarán los proveedores de componentes del sistema o colaboradores externos durante las etapas de desarrollo, instalación, operación y prueba de este.
- Implantar y controlar conforme a las directrices y en coordinación con el Responsable de Seguridad de la Información (CISO), las medidas específicas de seguridad del sistema y que éstas se integren adecuadamente dentro del marco general de seguridad, incluyendo la determinación e implementación de las configuraciones autorizadas de hardware y software a utilizar en el sistema y sus modificaciones.
- Llevar a cabo el proceso formal de análisis y gestión de riesgos en el sistema. Resultado de éste es la declaración de Requisitos de Seguridad (DRES), también designada como declaración de aplicabilidad (DA), para su aprobación.
- Elaboración de la documentación de seguridad del sistema para su aprobación.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
- Velar por el cumplimiento de las obligaciones asignadas a los Administradores de Seguridad del Sistema (ASS) y los Usuarios Privilegiados del mismo.
- Apoyar al CISO en la investigación de los incidentes de seguridad que afecten al sistema.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 57 de 67	

Tareas:

- Elaborar los Procedimientos Operativos de Seguridad.
- Elaborar en colaboración con el CISO los planes de mejora de la seguridad.
- Elaborar los planes de continuidad.
- Decidir sobre la suspensión temporal del servicio, si las condiciones de seguridad lo aconsejan.
- En relación con el ciclo de vida: elabora la especificación, la arquitectura, el desarrollo, la operación y los cambios en el sistema.


Administrador de Seguridad del Sistema (ASS)

La persona designada como ASS figurará en la Documentación de Seguridad del Sistema de información y dependerá de forma funcional del responsable del Sistema (RSIS) y del Responsable de Seguridad de la Información (CISO).

Para el desarrollo de sus cometidos, podrá contar con usuarios privilegiados, que serán administradores de redes y/o sistemas.

Responsabilidades:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurarse de que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurarse de 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 del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 58 de 67	

- Informar al Responsable de Seguridad, al Responsable de Seguridad de Información y al Responsable del Sistema, de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- En emplazamientos donde se encuentren ubicados varios sistemas de información, la función de ASS de cada uno de ellos podría recaer en la misma persona.

Tareas:

- Aplica la configuración de seguridad en el sistema.
- Implanta las medidas de seguridad en el sistema.
- Aplica los procedimientos operativos de seguridad del sistema.


Oficina de Seguridad (OSEG)

Dentro de la estructura del Comité de Seguridad de la Información (CSI), y como elemento operativo del CISO, se constituye una Oficina de Seguridad TIC (OSTIC) cuyas competencias estarán relacionadas con las siguientes áreas de trabajo:

- Marco normativo y análisis y gestión de riesgos.
- Mantenimiento del ENS y de su documentación asociada.
- Colaboración en materia de ciberseguridad con otras Direcciones del Grupo.
- Seguridad en las interconexiones y conectividad.
- Vigilancia y determinación de superficie de exposición.
- Monitorización y gestión de incidentes.
- Observatorio digital y cibervigilancia.
- Otras funciones conexas o concordantes.

La Oficina de Seguridad estará conformada por:

- El Responsable de Seguridad de las TIC (CISO).
- Los Administradores Especialistas en Seguridad (AES), en función de los temas a tratar.
- Consultores normativos y especialistas en ciberseguridad.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 59 de 67	

Las funciones de la Oficina de Seguridad serán, entre otras, que les puedan ser encomendadas por el Comité de Seguridad de la Información o el CISO:

- Órgano de trabajo en apoyo de la labor del CISO.
- Gestión operativa y mantenimiento del Plan de Implantación de seguridad, explotación y mantenimiento.
- Análisis y debate de las cuestiones relacionadas con la seguridad de los sistemas de información dentro de su ámbito de competencia.
- Redacción y presentación de propuestas a los distintos comités.

La Oficina de Seguridad de la Información funcionará como un órgano permanente.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REMPLAZABLE, ESTÁNDAR, BAJA Página 60 de 67	

Equipo de Respuesta a Incidentes (ERI)

Este equipo se encarga de gestionar los incidentes de seguridad bajo las directrices marcadas por el Comité de Seguridad de la Información y funcionales del Responsable de Seguridad de las TIC (CISO) y posibles alertas recibidas del Centro de Operaciones de Ciberseguridad (SOC).


Está compuesto por un equipo con capacidades de atención inmediata denominado primer nivel de atención (L1) y por un grupo de especialistas para aquellos incidentes no resueltos por el primer nivel que requieran un mayor grado de especialización.

En caso necesario, podrá recurrir al SOC para obtener capacidades adicionales, como, por ejemplo, análisis forense o determinadas capacidades de detección.

Se establecerán unos SLA y unas instrucciones de coordinación con el SOC cuando haya que atender eventos o incidentes fuera del horario normal de trabajo o durante festivos.

Entre los cometidos del ERI se encuentran:

- a) Aplicación de inteligencia para la detección, respuesta coordinada, investigación de ciberataques y ciberamenazas y resolución de incidentes de seguridad, siempre en coordinación con el CoCS y el Responsable de Seguridad de las TIC (CISO).
- b) Llevar a cabo el registro, seguimiento y resolución de los incidentes de seguridad en los sistemas bajo su responsabilidad.
- c) Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- d) Realizar análisis forense digital y de seguridad cuando la complejidad del incidente así lo requiera, en coordinación con el Responsable de Seguridad de las TIC (CISO).
- e) Proponer al CISO acciones inmediatas a corto plazo si se detecta un comprometimiento de la información que pudiera tener consecuencias graves.
- f) Asegurar los elementos críticos del sistema, si se ha visto comprometida la seguridad de este.
- g) Determinar, hasta donde sea posible, el modo, los medios, los motivos y el origen del incidente, colaborando con el Responsable de Seguridad de las TIC (CISO) en la obtención de conclusiones y aprendizaje de este, de modo que se posibilite la prevención de incidentes similares en el futuro.
- h) Gestión de vulnerabilidades (análisis y determinación de las acciones de subsanación o parcheado) de aplicaciones y servicios.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 61 de 67	

Centro de Operaciones de Seguridad (SOC)

En relación a los servicios que presta el SOC al Grupo Oesía, operará siempre bajo la responsabilidad y dirección del Responsable de Seguridad de las TIC (CISO) como Director de la Oficina de Seguridad TIC.

El Centro de Operaciones de Ciberseguridad (SOC) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

Funciones

El Centro de Operaciones de Ciberseguridad (SOC) puede llevar a cabo las siguientes funciones:

- Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa, ya sea mediante interfaces previstas o instalando las correspondientes sondas.
- Análisis y correlación de eventos de seguridad y registros de actividad de los sistemas.
- Operación y actualización de los dispositivos de defensa.
- Podrá constituir un Equipo de Respuesta a Incidentes de Seguridad (ERI) fuera del horario normal de trabajo del ERI y en festivos.
- Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Análisis forense digital y de seguridad.
- Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 62 de 67	

35 ANEXO 3: GLOSARIO

ACTIVO: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS): Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.

AMENAZA: Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

ANÁLISIS O VALORACIÓN DE RIESGOS: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. ENS. Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema (STIC 811).

Interpretación, almacenamiento y procesado automático.

ASTIC: Autoridad de Seguridad de las TIC. Normalmente es una persona de la Alta Dirección o vinculada a la Alta Dirección.

AUDITORIA: Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.


AUDITORÍA DE LA SEGURIDAD: Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, hay que asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. ENS.

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.

CIBERINCIDENTE: Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real y adverso sobre un sistema de información y/o la información que trata o los servicios que presta. La diferencia principal entre un ciberincidente y un evento de seguridad es que el primero provoca un impacto sobre los activos.

CISO/RSEG: El Chief Information Security Officer (CISO) o Responsable de la Seguridad Lógica de un sistema (RSEG).

Es el responsable de seguridad y determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 63 de 67	

Es la persona encargada de velar por la seguridad de la información de la organización. Su labor consiste en estar al día de la evolución tecnológica en la medida en que afecta a la seguridad de la información, estableciendo puentes entre el responsable de seguridad corporativa y los responsables de tecnología.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Órgano colegiado que coordina las actividades de la organización en materia de seguridad de la información. Asume los roles de Responsable de la Información y Responsable de los Servicios, por lo que categoriza la información y los servicios.

COMITÉ DE SEGURIDAD CORPORATIVA: Órgano colegiado que coordina las actividades de la organización en materia de seguridad, coordina las acciones de seguridad dentro de la organización y hace de órgano de enlace con la Alta Dirección en asuntos de seguridad.

CONFIDENCIALIDAD Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

DATOS: Representación de la información usando algún formato que permita su comunicación,

DATOS DE CARÁCTER PERSONAL: Cualquier información concerniente a personas físicas identificadas o identificables, que requieren unas medidas especiales de protección.

DISPONIBILIDAD: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

DUEÑO DEL RIESGO: Persona o entidad que tiene la responsabilidad y la autoridad para gestionar los riesgos, normalmente el ASTIC de la Organización.

DECLARACIÓN DE CONFORMIDAD: Manifestación escrita de los órganos o entidades de derecho público, firmada por su responsable, mediante la que se da publicidad que los sistemas a que se refieren cumplen con las exigencias del Esquema Nacional de Seguridad aprobado por Real Decreto 3/2010, de 8 de enero.

DISPONIBILIDAD: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

EFFECTIVIDAD / EFICACIA:

Efectividad. Capacidad de lograr el efecto que se desea o se espera.

Eficacia. Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

EFICIENCIA: Relación entre el resultado alcanzado y los recursos utilizados.

EVENTO DE SEGURIDAD: Suceso de seguridad de la información. Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

EVIDENCIA DE AUDITORÍA: Las evidencias consisten, principalmente, en las demostraciones y testimonios (documentales, automatizadas, etc.) de los resultados de la aplicación de los

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 64 de 67	

procedimientos de auditoría (pruebas). Éstas deben ser suficientes para soportar las conclusiones del auditor. Para ello deben acreditar determinadas situaciones o hechos irrefutables en cuanto a los hechos a los que se refieren. La evaluación de estas evidencias corresponde al auditor para emitir su opinión.

GESTIÓN DE INCIDENTES: Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

IMPACTO: Consecuencia que sobre un activo tiene la materialización de una amenaza.

INCIDENTE DE SEGURIDAD: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información que genera un impacto negativo en los activos.

INFORMACIÓN: Caso concreto de un cierto tipo de información.

INTEGRIDAD: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

INTERCONEXIÓN: Se produce una interconexión entre Sistemas, cuando existe una conexión y se habilitan flujos de información entre los mismos, con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes responsables o una combinación de las anteriores.

MANEJAR INFORMACIÓN: Presentar, elaborar, almacenar, procesar, transportar o destruir información.

MEDIDAS DE SEGURIDAD: Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.


MÍNIMO PRIVILEGIO: Principio según el cual los sujetos deben acceder exclusivamente a aquellos objetos que precisen inexcusablemente para ejecutar sus trabajos o procesos.

PLAN DE RESPUESTA A CIBERINCIDENTES: Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciberincidente.

POLÍTICA DE SEGURIDAD: Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

PRINCIPIOS BÁSICOS DE SEGURIDAD: Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

PRINCIPIOS DE SEGREGACIÓN DE FUNCIONES: La separación o segregación de funciones es una regla básica en los controles: evitar que una persona pueda dominar todo un proceso, de tal forma que errores u omisiones, o incumplimientos de controles no puedan ser identificados. Por lo tanto, el

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 65 de 67	

auditor debe identificar donde no se cumple con esta norma fundamental, para evaluar el impacto en la efectividad de los controles.

PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD: Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. En su caso será la descripción de la aplicación de la Declaración de Requisitos de un Sistema (DRS) correspondiente. Los POS definen los principios que deberán adoptarse en materia de seguridad, los procedimientos operativos que deberán seguirse y las responsabilidades del personal. Los POS se elaborarán bajo la responsabilidad del Responsable del Sistema.

PROCESO: Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

PROCESO DE SEGURIDAD: Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

RESPONSABILIDAD: Obligación o deber de realizar alguna acción.

RESPONSABLE DE LA INFORMACIÓN: Persona u órgano colegiado que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

RESPONSABLE DEL SERVICIO: Persona u órgano colegiado que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

RESPONSABLE DEL SISTEMA (RSIS/AOSTIC): Persona que se encarga de la explotación del sistema de información.

RIESGO: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

SEGURIDAD DE LA INFORMACIÓN (SEGINFO): Seguridad de la Información. Es la protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad y disponibilidad.

SEGURIDAD EN LOS DOCUMENTOS (SEGINFODOC): Entiende de las medidas de protección aplicables a los documentos durante todo su ciclo de vida, es decir, durante su elaboración, almacenamiento, transporte o destrucción, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que contienen.

SEGURIDAD EN LAS EMPRESAS (SEGINFOEMP): Entiende de las medidas de protección dirigidas a las empresas y aplicables por ellas, con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información del Ministerio de Defensa, o de otros Organismos públicos, nacionales o internacionales, manejada por éstas, como consecuencia de su participación en programas, proyectos o contratos.

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 66 de 67	

SEGURIDAD DE LA INFORMACIÓN EN LAS INSTALACIONES (SEGINFOINST): Entiende de las medidas de protección aplicables a las instalaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información presente en el interior de estas.

SEGURIDAD DE LA INFORMACIÓN EN LAS PERSONAS (SEGINFOPER): Entiende de los requisitos exigidos a las personas con el objeto de garantizar razonablemente el correcto uso de la información por éstas.

SEGURIDAD DE LA INFORMACIÓN EN LOS SISTEMAS (SEGINFOSIT): Entiende de las medidas de protección aplicables en los sistemas de información y telecomunicaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que manejan.

SERVICIO: Función o prestación desempeñada por alguna entidad destinada a cuidar intereses o satisfacer necesidades de la empresa o de los clientes.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. ENS

SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES: Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única autoridad.

TIPO DE INFORMACIÓN: Una categoría específica de información (por ejemplo, datos de carácter personal, médicos, financieros, investigaciones, contratos, información delicada, ...). Estos tipos los define una organización y, en algunos casos, vienen definidos por alguna normativa de carácter legal.

TRAZABILIDAD: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. ENS

	POLÍTICA	ORG-01_01	V2.0
	SEGURIDAD DE LA INFORMACIÓN	USO PÚBLICO, REPLAZABLE, ESTÁNDAR, BAJA Página 67 de 67	

36 ANEXO 4: ABREVIATURAS

- AEPD:** Agencia Española de Protección de Datos
- AOS/RSIS:** Autoridad Operacional del Sistema TIC
- AOSTIC/RSIS:** Autoridad Operacional del Sistema TIC
- AR:** Análisis de Riesgos
- ASS:** Administrador de Seguridad del Sistema
- ASTIC:** Autoridad de Seguridad TIC
- CCN:** Centro Criptológico Nacional
- CCN-CERT:** Centro Criptológico Nacional – Computer Emergency Response Team
- CERT:** Computer Emergency Response Team. Equipo de Respuesta a Incidentes Informáticos o ciberincidentes.
- CIO:** Chief Information Officer
- CISO/RSEG:** Chief Information Security Officer
- CSC:** Comité de Seguridad Corporativa.
- CSI:** Comité de Seguridad de la Información
- CSO:** Chief Security Officer
- DPO:** Data Protection Officer
- ENS:** Esquema Nacional de Seguridad
- ERI:** Equipo de Respuesta a Incidentes de Seguridad.
- ISO:** International Organization for standardization
- LOPD:** Ley Orgánica de Protección de Datos de Carácter Personal
- OSI:** Organización y Sistemas de Información
- POS:** Procedimientos Operativos de Seguridad
- PPS:** Plan Permanente de Seguridad
- RSEG/CISO:** Responsable de la Seguridad
- RSERV:** Responsable del Servicio
- RSIS/AOSTIC/AOS** Responsable del Sistema STIC
- SGSI:** Sistema de Gestión de la Seguridad de la Información.
- STIC:** Seguridad en las Tecnologías de la Información y las Comunicaciones.
- TIC:** Tecnologías de la Información y las Comunicaciones