POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

14/DIC/21

USO PÚBLICO, INTEGRIDAD REEMPLAZABE, DISPONIBILIDAD ESTÁNDAR, CRITICIDAD BAJA

Ámbito de difusión:	Uso público / Todo el personal de la empresa
Responsable	COMITÉ DE SEGURIDAD TIC / ALTA DIRECCIÓN

CONTROL DE VERSIONES					
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

Índice

1 Aprobación y entrada en vigor

Esta política se ha aprobado el día 14/DIC/2021 por el Comité Ejecutivo del Grupo OESÍA, 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 la anterior Política que fue aprobada el día 20/09/2021 por el Comité Ejecutivo del Grupo OESÍA.

2 Proceso de desarrollo y aprobación de la Política

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.

El Comité de Seguridad de la Información revisará una vez al año, o cuando las circunstancias así lo aconsejen, el contenido de la Política de Seguridad de la información, 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.

Los Procedimientos de Seguridad estarán disponibles para 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.

3 Introducción

El Grupo OESÍA 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, autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

En este sentido, el Grupo OESÍA ha decido 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.

La seguridad se entenderá en el Grupo OESÍA como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural que no sea conforme con el mismo.

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 eventos e incidentes de seguridad.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución que afecten a la confidencialidad, integridad, autenticidad, trazabilidad o 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.

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.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Concienciación, formación y adiestramiento.
m) Registro de actividad.
n) Incidentes de seguridad.
o) Continuidad de la actividad.
p) Mejora continua del proceso de seguridad.

Los diferentes departamentos del Grupo OESÍA 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:

Prevención

Las áreas del Grupo OESÍA 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.

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.

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.

Respuesta

Las distintas áreas del Grupo OESÍA 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.

Recuperación

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

4 Alcance

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

5 Misión

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.

6 Valores corporativos

El Grupo OESÍA tiene como misión 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 un valor 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 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.

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 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.

7 Marco legal

1. Ley 15/1999 de 13 de diciembre de Protección de Datos de carácter personal. Derogada por la Ley 3/2018, salvo artículos 22, 23 y 24. Aporta criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.
2. RD 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD. Desarrolla y complementa el contenido de la Ley Orgánica 15/1999, de Protección de Datos de carácter personal.
3. Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico. Regula determinados aspectos jurídicos de los servicios de la sociedad de la información, como pueden ser, el comercio electrónico, la contratación en línea, la información y publicidad y los servicios de intermediación
4. Ley 59/2003 de 19 de diciembre de Firma Electrónica. Modificada por la Ley 39/2015. Regula la firma electrónica (que surge como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet), su eficacia jurídica y la prestación de servicios de certificación; deberá adaptarse a lo que dice el Reglamento UE 910/2014 (más conocido como eIDAS).
5. Ley 25/2007 de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Estipula cómo conservar los datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (transposición de la Directiva 2006/24/CE).
6. Ley 37/2007 de 16 de noviembre sobre reutilización de la información del sector público. Establece un conjunto mínimo de normas que regulan la reutilización y los instrumentos prácticos para facilitar la reutilización de los documentos existentes conservados por organismos del sector público de los Estados miembros (transposición de la Directiva 2003/98/CE sobre la conservación y reutilización de la información del sector público).
7. Decreto 232/2007 de 18 de diciembre por el que se regula la utilización de medios electrónicos, informáticos y telemáticos en los procedimientos administrativos. Garantiza a la ciudadanía el pleno ejercicio de los derechos reconocidos en las leyes, y posibilita a los órganos y personal de la Administración Pública el cumplimiento de las obligaciones que les vienen impuestas por el ordenamiento jurídico.
8. Ley 56/2007 de 28 de diciembre de Medidas de Impulso de la Sociedad de la Información. Enmarca el conjunto de medidas que constituyeron el Plan Avanza 2006-2010 para el

desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, aprobado por el Gobierno en noviembre de 2005, continuado por el Plan Avanza 2 (2011-2015).

9. RD 1671/2009 de 6 de noviembre por el que se desarrolla parcialmente la Ley 11/2007. Derogado en parte por las Leyes 39 y 40/2015. Desarrollo parcial de la Ley 11/2007 en lo relativo a la transmisión de datos, sedes electrónicas y punto de acceso general, identificación y autenticación, registros electrónicos, comunicaciones y notificaciones, y documentos electrónicos y copias.
10. RD 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. Crea las condiciones necesarias de confianza en el uso de los medios electrónicos, para lo cual establece los principios básicos y requisitos mínimos a cumplir en materia de seguridad, así como una serie de medidas de seguridad específicas que se deben aplicar.
11. RD 4/2010 de 8 de enero por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Determina los criterios de seguridad, normalización (estandarización) y conservación de la información de los sistemas informáticos de la Administración Pública, con el objetivo de asegurar la interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios.
12. Decreto 21/2012 de 21de febrero de Administración Electrónica. Regula los medios electrónicos necesarios para que las relaciones entre la ciudadanía y la Administración sean seguras, ágiles y con plenas garantías jurídicas.
13. Ley 9/2014 de 9 de mayo General de Telecomunicaciones. Regula las telecomunicaciones, que comprenden la explotación de las redes, y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados.
14. Reglamento UE 910/2014 (eIDAS) de 9 de julio del Parlamento Europeo y del Consejo. Vela por la interoperabilidad respecto a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (deroga la Directiva 1999/93/CE).
15. Ley 39/2015 de 1 de octubre del Procedimiento Administrativo Común (PAC) de las AAPP. Regula los requisitos de validez y eficacia de los actos administrativos, el PAC a todas las AAPP, incluyendo el sancionador y el de reclamación de responsabilidad de las AAPP, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria, estableciendo la obligación de cumplir con el Esquema Nacional de Seguridad.

16. Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público. Establece y regula las bases del régimen jurídico de las AAPP, los principios del sistema de responsabilidad de las AAPP y de la potestad sancionadora, así como la organización y funcionamiento de la AGE y de su sector público institucional para el desarrollo de sus actividades, estableciendo la aplicación del Esquema Nacional de Seguridad en dichas actividades.
17. RD 951/2015 de 23 de octubre de modificación del ENS. Actualiza el ENS, adoptando en cada momento los mecanismos que mejoren la respuesta en materia de seguridad de los sistemas tecnológicos utilizados en la Administración, en particular frente a las ciberamenazas, y reforzando los servicios de confianza y la protección para las transacciones electrónicas.
18. Reglamento (UE) 2016/679 de 27 de abril. Reglamento General de Protección de Datos. Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
19. Ley 3/2018 de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales. Adapta el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completa sus disposiciones y garantiza los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución
20. RD-Ley 14/2019 de 31 de octubre Por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Regula un marco normativo que comprende medidas urgentes relativas a la documentación nacional de identidad; a la identificación electrónica ante las Administraciones públicas; a los datos que obran en poder de estas; a la contratación pública; y al sector de las telecomunicaciones.
21. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia
22. Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

23. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, por la que se transpone la Directiva NIS (UE 2016/1148). Relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.
24. Instrucciones Técnicas de Seguridad, Normas CCN-STIC, recomendaciones, e Informes de Amenazas del Centro Criptológico Nacional:
25. Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
26. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
27. Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
28. Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
29. Normativa ISO 27001/27002.
30. Ley 1/2019, de 20 de febrero, de Secretos Empresariales. Por la que se regula la protección de los secretos empresariales.
31. Normativa nacional e internacional para el manejo de información clasificada.
    - Ley de Secretos Oficiales y normas que la desarrollan.
    - Política de Seguridad de la Información del Ministerio de Defensa.
    - Normas de la Autoridad Nacional para la Protección de la Información Clasificada.
    - Normativa de Seguridad OTAN (North Atlantic Treaty Organization – NATO).
    - Normativa y guías CCN-STIC para manejo de información clasificada.
    - Normativa OCCAR (Organisation Conjointe de Coopération en matière d'ARmement).
    - Normativa ESA (European Space Agency) para manejo de información clasificada.
    - Normativa LoI/FA EDIR (Letter of Intent / Framework Agreement for European Defence Industrial Restructuration).
    - Directivas de la Unión Europea para manejo de Información Clasificada.

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:

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

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.

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.

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.

Comités: funciones y responsabilidades

Comité de Seguridad Corporativa

Composición:

Presidente: ASTIC de OESÍA (Director Corporativo de Capital Intangible).

Secretario: CSO.

VOCALES:

CISO.

DPO.

Director de seguridad física.

Director Oficina Técnica COO.

Director de Infraestructura.

Director de Operaciones.

Director de Talento.

Director de Arquitectura y Medios TIC.

Director de Organización y Sistemas.

Responsable de Seguridad Industrial.

Responsable de Seguridad en los Documentos.

Director Jurídico.

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.
- 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.

Comité de Seguridad de la Información

Composición:

Presidente: CSO

Secretario: CISO

Vocales:

DPO

Director de Arquitectura y Medios.

Director de proyecto del POS y/o responsable de la Oficina Técnica de Seguridad.

Jefe del SOC.

AOSTIC's 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 al mes, 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.
- 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 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.

Roles: funciones y responsabilidades

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 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 transmitirlas 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.

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
- 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.
- 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.

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), 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.

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 sistemas que dependan de proyectos, los RSIS relativos a cada proyecto 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.

Responsabilidades:

- Identificar y valorar las necesidades relacionadas con la seguridad del sistema.
- Coordinar con el resto de las áreas del Grupo OESÍA, los apoyos y la financiación necesaria para mantener la seguridad del sistema, 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.

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.
- 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.

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) 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 un Responsable del Sistema (RSIS), precisando sus funciones y responsabilidades dentro del marco establecido por esta Política de seguridad de la Información.

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.

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.

13 Categorización de sistemas

Todos los sistemas del Grupo OESÍA tendrán una categorización 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.

14 Categorización de la Información

La información generada en el Grupo OESÍA, se categorizará por la persona que la genera y siempre se realizará 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 para facilitar su uso y manipulación.

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.

15 Datos de carácter personal

El Grupo OESÍA 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 OESÍA 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.

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 y registrado.

Existirá un sistema de control de acceso a las instalaciones, que, en el caso de las instalaciones críticas, se basará en doble factor.

17 Protección de las instalaciones

Los sistemas se instalarán en áreas separadas (DPD 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 contraincendios, 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.

18 Integridad y actualización de los sistemas

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Todo el software y el hardware deberá estar actualizado 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.

19 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, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

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 presente real decreto, 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 estos.

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 clasificación de la información, para permitir el tratamiento adecuado de la misma por parte de todos los miembros de la organización.

20 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 apartado 26 del Anexo II, de la Ley 32/2003 de 3 de noviembre, 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 y como mínimo, de mínimos privilegios.

21 Registro de seguridad

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.

22 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 del CCN y la Guía Nacional de Notificación y Gestión de Ciberincidentes y se usará la herramienta LUCIA.

23 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.

24 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.

25 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: instalación, mantenimiento, gestión de incidentes 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.

26 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.
b) Formación, la adquisición de habilidades básicas de ciberseguridad para el desarrollo de sus competencias profesionales.
c) Adiestramiento, la puesta a prueba y valoración de las habilidades básicas de ciberseguridad mediante simulacros, ejercicios o supuestos prácticos.

27 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.

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.

28 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.

29 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, se empleará alguna metodología reconocida internacionalmente.

La gestión de riesgos 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 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.

El Comité de Seguridad de la Información consolidará las necesidades de recursos trasladadas por los RSIS 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 estos. En ningún caso, la externalización se podrá considerar como sustituto de otras salvaguardas y siempre como un complemento a estas.

30 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 estos 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.

31 Terceras partes

Cuando el Grupo OESÍA 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.

Cuando el grupo OESÍA 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 Corporativa y por parte de los responsables de los servicios afectados, antes de seguir adelante.

32 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 Secirity Officer (CISO) o Responsable de la Seguridad Lógica de un sistema (RSEG).

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

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.

EFECTIVIDAD / 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 procedimientos de auditoría (pruebas). Éstas deben ser suficientes para soportar las conclusiones del auditor. Para ello deben acreditar determinadas situaciones o hechos irrebatibles 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 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)

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.

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.

33 ABREVIATURAS

AEPD

Agencia Española de Protección de Datos

AOS/RSIS

Autoridad Operacional del Sistema

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

ISO

International Organization for standardization

LOPD

Ley Orgánica de Protección de Datos de Carácter Personal

POS

Procedimientos Operativos de Seguridad

RSEG/CISO

Responsable de la Seguridad

RSERV

Responsable del Servicio

RSIS/AOSTIC/AOS

Responsable del Sistema

STIC

Seguridad de las Tecnologías de la Información y las Comunicaciones

TIC

Tecnologías de la Información y las Comunicaciones

OESÍA Networks, S.L.

Calle Marie Curie, 19

28251 – Madrid,

Teléfono: 91 309 86 00, Fax: 91 375 82 16

http://www.OESÍA.com