POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

20/sep/21

USO PÚBLICO

Índice

1 Control de versiones

SÍNTESIS DEL DOCUMENTO	
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	20/09/21	Comité de Seguridad TIC	Creación	Comité de Seguridad Corporativa	Comité Ejecutivo

2 Aprobación y entrada en vigor

Esta política se ha aprobado el día 20/09/2021 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 la anterior Política que fue aprobada el día 03/07/2018 por el Subcomité de Producción Digital.

3 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, autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

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

Toda la organización tiene responsabilidades en materia de Seguridad de la Información.

Los requisitos de seguridad impuestos por los clientes para los productos o servicios que se le prestan deberán cumplirse en todo momento y atender a todo el ciclo de vida de los mismos.

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:

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 áreas deben:

- Autorizar los sistemas antes de entrar en operación y retirarlos del servicio cuando ya no sean necesarios.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

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 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.

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.

4 Alcance

Esta Política de seguridad de la información 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 a 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.

5 Valores corporativos

El Grupo OESIA 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.

6 Marco legal

1. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y desarrollo normativo asociado

2. ISO 27001/27002.

3. 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).

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

5. Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

6. 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.

7 Organización de la seguridad de la información

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 elaborado, 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 al 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.

Roles: funciones y responsabilidades

Responsable de Seguridad Corporativa (CSO)

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

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 OESIA 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 OESIA y las expectativas de los clientes.
- Coordinar todas las funciones de seguridad del Grupo OESIA.
- 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 OESIA.
- 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 OESIA 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[1].

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.

[1] El RSIS (Responsable del Sistema), también es conocido como AOSTIC (Autoridad Operacional del Sistema TIC) o AOS (Autoridad Operacional del Sistema), es un cargo no técnico, que vela por el cumplimiento de los requisitos operativos, incluidos los de seguridad.

- 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.

8 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.

9 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, que 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.

Esta Política de Seguridad de la Información se desarrollará por medio de Normas de Seguridad y Procedimientos de Seguridad que tratan aspectos específicos según el marco legal y regulatorio vigente.

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.

10 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.

11 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.

12 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.

13 Gestión de riesgo

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 a la selección de las salvaguardas necesarias.

Este análisis se repetirá regularmente:

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

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

14 Obligaciones del personal

Todos los miembros del Grupo OESIA 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 OESIA 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 OESIA 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.

15 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.

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.

16 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. ENS.

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, 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. ENS.

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. En particular asume los roles de responsable de la información y responsable de 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. ENS.

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. ENS.

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. ENS

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. ENS.

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. ENS.

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. ENS.

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. ENS.

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. ENS.

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. ENS.

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. ENS.

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.

17 ABREVIATURAS

AEPD

Agencia Española de Protección de Datos

AOS/RSIS

Autoridad Operacional del Sistema

AOSTIC/RSIS

Autoridad Operacional del Sistema TIC

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.oesia.com