NexTReT

Política de Seguridad

REF. PL-SEG-01

Albert Domingo Melgosa
NexTReT, S.L.
CIF: B60345527

Fecha:
2022.10.19
17:03:19
+02'00'

Albert Domingo Melgosa
Consejero Delegado
Barcelona, 19/10/2022

ÍNDICE

1. Exposición de Motivos

NexTReT depende de los Sistemas TIC (Tecnologías de Información y Comunicaciones) para conseguir sus objetivos.
Estos sistemas tienen que ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.
El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza en los incidentes.
Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos tienen que aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la ISO 27001, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir, analizar y corregir las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.
Los diferentes departamentos tienen que asegurar que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación tienen que ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Los departamentos tienen que estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, según el Artículo 7 y el Artículo 8 del ENS y conforme las directrices de la ISO 27001.

2. Gestión de Incidentes de Seguridad

2.1 Prevención

Los departamentos tienen que evitar, o al menos prevenir en lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 19 establece que los sistemas tienen que diseñarse y configurarse de forma que garanticen la seguridad por defecto, en línea con la política de mínimo privilegio “Need to Know”. De igual forma, el artículo 17 del citado ENS define que los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.
Para lo cual los departamentos tienen que implementar las medidas mínimas de seguridad determinadas por el ENS y la ISO 27001, 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, tienen que estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política, los departamentos tienen que:

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

2.2 Detección

Dado que los servicios se pueden degradar rápidamente a causa de incidentes, que van desde una simple desaceleración hasta su detención, los servicios tienen que monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS y la ISO 27001.
La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.
Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.
Se tendrán que establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel de sistema.

2.3 Respuesta

Los departamentos tienen que:

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

2.4 Recuperación

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

3. Alcance

Esta política, aplica a los siguientes Sistemas de Información asociados a:

Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad):

- Servicios de instalación, gestión, operación, administración, monitorización, auditoría, asistencia técnica y soporte de soluciones e infraestructuras de Tecnologías de la Información y las Comunicaciones (TIC y IoT) y Seguridad Informática, VSOC gestión y vigilancia de seguridad “spidernext”.
- Suministro y servicios de mantenimiento de licencias, hardware, software.

- Servicios genéricos de Centro de Proceso de Datos (Datacenter) y servicios en la nube (Cloud Computing) incluyendo modelos SaaS, PaaS, IaaS o XaaS (todo como servicio).
- Consultoría, implementación y auditoría de Seguridad de la Información, Cumplimiento legal y normativo.
- Servicios de consultoría, diseño, desarrollo y mantenimiento de aplicaciones informáticas incluyendo soluciones basadas en entornos de internet, móvil y escritorio.
- Servicios de análisis de datos e inteligencia artificial.

Norma Internacional ISO 27001:

- El Sistema de Información que da soporte a los procesos de: Diseño, desarrollo, implantación y mantenimiento de proyectos de desarrollo de aplicaciones, sistemas y comunicaciones. Consultoría, implementación y auditoría de Seguridad de Tecnologías de la Información. Prestación servicios técnicos en las modalidades de servicios profesionales y outsourcing. De acuerdo con la declaración de aplicabilidad en vigor 5.0.

Ver documento: *(PR-SEG-03) Cuerpo normativo – Seguridad en la Operativa*

4. Misión y Servicios Prestados

NexTReT como empresa privada, vela por la gestión de sus intereses; y en el ámbito de la prestación de sus servicios para la Administración Pública y Empresas Privadas, sirve con objetividad los intereses generales prestando los servicios que contribuyen a satisfacer las necesidades de los servicios prestados.

5. Marco Normativo

Como base normativa para realizar la presente política de seguridad, se ha analizado la legislación vigente, que afecta al desarrollo de las actividades de la Administración Local y Privada en el que a Administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información. El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 209/2003, de 21 de febrero, por el cual se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Ver documento: *(FR-SGSI-09) Marco normativo seguridad.*

5.1 Procedimiento Administrativo

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

5.2 Protección de Datos de Carácter Personal

- 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 el que respeta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley 3/2018, de 5 de diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales.

5.3 Administración Electrónica

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, como norma básica en esta materia.
- Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo (Identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior)
- La Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

5.4 Firma Electrónica

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- COM (2001) 298 - final, de la Comisión Europea - Seguridad de las redes y de la información: Propuesta para un enfoque político europeo.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

5.5 Seguridad de las Redes y de la Información

- Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad. Como complemento a la legislación vigente, existe en la actualidad la norma internacional UNE ISO/IEC 27002 “Código de Buenas Prácticas para la gestión de la seguridad de la información” que se ha configurado como un estándar en la hora de auditar los aspectos relacionados con la seguridad de la información en las organizaciones.

6. Organización de la Seguridad

6.1 Comités: Funciones y Responsabilidades

El Comité de Seguridad es el Órgano que coordina la Seguridad de la Información a nivel de Organización.

Estará constituido por el Responsable de Seguridad de la Información y por representantes de otras áreas afectadas por el ENS.

6.1.1 Funciones Asociadas

- Responsabilidades derivadas del tratamiento de datos de carácter personal.
- Asunción de la figura de Responsable de Servicio para todos los servicios prestados en el marco de la RD 311/2022.
- Asunción de la figura de Responsable de la Información para todas las informaciones empleadas por los servicios prestados en el marco de la RD 311/2022.
- Atender las inquietudes de los Órganos superiores competentes y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a los Órganos superiores competentes.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de la Organización en cuanto a la 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 porque sea aprobada por los Órganos superiores competentes.
- Aprobar la normativa de seguridad de la información.
- 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 al respeto.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respeto. 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 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.
- Velar porque la seguridad de la información se tiene en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, tendrá que 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 cuales no tenga suficiente autoridad para decidir.

6.1.2 En caso de Ocurrencia de Incidentes de Seguridad de la Información

Aprobará el Plan de Mejora de la Seguridad, con su dotación presupuestaria correspondiente. El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico, propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los cuales tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Grupos de trabajo especializados internos, externos o mixtos.
- Asesoría externa.

- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

El Responsable de la Seguridad de la Información es el secretario del Comité de Seguridad de la Información y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

6.2 Definición de roles

La Política de Seguridad, según requiere el Anexo II del Esquema Nacional de Seguridad en su sección 3.1, tiene que identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la organización Administrativa.
Se establecen los siguientes roles en la organización relacionados con la Seguridad de la Información.

6.2.1 Responsable de la Información

Corresponde al nivel de un Órgano de Gobierno de máximo nivel, constituido por los Órganos superiores competentes, que entiende la misión de la organización, determina los objetivos que se propone conseguir y responde que se consigan.
Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.
La persona u órgano que lo asuma tendrá que ser identificada para cada Información que trate la organización.

6.2.1.1 Funciones Asociadas

- Tiene la responsabilidad última del uso que se haga de una cierta información y, por lo tanto, de su protección.
- El Responsable de la Información delega en el Comité de Seguridad como responsable de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- El Responsable de la Información delega en el Responsable de cada uno de los Activos como responsable de Determinar los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo Y del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y del Responsable del Sistema.

6.2.1.2 Compatibilidad con otros Roles

Este rol podrá coincidir con el del Responsable de Servicio y con el de Responsable del tratamiento requerido por el RGPD.
Este rol no podrá coincidir con el de Responsable de Seguridad, excepto en organizaciones de reducida dimensión que funcionen de forma autónoma.
Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

6.2.2 Responsable del Servicio

Cuando sea diferente del Responsable de la Información, puede corresponder al nivel de un Órgano de Gobierno de máximo nivel, igual que el Responsable de la Información, o bien al de una Dirección ejecutiva o gerencia, que entiende qué hace cada departamento, y como los departamentos se coordinan entre sí para conseguir los objetivos marcados por los Órganos superiores competentes.
Sus funciones podrán ser asignadas a personas individuales, o bien ser asumidas por el Comité de Seguridad de la Información.
El Responsable del Servicio delega en el Responsable de cada uno de los Activos como responsable de Determinar los niveles de seguridad en cada dimensión dentro del marco establecido en el Anexo Y del Esquema Nacional de Seguridad.
La persona u órgano que lo asuma tendrá que ser identificada para cada Servicio que preste la organización.

6.2.2.1 Funciones Asociadas

- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por lo tanto, de su protección.
- El Responsable del servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Determinará los niveles de seguridad en cada dimensión del servicio dentro del marco establecido en el Anexo Y del Esquema Nacional de Seguridad.
- Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta del Responsable de la Seguridad y del Responsable del Sistema.
- La prestación de un servicio siempre tiene que atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredar los requisitos de seguridad del mismo, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

6.2.2.2 Compatibilidad con otros Roles

Podrá coincidir en la misma persona u órgano el rol de Responsable de la Información y del Responsable del Servicio, aunque generalmente no coincidirán cuándo:

- El servicio gestione información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- La prestación del servicio no dependa de la unidad a la cual pertenece el Responsable de la Información.
- Este rol podrá coincidir con el del Responsable de Servicio y con el de Responsable de Fichero requerido por el RGPD.
- Este rol no podrá coincidir con el de Responsable de Seguridad, excepto en organizaciones de reducida dimensión que funcionen de forma autónoma.
- Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

6.2.3 Responsable de Seguridad de la Información

Corresponde al nivel de una Dirección ejecutiva o Gerencia.
Se nombrará formalmente como tal a una única persona en la organización. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá haber más de una persona asumiendo el rol en la organización, aunque pueda delegar parte de sus funciones en otras personas.

6.2.3.1 Funciones Asociadas

- Reportará directamente al Comité de Seguridad de la Información.
- Actuará como Secretario del Comité de Seguridad de la Información.
- Convocará al Comité de Seguridad de la Información, recopilando la información pertinente.
- Pertenecerá al Comité de Seguridad Corporativa, para coordinar las necesidades de Seguridad de la Información en el marco del resto de necesidades de Seguridad Corporativa.
- Mantendrá la seguridad de la información empleada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, según el que establece en la Política de Seguridad de la Organización.
- Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Recopilará los requisitos de seguridad de los Responsables de Información y del Servicio y determinará la categoría del Sistema.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará a los Responsables de Información y a los Responsables de Servicio, información sobre el nivel de riesgo residual esperado después de implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Coordinará la elaboración de la Documentación de Seguridad del Sistema.
- Participará en la elaboración, en el marco del Comité de Seguridad de la Información, la Política de Seguridad de la Información, para su aprobación por la Dirección.
- Participará en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de Seguridad de la Información.
- Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que tendrán que ser aprobados por el Comité de Seguridad de la Información.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que tendrán que ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

6.2.3.2 En caso de ocurrencia de incidentes de seguridad de la información

- Analizará y propondrá Salvaguardas que prevengan incidentes similares en un futuro.

6.2.3.3 Compatibilidad con otros Roles

Este rol únicamente podrá coincidir con la del Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Este rol no podrá coincidir con el de Responsable de Sistema y el de Administrador de Seguridad del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

6.2.3.4 Delegación de Funciones

Por determinados Sistemas de Información que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, se podrán designar los Responsables de Seguridad Delegados que se consideren necesarios.
La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final seguirá recayendo sobre el Responsable de la Seguridad.
Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad, pudiendo ser, por ejemplo, la seguridad de sistemas de información concretos o de sistemas de información horizontales.
Cada Responsable de Seguridad Delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.
La delegación de funciones pasará previamente por el comité.

6.2.4 Responsable del Sistema

Corresponde al nivel de una Dirección Operativa.
Se nombrará formalmente como tal a una única persona para cada Sistema. El rol no podrá ser desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas.

6.2.4.1 Funciones Asociadas

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El Responsable del Sistema puede acordar la suspensión del uso de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión tiene que ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
- Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
- Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.
- Elaborar los Planes de Continuidad del Sistema porque sean validados por el Responsable de Seguridad de la Información, y coordinados y aprobados por el Comité de Seguridad de la Información.
- Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
- Elaborará las directrices para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios) y las facilitará al Responsable de Seguridad de la Información para su aprobación.

6.2.4.2 En caso de Ocurrencia de Incidentes de Seguridad de la Información

- Planificará la implantación de las Salvaguardas en el sistema.
- Ejecutará el plan de seguridad aprobado.

6.2.4.3 Compatibilidad con otros Roles

Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio.
Este rol podrá coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o media que tengan una estructura autónoma de funcionamiento.
En grandes organizaciones no tendría que coincidir con el de Administrador de la Seguridad del Sistema, independientemente del tamaño del Sistema.

6.2.5 Administrador de la Seguridad del Sistema

Corresponde al nivel de un empleado calificado en seguridad informática de sistemas.
Podrá nombrarse formalmente como tales varias personas para cada Sistema. El rol no podrá ser desarrollado por un órgano colegiado, ni podrá delegar parte de sus funciones en otras personas.
Si procede, se nombrarían nuevos Administradores de la Seguridad del Sistema.
Será propuesto por el Responsable del Sistema, a quien reportará en todo lo relacionado con seguridad de la información.

6.2.5.1 Funciones Asociadas

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que la trazabilidad, pistas de auditoría y otros registros de seguridad requeridos se encuentren habilitados y registren con la frecuencia deseada, de acuerdo con la política de seguridad establecida por la Organización.
- Aplicar a los Sistemas, usuarios y otros activos y recursos relacionados con el mismo, tanto internos como externos, los Procedimientos Operativos de Seguridad y los mecanismos y servicios de seguridad requeridos.
- Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de información y los mecanismos y servicios de seguridad requeridos.
- La gestión, configuración y actualización, si procede, del hardware y software en los cuales se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Aprobar los cambios en la configuración vigente del Sistema de Información, garantizando que sigan operativos los mecanismos y servicios de seguridad habilitados.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Monitorizar el estado de la seguridad del sistema.

6.2.5.2 En caso de Ocurrencia de Incidentes de Seguridad de la Información

- Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- Ejecutar el plan de seguridad aprobado.
- Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.

- Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones tendrían que estar documentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad en los mismos (estas actuaciones quedarán documentadas para reducir el margen de discrecionalidad del Administrador de Seguridad del Sistema al mínimo número de casos).
- Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- Investigar el incidente: Determinar la manera, los medios, los motivos y el origen del incidente.

6.2.5.3 Compatibilidad con otros Roles

Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad Corporativa o de la Información.
Este rol podrá coincidir con el de Responsable del Sistema en organizaciones de una dimensión reducida o media que tengan una estructura autónoma de funcionamiento.
En grandes organizaciones no tendría que coincidir con el de Responsable del Sistema, independientemente del tamaño del Sistema.

6.2.5.4 Delegación de Funciones

En determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo sus funciones, se podrán designar Administradores de Seguridad del Sistema Delegados.
Los Administradores de Seguridad del Sistema Delegados serán responsables, en su ámbito, de aquellas acciones que delegue el Administrador de Seguridad del Sistema relacionadas con la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
El Administrador de Seguridad del Sistema Delegado será designado a solicitud del Administrador de Seguridad del Sistema, del que dependerá funcionalmente.
La delegación de funciones pasará previamente por el comité.
Su identidad aparecerá reflejada en la documentación de seguridad del sistema de información.

6.2.6 Responsable en materia de Protección de Datos

6.2.6.1 Designación o no de un Delegado de Protección de Datos:

El artículo 37 del RGPD establece que el responsable y el encargado del tratamiento deben designar un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

En este caso, NexTReT no cumple ninguno de los requisitos anteriores, por lo que no necesita establecer la figura del Delegado de Protección de Datos.

Sí existe, sin embargo, el Responsable en materia de protección de datos, que tiene encomendadas funciones similares a las que se le atribuye a un Delegado de Protección de Datos.

6.2.6.2 Artículo 39 del RGPD:

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o el encargado del tratamiento y los empleados que se ocupen del tratamiento, de las obligaciones que les incumben en virtud de este Reglamento y otras disposiciones de protección de datos de la Unión o de los estados miembros.

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

c) ofrecer el asesoramiento que se le pida sobre la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del reglamento.

d) cooperar con la autoridad de control.

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del reglamento, y realizar consultas, en su caso, sobre cualquier otro asunto.

6.2.6.3 Según el RGPD, la posición del DPO / DPD comporta:

- La participación de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
- Recibir el apoyo del responsable o encargado, que deberán facilitarle los recursos necesarios para el cumplimiento de sus funciones.
- No recibir ninguna instrucción en cuanto al ejercicio de estas funciones y no ser destituido ni sancionado por el responsable o el encargado por causas relacionadas con este ejercicio de funciones.
- Rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado.
  Esta característica debe interpretarse en el sentido de que el DPD debe poder relacionarse con niveles jerárquicos que tengan la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones que realice el DPD.

7. Datos de Carácter Personal

NexTReT trata datos de carácter personal. *Ver:* ***Registro de Actividades del Tratamiento (RAT)*** donde se recogen los ficheros afectados y los correspondientes responsables. Todos los sistemas de información de NexTReT se ajustarán a los niveles de seguridad requeridos por la normativa, a fin y efecto, de la naturaleza y finalidad de los datos de carácter personal recogidos.

8. Gestión de Riesgos

8.1 Justificación

Todos los sistemas sujetos a esta Política tendrán que realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los cuales están expuestos.
El análisis de riesgos será la base para determinar las medidas de seguridad que se tienen que adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según el previsto en el Artículo 7 del ENS y la ISO 27001.

8.2 Criterios de evaluación de 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.
Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.
Tendrán que tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.
Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de los servicios prestados.

8.3 Directrices de tratamiento

El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8.4 Proceso de Aceptación del Riesgo Residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.
Los niveles de Riesgo residuales esperados sobre cada Información después de la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) tendrán que ser aceptados previamente por su Responsable de esta Información.
Los niveles de Riesgo residuales esperados sobre cada Servicio después de la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) y la ISO 27001 y tendrán que ser aceptados previamente por el Responsable de este Servicio.
Los niveles de Riesgo Residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, porque este proceda, si procede, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

8.5 Necesidad de realizar o actualizar evaluaciones de riesgos

El análisis de los riesgos y su tratamiento tiene que ser una actividad repetida regularmente, conforme lo que establece en el Artículo 7 del ENS y la ISO 27001. Este análisis se repetirá:

- Regularmente, al menos una vez en el año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.

- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

9. Obligaciones del Personal

Todos los miembros de la Organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.
El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos de la organización, constituyendo su incumplimiento, infracción grave a efectos laborales, conforme al convenio colectivo laboral.

Ver la Normativa de Seguridad: *(PL-SGSI-04) FOP - Funciones y Obligaciones del Personal*

10. Formación y Concienciación del Personal

El objetivo de NexTReT es concienciar de forma continua en la Ciberseguridad a los empleados, para ello, se realizan:

- Formación inicial a la incorporación de los empleados a la organización
- Envío trimestral de píldoras de concienciación en Ciberseguridad.
- Envío puntual de píldoras informativas de Ciberseguridad, respondiendo a situaciones de riesgo.
- Formación anual a todo el personal de actualización en Ciberseguridad.
- Formación específica según el puesto de trabajo y necesidades concretas.
- Realización esporádica de campañas de simulación de phishing, con una periodicidad mínima bianual.

La Dirección se compromete a la formación y concienciación del personal de NexTReT.

11. Terceras Partes

Cuando se presten servicios o se gestione información otras organizaciones, se los hará partícipes de esta Política de Seguridad de la Información, se establecerán canales de reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando se utilicen servicios de terceros o ceda información a terceros, se los hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad (FOP) que concierna a estos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en esta 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 establece en esta Política.
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se

incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

12. Revisión y Aprobación de la Política de Seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.
Los cambios sobre la Política de Seguridad de la Información tendrán que ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11, en el Capítulo III Artículo 12 del ENS y la ISO 27001. Cualquier cambio sobre la misma tendrá que ser difundido a todas las partes afectadas.

La Política de Seguridad estará Notificada, Comunicada y disponible para todo el personal de NexTReT.

13. Referencias

- PL-SGSI-04) FOP - Funciones y Obligaciones del Personal
- (PR-SEG-03) Cuerpo normativo – Seguridad en la Operativa
- Funciones y Responsabilidades - Matriz RACI.
- (FR-SGSI-09) Marco normativo seguridad.
- (PR-SEG-01) Protocolo Actuación Incidentes de Seguridad.

Control de Versiones

Versión	Fecha	Editor	Descripción
5.0	21/09/2022	XBO	Adaptación de la Política a los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), Marco Normativo y revisión de todos los apartados.
4.0	28/04/2022	XBO	Cambios en el apartado 3. Alcance, apartado 6.2 Definición de roles, adecuación a la ISO 27001, Revisión y cambios en todos los apartados.
3.0	22/04/2021	XBO	Cambios en el apartado 3. Alcance.
2.0	25/03/2021	XBO	Cambios en los apartados 5. Marco Normativo y se añaden los apartados 6.2.6 Delegado de Protección de Datos y 10. Formación y Concienciación del Personal.
1.0	10/09/2020	XBO	Versión inicial.