Política de Seguridad bajo el Esquema Nacional de Seguridad - Diciembre 2023 v1.1-

Table of contents:

1. Exposición de Motivos 3

2. Misión 4

3. Alcance 4

4. Marco Normativo 4

I. Procedimiento Administrativo 4

II. Protección de datos de carácter personal 4

III. Administración Electrónica 5

IV. Firma Electrónica 5

V. Seguridad de las Redes y de la información 5

5. Organización de Seguridad 6

6. Datos de carácter personal 17

7. Gestión de riesgos 18

8. Gestión de incidentes de seguridad 19

9. Obligaciones del personal 21

10. Formación y concienciación 21

11. Terceras Partes 22

12. Revisión y aprobación de la política de seguridad 23

13. Referencias 23

Version	Modified date	Approved Date	Author	Reason/Comments	Approval
1.0	10/19/2023	Pendent	Carmen Galea	First version Policy ENS	
1.1	12/15/2023	12/15/2023	Carmen Galea	Correction of internal audit findings	Daniel Rodríguez

1. Exposición de Motivos

Redtrust, como fabricante de software de gestión de certificados digitales, depende de los Sistemas TIC (Tecnologías de Información y Comunicaciones) para conseguir sus objetivos. El software Redtrust y los sistemas que los soportan deben ser desarrollados con diligencia, tomando las medidas adecuadas desde las fases de diseño para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada, de los productos desarrollados o de los servicios prestados.

El objetivo de la Seguridad de la Información es garantizar la resiliencia de la organización y su reputación, la calidad de la información y del software desarrollado, así como la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza en los incidentes.

Para defenderse de las amenazas, se requiere una estrategia capaz de adaptarse a los cambios en las condiciones del entorno. Esto implica que los departamentos tienen que aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de la calidad del software y los niveles de prestación de servicios, seguir, analizar y corregir las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes.

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.

Para todo ello, Redtrust cuenta con un Sistema de Gestión de la Seguridad de la información basado en el Esquema Nacional de Seguridad que sigue un ciclo de mejora continua

2. Misión

Redtrust es un fabricante europeo de software de gestión de certificados digitales que, en el ámbito de la prestación de sus servicios contribuye a satisfacer las necesidades de sus diferentes clientes, tanto de la Administración Pública como procedentes del Sector Privado, sirviendo con objetividad y diligencia los intereses generales. Como Empresa Privada, vela también, por la gestión de sus propios intereses.

3. Alcance

La presente Política aplica a:

- Los sistemas de información que dan soporte al software y los servicios de uso seguro, controlado y centralizado de los certificados digitales.

4. 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 lo 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.

I. Procedimiento Administrativo

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

II. 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.

III. 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 servicio electrónicos de confianza.

IV. 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.

V. 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.

5. Organización de Seguridad

I. Comité: Funciones y Responsabilidades

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

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

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 Ley 11/2007.
- Asunción de la figura de responsable de la Información para todas las informaciones empleadas por los servicios prestados en el marco de la Ley 11/2007.
- 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 para que 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 respecto. 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, con sus dotaciones presupuestarias correspondientes. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- 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, 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.
- El Comité de Seguridad de la Información no es un comité técnico, pero, en caso de ocurrencia de incidentes de Seguridad 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.

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.

II. Responsable de la información

Corresponde al 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 han sido asumidas por el Comité de Seguridad de la Información y las personas que lo componen son identificadas en un acta generada por nuestra organización.

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.

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 coincidirá 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.

III. 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 General, 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 han sido asignadas al Comité de Seguridad de la Información que a su vez 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.

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.

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.

IV. Responsable de seguridad de la información

Ha sido nombrada formalmente como tal a una única persona en la organización mediante acta.

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.

En caso de ocurrencias de incidentes de seguridad de la información

Analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.

Compatibilidad con otros roles

Este rol únicamente podría llegar a 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 coincidirá con el de responsable de Sistema y el de Administrador de Seguridad del Sistema.

Delegación de funciones

En situación de que nuestro Sistema de Información adquiriera una mayor 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/la 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.

V. Responsable del sistema

Corresponde al nivel de una Dirección Operativa.

Se nombra formalmente como tal a una única persona para cada Sistema. El rol no será desarrollado por un órgano colegiado, aunque pueda delegar parte de sus funciones en otras personas

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 que serán 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.
- Planificará la implantación de las salvaguardas en el sistema.

En caso de ocurrencia de incidentes de seguridad de la información

Supervisará las acciones de mitigación de impacto y restauración de las operaciones de acuerdo con los planes aprobados.

Compatibilidad con otros roles

Este rol no coincidirá con el de responsable de Información, con el de responsable de Servicio.

No obstante, este rol podría coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o media que tengan una estructura autónoma de funcionamiento.

VI. Administrador de la seguridad del sistema

Corresponde al nivel de un empleado calificado en seguridad informática de sistemas. Se nombra formalmente como tales al equipo de IT.

El rol no se desarrollará por un órgano colegiado (dada nuestra magnitud, no consideramos el equipo de IT como órgano colegiado sino como dos personas responsables de la administración), ni delegará parte de sus funciones en otras personas.

Si procede, se nombrarían nuevos Administradores de la Seguridad del Sistema en caso de que se incremente el tamaño de Redtrust.

Será propuesto por el responsable del Sistema, a quien reportará en todo lo relacionado con Seguridad de la Información.

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.
- Verificar el correcto funcionamiento de los Sistemas de Información tras la realización de cambios en las configuraciones vigentes, 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.

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.

Compatibilidad con otros roles

Este rol no coincidirá con el de responsable de Información, con el de responsable de Servicio ni con el de responsable de Seguridad Corporativa o de la Información.

Delegación de funciones

En caso de que nuestro sistema de información aumentase su complejidad, distribución, separación física de sus elementos o número de usuarios requieran 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.

VII. Responsable en materia de protección de datos

En Redtrust confiamos en ofrecer todas las garantías necesarias de seguridad de la información. Es por ello que optamos por disponer de, no solo un responsable de protección de datos sino una Delegada de protección de datos designada ante la AEPD.

Designación o no de un delegado de protección de datos

Según lo que establece el artículo 37 del RGPD, el responsable y el encargado del tratamiento deben designar un Delegado de Protección de Datos siempre que:

- el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
- las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, debido a su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- 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.

Pese a que Redtrust no cumple ninguno de los requisitos anteriores, por lo que no se necesitaría establecer la figura del Delegado de Protección de Datos sí ha sido voluntad de la organización la designación de esta figura (cuya verificación puede realizarse ante la consulta DPD de la propia AEPD).

Funciones

Según lo establecido por el 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.

Asimismo, según el RGPD, la posición del DPO/DPD comporta para nosotros:

- 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.

6. Datos de carácter personal

Redtrust trata datos de carácter personal.
Disponemos de Registro de Actividades del Tratamiento (RAT que ha sido realizado con un modelo RoPA con análisis de criticidad de los datos tratados por nuestra organización) donde se recogen los ficheros afectados y los correspondientes responsables. Todos los sistemas de información de Redtrust 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.

7. Gestión de riesgos

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.

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.

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.

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 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.

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. 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.

8. Gestión de incidentes de seguridad

Prevención

Los departamentos tienen que evitar, o al menos prevenir en lo posible, que la información, los productos desarrollados o los servicios prestados 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, 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.

Detección

Dado que los sistemas se pueden degradar rápidamente a causa de incidentes, que van desde una simple desaceleración de las operaciones hasta su detención o, paralelamente, pueden producirse modificaciones no autorizadas en el código desarrollado, con potencial afectación a múltiples clientes de Redtrust, deben establecerse mecanismos de monitorización continua para detectar anomalías en los niveles de prestación de dichos servicio, así como cambios o accesos no autorizados a los repositorios de código y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

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.

Respuesta

Redtrust, a través de sus diferentes departamentos:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto único de contacto para las comunicaciones en cuanto a incidentes detectados dentro de la organización o bien a aquellos que afecten a otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT)

Recuperación

Para garantizar el correcto restablecimiento de los servicios, Redtrust desarrolla Planes de Continuidad de los sistemas TIC como parte de su Plan General de Continuidad de Negocio y las correspondientes actividades de recuperación.

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.

Nuestra Normativa de Seguridad: 00 – Redtrust Controles y Políticas ENS.

10. Formación y concienciación

El objetivo de Redtrust 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 periódico de píldoras de concienciación en Ciberseguridad.
- Envío periódico 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.

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

11. Terceras Partes

En Redtrust adquirimos un especial compromiso:

- Cuando se presten servicios o se gestione información de otras organizaciones, se les 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 les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad 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 nuestra Política de Seguridad de la Información serán aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11, en el Capítulo III Artículo 12 del ENS, en nuestro caso es aprobada por la dirección general mediante acta.

Cualquier cambio sobre la misma tendrá que ser difundido a todas las partes afectadas.

La Política de Seguridad esta Notificada, Comunicada y disponible para todo el personal de Redtrust.

13. Referencias

- 00 – Redtrust – Controles y Políticas ENS (considerada nuestra Normativa de Seguridad)
- Funciones y Responsabilidades - Matriz RACI y Job Codes and Descriptions.