POLÍTICA DE SEGURIDAD

DOCUMENTO Nº:	FECHA:
NVI24-Q-ENS003_ED01	**25.10.2024**

Preparado por:	Revisado y aprobado por:	
Inmaculada Huertas	Virgilio García	Fernando Lasagni
HUERTAS OLIVARES INMACULADA MONTEMAYOR - 44201247P Firmado digitalmente por HUERTAS OLIVARES INMACULADA MONTEMAYOR - 44201247P Fecha: 2024.10.25 14:12:17 +02'00'	GARCIA ORGEIRA VIRGILIO - 71650237Q Firmado digitalmente por GARCIA ORGEIRA VIRGILIO - 71650237Q Fecha: 2024.10.27 19:39:47 +01'00'	LASAGNI FERNANDO ADRIAN - X7103487Y Digitally signed by LASAGNI FERNANDO ADRIAN - X7103487Y Date: 2024.10.28 09:33:49 +01'00'

NVI-FO7-14_ED01

CONTROL DE EDICIONES

Ed.	Fecha	Control de ediciones
01	25.10.2024	Implantación del Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad (ENS)

ÍNDICE

1. OBJETO Y ALCANCE

Texto aprobado el día 25 de octubre de 2024 por la Dirección General NOVAINDEF

Esta Política de Seguridad de la Información (en adelante, Política de Seguridad) entrará en vigor el día posterior a la fecha anteriormente indicada y hasta que sea reemplazada por una nueva política.

2. OBJETO

NOVAINDEF considera la información un activo esencial para el cumplimiento adecuado de sus funciones. Buena parte de la información contenida en los sistemas de información de las AA.PP. y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

En su esfuerzo por asegurar que los servicios ofrecidos a través de medios electrónicos a los clientes sean proporcionados con niveles de seguridad equivalentes a los experimentados cuando interactúan en persona en las instalaciones de la empresa, NOVAINDEF desarrolla y aprueba esta Política de Seguridad de la Información, aplicando las medidas mínimas de seguridad exigidas por el ENS en lo referente a:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Las diferentes áreas y servicios deben cerciorarse de que la seguridad de la información es una parte vital de los servicios públicos prestados por NOVAINDEF, y ha de custodiar dicha información en todo su ciclo de vida (recogida, transporte, tratamiento, almacenamiento y destrucción). Las áreas y servicios deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, garantizando así la continuidad en la prestación de los servicios con una calidad y seguridad adecuada.

Esta Política de Seguridad asegura un compromiso manifiesto de las máximas autoridades de la entidad para la difusión, consolidación y cumplimiento de la presente Política.

3. ALCANCE

La presente Política de Seguridad tiene aplicación a todas las áreas, servicios, empleados internos y externos de NOVAINDEF, cualquiera que sea su clasificación jerárquica. Igualmente, aplica a todos los sistemas de la información e infraestructuras de comunicación utilizadas para la realización de las funciones propias de NOVAINDEF.

Con esta política de seguridad de la información, la organización muestra su compromiso por establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de acuerdo con los principios recogidos en el artículo 5 del Real Decreto 311/2022. Esto es:

- Entender la seguridad como un proceso integral.
- Gestionar la seguridad basándonos en los riesgos.
- Monitorizar y vigilar continuamente los eventos de seguridad para garantizar la prevención, detección, respuesta y conservación.
- Establecer defensas
- Evaluar el estado de la seguridad periódicamente
- Realizar una diferenciación clara de las responsabilidades

4. MISIÓN Y OBJETIVOS

NOVAINDEF, en el empeño por cumplir los intereses, funciones y competencias encomendadas, pone a disposición de sus clientes los servicios y actividades necesarias para satisfacer las aspiraciones e intereses de dichos clientes. NOVAINDEF hace uso de las tecnologías apropiadas y pone en valor la relación electrónica con sus clientes, creando la confianza necesaria basada en un sistema de seguridad de la información integral y que alcanza a toda la empresa

Estos sistemas pretenden garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. Para ello, se establecen como objetivos generales en materia de seguridad de la información los siguientes:

1. Disponer de las medidas de control necesarias para el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada, especialmente en lo relativo a la protección de datos personales y a la prestación de servicios a través de medios electrónicos.
2. Asegurar el acceso, integridad, confidencialidad, disponibilidad, autenticidad, trazabilidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con rapidez a los incidentes.
3. Proteger los recursos de información de la entidad y la tecnología utilizada para su procesamiento frente a amenazas, internas o externas, deliberadas o accidentales.
4. Proporcionar confianza a los clientes protegiendo su información durante todo su ciclo de vida.
5. Facilitar la mejora continua de los procesos de seguridad, procedimientos, productos y servicios.
6. Garantizar la continuidad de la entidad estableciendo proyectos de contingencia en los servicios críticos y manteniendo en todo momento la seguridad.
7. Concienciar, formar y motivar al personal sobre la importancia de la seguridad en el entorno del trabajo.

5. MARCO NORMATIVO

Este Esquema Nacional de Seguridad (ENS), regulado actualmente por el Real Decreto 311/2022, de 3 de mayo determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione en el ejercicio de sus competencias.

El Esquema Nacional de Interoperabilidad (ENI), regulado por el Real Decreto 4/2010, de 8 enero, establece el conjunto de criterios y recomendaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que

garanticen la interoperabilidad. Las normas técnicas complementarias de interoperabilidad desarrollan ciertos aspectos técnicos.

Las Leyes 39/2015 y 40/2015 regulan el Procedimiento Administrativo Común y el Régimen Jurídico de las Administraciones Públicas. Dentro de estas leyes se hace referencia expresa al ENS como sistema de gestión segura de la información para las administraciones y al ENI como referencia en la interoperabilidad de las administraciones.

[Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, por la que se regulan los procedimientos de contratación de las Administraciones Públicas]

Así mismo, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales, tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, además de garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

El Reglamento (UE) 2016/679, de 27 de abril de 2016, de Tratamiento de Datos de Carácter Personal y Libre Circulación de Datos establece la obligación de disponer medidas técnicas y organizativas para garantizar la confidencialidad, disponibilidad e integridad de la información. Así mismo dispone que dichas medidas han de ser proactivas y el responsable del tratamiento ha de ser capaz de demostrar que se siguen esas medidas y demostrar su aplicación.

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión en la que se establecen las obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información; establecer requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales.

El Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información que asegura la alineación del derecho español con el marco armonizado europeo conforme a la Directiva 2016/1148 (Directiva NIS).

Con este Real Decreto se pretende concretar algunas de las principales obligaciones y procedimientos a utilizar a fin de asegurar una óptima gestión de riesgos de seguridad en

redes y sistemas de información en sectores críticos, así como para asegurar una adecuada coordinación entre los distintos actores implicados en este tipo de situaciones de riesgo. Para ello, se han establecido una serie de obligaciones organizativas y de actuación para los operadores sujetos a este régimen, como son la definición de medidas técnicas y organizativas para la adecuada gestión de los riesgos de ciberseguridad, designación de un responsable de seguridad, notificación y gestión de incidentes de seguridad.

La ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

Asimismo, en el documento ENS.REG.05 CM Cuadro de mando se llevará a cabo la revisión y actualización del marco regulatorio conforme indica la norma de cumplimiento normativo. El mismo se revisará de forma periódica anualmente, así como de forma extraordinaria cuando tenga lugar algún cambio que obligue a la actualización y revisión de estas.

6. ORGANIZACIÓN DE SEGURIDAD

Para gestionar y coordinar proactivamente la seguridad de la información se constituye como órgano de gestión el **COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**.

Este Comité estará constituido por los siguientes cargos:

RESPONSABLE DE LA INFORMACIÓN

Determinará los requisitos de la información tratada.

Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. Asesorará y tendrá potestad para determinar técnicamente los requisitos de la información y de los servicios en materia de seguridad. Tendrá la potestad, igualmente, de determinar los niveles de seguridad de la información.

Así mismo informará sobre el estado de la seguridad en el área de los sistemas de la información y comunicación. Podrá convocar las reuniones, remitir información y comunicados a los miembros de la comisión.

RESPONSABLE DE SERVICIO

Determinará los requisitos de los servicios prestados.

Será la persona o personas responsables de la explotación de las distintas áreas de la entidad estableciendo requisitos, fines y medios para la realización de dichas tareas. Determinará los requisitos de seguridad de los servicios prestados. Esto incluye la responsabilidad de determinar los niveles de seguridad de los servicios y para ello, podrá recabar asesoramiento del responsable de seguridad y del responsable del sistema.

Incluirá las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control. Tendrá, además, la misión de valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios, teniendo en consideración la repercusión en la capacidad de NOVAINDEF SL para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Además, tendrán la obligación de vigilar el cumplimiento de las normas de seguridad dentro de su área e informar al responsable de la Información del cumplimiento de la normativa de seguridad aprobada por el Comité de Seguridad.

RESPONSABLE DE LA SEGURIDAD

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

Es la persona designada por el máximo órgano de gobierno para la supervisión del sistema de seguridad de la información y será el encargado de determinar las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios.

Las dos funciones esenciales del Responsable de la Seguridad son:

a. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en esta Política de Seguridad de la Información de la organización.
b. Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios así lo requiriera, NOVAINDEF podrá designar responsables de Seguridad delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos responsables de Seguridad delegados tendrán dependencia directa del Responsable de Seguridad.

Entre las funciones que se le atribuyen al Responsable de Seguridad, se encuentran las siguientes:

- Coordinará y controlará las medidas definidas en el Registro de Actividades del Tratamiento y en general se encargará del cumplimiento de las medidas de seguridad que detalla el informe de evaluación de impacto en la protección de datos.
- Reportará directamente al Comité de Seguridad de la Información.
- Asumirá las funciones del Secretario del Comité de Seguridad de la Información.
- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y realizará la categorización 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 Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras 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, de la Política de Seguridad de la Información, para su aprobación por parte de los Órganos de Gobierno municipales.
- 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 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.
- Analizará y propondrá salvaguardas que prevengan incidentes similares en caso de que estos se hubieran producido.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información.
- Elaborará los Planes de Continuidad de Sistemas que deberán 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.

RESPONSABLE DEL SISTEMA

Se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados. Sus funciones, de manera concreta, son las siguientes:

a. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
b. Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
c. Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
d. El Responsable del Sistema puede acordar la suspensión del manejo 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 debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.

e. Aplicar los procedimientos operativos de seguridad elaborados y aprobados por el Responsable de Seguridad.
f. 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.
g. Realizar ejercicios y pruebas periódicas de los Planes de Continuidad del Sistema para mantenerlos actualizados y verificar que son efectivos.
h. 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.

Si el sistema de información, dado su complejidad, distribución, separación física o número de usuarios requiriera personal adicional para el desempeño de estas funciones, NOVAINDEF podrá designar responsables del Sistema delegados, en los que se podrá delegar funciones, pero nunca responsabilidades. Estos responsables del Sistema delegados tendrán dependencia directa del Responsable del Sistema.

ADMINISTRADOR DE SEGURIDAD

Sus funciones más significativas serían las siguientes:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
b. 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.
c. La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
d. La aplicación de los Procedimientos Operativos de Seguridad (POS).
e. Asegurar que los controles de seguridad establecidos son adecuadamente observados.
f. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

g. 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.
h. 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.
i. Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
j. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Esta función será asumida por la figura del Responsable del Sistema.

SECRETARÍA

Tendrá la obligación de supervisar que los procedimientos aprobados por el Comité se ajusten a derecho, así como de asesorar al Comité en esta materia. Además, levantará acta de las reuniones. Esta función será asumida por la figura del Responsable de Seguridad.

DELEGADO DE PROTECCIÓN DE DATOS

Velará y asesorará para proteger el cumplimiento de los derechos de los interesados en materia de protección de datos.

NOMBRAMIENTOS

Los miembros de este Comité serán nombrados por Dirección general de NOVAINDEF y posteriormente se informará al resto de los empleados de NOVAINDEF, contemplando medidas transitorias con objeto de garantizar el cumplimiento de la seguridad.

Además, las futuras resoluciones de nombramientos de responsables de áreas, responsables de entidad vinculada o cambios en la distribución de funciones de área y entidades deberán contemplar expresamente el nombramiento como miembro en este Comité de Seguridad de la información.

6.1 FUNCIONES DEL COMITÉ DE SEGURIDAD

Sus funciones son las siguientes:

- Responsabilidades derivadas del tratamiento de datos personales.
- Atender las inquietudes de la Corporación y de las diferentes áreas.
- Informar regularmente del estado de la seguridad de la información al órgano superior de gobierno.
- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de NOVAINDEF en lo que respecta 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 el propio Comité de Seguridad antes de su aprobación final en pleno.
- Aprobar la normativa de seguridad de la información.
- Evaluar los riesgos de manera periódica para establecer las adecuadas medidas de seguridad necesarias atendiendo a los resultados.
- 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 NOVAINDEF y recomendar posibles actuaciones respecto de ellos.
- 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.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- 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 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.
- Establecer medidas adecuadas para la formación, información y concienciación de todo el personal en materia de seguridad de la información y protección de datos de carácter personal.
- 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.
- En caso de ocurrencia de incidentes de seguridad de la información aprobará el Plan de Mejora de la Seguridad.

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 que 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.

6.2 GESTIÓN Y ESTRUCTURA DE LA DOCUMENTACIÓN

Se deberá comunicar la información documentada relativa a los controles de seguridad al personal que trabaja en NOVAINDEF (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del ENS.

La información documentada será clasificada en: pública o publicable, interna, confidencial y secreta, dando el uso adecuado de acuerdo con dicha clasificación y según el criterio que se establezca en la normativa de clasificación de la información.

Un procedimiento definirá los criterios de etiquetado de los documentos que formen parte del Sistema de información.

Así, la documentación que compone dicho sistema se distribuye de la siguiente manera.

1. Política de Seguridad de la Información: Conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.
2. Normativa: Marco regulatorio que contiene las conductas permitidas o prohibidas, así como también define el alcance, conceptos básicos, marco, responsabilidades y objetivos de una determinada medida o conjunto de medidas.
3. Procedimiento: Protocolos que definen y detallan procesos y mecanismos, o fases que desarrollan las diferentes acciones para la consecución de un determinado resultado.
4. Registros: Se trata de herramientas y tablas que recopilan datos e indicadores con los que monitorizar el cumplimiento de un control o evaluar la eficacia de este.

Este mismo orden determina la jerarquía y prelación de estos documentos.

Se pondrá a disposición de los miembros de la organización, los documentos que le sean de interés, siendo igualmente comunicado tanto en el proceso de onboarding, como en la formación inicial.

Asimismo, en el registro *NVI24-Q-ENS001 Índice general de la documentación ENS*, se recopilarán todos los documentos que forman parte del catálogo del sistema objeto de esta política, el Responsable de Seguridad es el responsable de mantener y actualizar la documentación del sistema.

7. CONCIENCIACIÓN

NOVAINDEF establecerá los mecanismos necesarios, atendiendo a las propuestas del Comité de Seguridad, para que todo el personal disponga de la información, formación y concienciación apropiada para gestionar de acuerdo con esta Política de Seguridad y su normativa interna derivada la información, tanto en materia de privacidad como de seguridad.

El Comité establecerá mecanismos adecuados de difusión de la información y registrará todas las acciones formativas que se dispongan en este sentido.

8. GESTIÓN DEL RIESGO

NOVAINDEF realizará periódicamente y cada vez que los sistemas de la información sufran una alteración significativa un Análisis de Riesgos, siguiendo las directrices expuestas por el ENS en su artículo 6, de modo que se puedan anticipar los riesgos existentes. Este Análisis de Riesgos y sus conclusiones han de ser analizadas por el Comité de Seguridad y establecer las salvaguardas adecuadas para que el nivel de riesgo sea aceptable.

Para que esto se plasme el Comité desarrollará un procedimiento de Análisis de Riesgos y Evaluación de Impacto Potencial que ha de establecer claramente los valores de riesgo aceptables, los criterios de aceptación de riesgo residual, la periodicidad del análisis y cuándo se realizará de modo excepcional.

El análisis de riesgos que realice NOVAINDEF atenderá igualmente y de manera concreta a aquellos que se deriven del tratamiento de los datos personales en el desempeño de sus funciones.

9. PROTECCIÓN DE DATOS PERSONALES

NOVAINDEF únicamente recogerá datos personales cuando sean adecuados, pertinentes y no excesivos, y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas técnicas y organizativas pertinentes para el cumplimiento de la legislación en materia de protección de datos.

Estas medidas, tal y como se indica en la disposición adicional primera de la Ley 3/2018 de 5 de diciembre, sobre Protección de Datos y Garantía de Derechos Digitales, se corresponderán con las descritas en el Esquema Nacional de Seguridad, que estará definidas en las políticas, normativas y procedimientos que correspondan.

10. APROBACIÓN Y REVISIÓN DE ESTA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad ha de ser un documento que refleje fielmente el compromiso de NOVAINDEF y entidades vinculadas con la seguridad de la información. Por lo tanto, esta política podrá ser modificada a propuesta del Comité de Seguridad para adaptarse a cambios en el entorno legislativo, técnico u organizativo. Tanto la aprobación inicial de esta política como la revisión futura de la misma, se realizará por el órgano superior competente de la entidad tras propuesta del comité de seguridad de la información.