Índice:

Todas las personas que forman parte de NASERTIC tienen la obligación de conocer y cumplir esta Política de Seguridad siendo responsabilidad de NASERTIC disponer los medios necesarios para que la información llegue a las personas (tanto propias como subcontratadas) o servicios afectados. Este alcance cubre todos los activos de información, sistemas, procesos y personal bajo el control de NASERTIC.

1 OBJETIVOS/MISIÓN DE LA ORGANIZACFIÓN.

Nasertic ha determinado sus señas de identidad durante la reflexión y elaboración del PLAN ESTRATEGICO 2024-2028.

Establecimos nuestro PRÓPOSITO:

> GENERAMOS VALOR PARA NAVARRA A TRAVÉS DE LA INNOVACIÓN, EL CONOCIMIENTO Y LA TECNOLOGÍA PARA OFRECER NUEVAS SOLUCIONES PARA LOS SERVICIOS, LA ATENCIÓN A LA CIUDADANÍA Y LA GESTIÓN DE SUS INFRAESTRUCTURAS ASOCIADAS.

Este Propósito refleja nuestro claro compromiso para trabajar conjuntamente y de forma innovadora para encontrar nuevas soluciones a nuevos problemas con talento, con infraestructuras, con tecnología, con servicios por y para las personas

También revisamos nuestra VISIÓN, introduciendo sensibles modificaciones en cuanto a servicios y relaciones, consensuándola finalmente como:

> SER EL SOCIO REFERENTE EN INFRAESTRUCTURAS TECNOLÓGICAS Y SERVICIOS TRANSVERSALES DEL GOBIERNO DE NAVARRA SIENDO UN AGENTE FACILITADOR DE PROYECTOS ESTRATÉGICOS PARA EL DESARROLLO SOSTENIBLE DE NUESTRA REGIÓN.

La visión define las metas que pretendemos conseguir a corto plazo. Estas metas son realistas y alcanzables, puesto que la propuesta de visión tiene un carácter inspirador y motivador

Nuestros VALORES muestran cómo somos y cómo hacemos posible tanto el propósito como la visión. Son los principios profesionales que construyen nuestra identidad, representan nuestra cultura de empresa y guían nuestras relaciones internas y externas. Además, constituyen nuestra filosofía y orientan nuestras decisiones y conductas.

La lista de valores a seguir, son, pues, los siguientes:

- FLEXIBILIDAD.
- COMPROMISO Y RESPONSABILIDAD
- CALIDAD TÉCNICA Y PROFESIONALIDAD
- EFICIENCIA Y PRODUCTIVIDAD.
- TRABAJO EN EQUIPO.

El Marco Estratégico 2024-2028 señala los siguientes objetivos estratégicos:

1) Lograr que los servicios que ofrece Nasertic sean reconocidos como útiles por la ciudadanía.
2) Fomentar la compartición y el uso eficiente de infraestructuras y tecnología en Navarra.
3) Contribuir al desarrollo de nuevos ecosistemas público-privados.
4) Mejorar la experiencia de cliente en la prestación de los servicios.
5) Contribuir al fortalecimiento del sector privado en el ámbito de nuestras actividades.
6) Lograr la sostenibilidad económica en la inversión en infraestructuras y tecnologías.
7) Invertir en infraestructuras y tecnología que cubran las necesidades de agentes y sociedad.
8) Garantizar la estabilidad financiera y contribuir al desarrollo de CPEN.
9) Sumar eficazmente al desarrollo sostenible de Navarra y al equilibrio territorial.
10) Contribuir a que Navarra sea referente social en innovación, infraestructura y tecnología.

2 MARCO REGULATORIO

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), en adelante RGPD, de plena aplicación a partir del 25 de mayo de 2018, establece en su artículo 24, dentro de las obligaciones generales del responsable del tratamiento de datos personales, que, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado reglamento. Así mismo, dispone que dichas medidas se revisarán y actualizarán cuando sea necesario y que, cuando sean proporcionadas en relación con las actividades de tratamiento, entre dichas medidas se incluirá la aplicación por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

En el mismo sentido, el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPDGDD, referido a las obligaciones generales del responsable y encargado del tratamiento, establece que dichos responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del RGPD, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que

el tratamiento es conforme con el citado reglamento, con la LOPDGDD, sus normas de desarrollo y la legislación sectorial aplicable.

La disposición adicional primera de la LOPDGDD dispone que en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad, en adelante ENS. El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (que actualiza y deroga el Real Decreto 3/2010), tiene por objeto determinar la política de seguridad de la información en la utilización de los medios electrónicos por las entidades de su ámbito de aplicación.

El artículo 12 del ENS exige que todos los órganos superiores de las Administraciones Públicas, y las entidades con política de seguridad propia, dispongan formalmente de su política de seguridad, que se aprobará por la persona titular del órgano superior correspondiente o el órgano competente en el caso de otras entidades. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II del ENS (seguridad integral, gestión de riesgos, prevención, detección, respuesta y conservación, existencia de líneas de defensa, vigilancia continua y reevaluación periódica, y diferenciación de responsabilidades) y se desarrollará aplicando los requisitos mínimos consignados en el ya mencionado artículo 12.6.

Adicionalmente, la norma internacional UNE-ISO/IEC 27001:2022 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI).

La presente política de seguridad establece las pautas generales para asegurar el cumplimiento de las obligaciones del tratamiento de datos de carácter personal, así como la gestión de la seguridad de la información de manera integrada y coordinada con los requerimientos propios de las actividades de NASERTIC.

3 NORMATIVA DE SEGURIDAD

Normativa Aplicable (Nivel de Seguridad: Medio)
El Sistema de Seguridad adoptado por la organización se fundamenta en el marco regulatorio y técnico definido por el Esquema Nacional de Seguridad (ENS). Para un nivel de seguridad medio, se aplican las disposiciones generales del ENS y las medidas específicas correspondientes a este nivel. La normativa aplicable es la siguiente:

1.- Legislación y normativa aplicable.

- Le 39/2015, de 1 de Octubre de Procedimiento Administrativo Común de las Administraciones Públicas.
- Lewy 40/215 de 1 de Octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, que establece los principios básicos, requisitos mínimos y el

catálogo de medidas aplicables a sistemas clasificados en los niveles Bajo, Medio y Alto.

- Resolución de 13 de Octubre de 2016, la Secretaría de Estado de las Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Plan Nacional de Seguridad.
- Resolución del 7 de Octubre de 2016, la Secretaría de Estado de las Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad del Estado de la Seguridad.
- Resolución de 27 de Marzo de 2018, de la Oficina de Estado de la Función Pública, mediante la cual se aprueba la Instrucción Técnica de Seguridad de auditoría de la seguridad de los sistemas de información.
- Resolución de 13 de Abril de 2018 de la Secretaría de Estado de Función Pública, mediante la cual se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Real Decreto 4/2010 de 8 de Enero por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito del Gobierno Electrónico.
- Real Decreto 1671/2009 de 6 de Noviembre por el que se desarrolla parcialmente la Ley 11/200, de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de Abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD).
- Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y del comercio electrónico.
- Ley 37/2007, de 16 de Noviembre de reutilización de la información del sector público.
- Ley 1972013 de 9 de Diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2007 de 18 de Octubre de conservación de datos relativos a las redes de comunicaciones electrónicas y comunicaciones públicas.
- Ley 56/2007, de 28 de Diciembre, de medidas de promoción de la Sociedad de la Información.
- Ley 9/2014, de 9 de Mayo, de telecomunicaciones generales.
- Ley 7/1985 de 2 de Abril, reguladora de las Bases de Régimen Local, modificada por la Ley 11/1999 de 21 de Abril.

- Real Decreto Legislativo 1/1996 de 12 de Abril, por el que se aprueba el Texto Revisado de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015 de 30 de Octubre por el que se aprueba el texto revisado de la Ley del Estatuto Básico de los Empleados Públicos.
- Ley 59/2003. De 19 de Diciembre de firma electrónica.

2.- Normativa técnica y guías de referencia para nivel medio

Las siguientes guías complementan las obligaciones establecidas para un nivel de seguridad medio:

- Guías CCN-STIC de la Serie 800, que proporcionan directrices técnicas de aplicación del ENS en materia de gestión de riesgos, arquitectura segura, seguridad en la nube, monitorización y medidas de protección asociadas al nivel medio.
- Instrucciones Técnicas de Seguridad (ITS) emitidas por el Centro Criptológico Nacional (CCN), que desarrollan aspectos obligatorios para la aplicación del ENS en un nivel de seguridad medio, tales como auditorías, informes de conformidad, interconexiones y notificación de incidentes.

Estas guías, si bien no son obligatorias, son consideradas referencia oficial para la correcta adecuación de las medidas ENS.

3.- Normativa relacionada en materia de seguridad y protección de datos

Estas normas, aunque externas al ENS, se consideran de aplicación complementaria y necesaria:

- Reglamento General de Protección de Datos (RGPD), aplicable cuando los sistemas gestionan datos personales y cuya aplicación debe alinearse con las medidas ENS de nivel medio.
- Directiva NIS, que establece requisitos de seguridad para redes y sistemas de información y refuerza la necesidad de medidas de nivel medio, especialmente en organizaciones que gestionen servicios esenciales o relevantes.
- ISO/IEC 27001, norma internacional de referencia que, aunque no obligatoria, sirve como marco complementario para la gestión de la seguridad y el diseño de controles acordes al nivel medio.

Área	Guía NIST SP 800	Por qué es útil
Gestión del riesgo	**SP 800-30**, **SP 800-37**	Prioriza y gestiona riesgos efectivos.
Controles de seguridad	**SP 800-53**, **SP 800-53B**	Base de controles (baseline *moderate*).

Gestión y gobernanza	**SP 800-100**	Marco organizativo y roles.
Pruebas técnicas	**SP 800-115**	Pentesting, evaluaciones, validación de controles.

4 ROLES O FUNCIONES DE SEGURIDAD

Responsable de la Información (RINFO)

El Responsable de la Información será el Director Gerente de la Organización que coordinará un equipo formado por todos los directores de las diferentes áreas.

FUNCIONES

- Responsable último del uso que se haga de una cierta información y, por tanto, de su protección ante cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Debe establecer los requisitos de la información en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.
- En la aprobación formal de los niveles de seguridad, debe recabar la propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- Los criterios de valoración para los niveles de seguridad deben estar respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- Aceptar los riesgos residuales después de la evaluación del riesgo.

Responsable de los Servicios (RSERV)

Los responsables de los diferentes servicios serán las personas que gestionan directamente cada uno de los servicios que presta Nasertic.

A modo de ejemplo y sin ser exhaustivo:

- Responsable de Laboratorio.
- Responsable de Área de Sistemas y CPD.
- Responsable de Mainframe.
- Responsable del Área de Servicios de Telecomunicación.
- …

FUNCIONES

- Debe establecer los requisitos del servicio en materia de seguridad. O, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios.
- En la aprobación formal de los niveles de seguridad, debe recabar la propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
- Los criterios de valoración para los niveles de seguridad deben estar respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- Aceptar los riesgos residuales después de la evaluación del riesgo.

Responsable de Seguridad (RSEG)

El responsable de Seguridad será el Responsable de los Sistemas de Gestión que compondrá un equipo de trabajo compuesto por personas de todas las áreas de la empresa.

FUNCIONES

- 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 la Política de Seguridad de la Organización.
- Elaborar la Política de Seguridad.
- Determinación de la categoría del sistema.
- Realización del Análisis de riesgos.
- Realización de la declaración de aplicabilidad.
- Definición de medidas de seguridad adicionales.
- Elaboración de la configuración de la seguridad.
- Documentación de la seguridad del sistema.
- Elaboración de las normativas de seguridad aplicadas.
- Aprobación de los procedimientos operativos de seguridad.
- Reportar a Dirección el estado de seguridad del sistema.
- Participación en la elaboración de los planes de mejora de la seguridad.
- Elaboración de los planes de concienciación y formación en materia de seguridad.
- Validación de los planes de continuidad.

- Aprobación de los ciclos de vida: especificación, arquitectura, desarrollo, operación, cambios

Responsable del Sistema (RSIS)

El Responsable del Sistema será el Responsable de Sistemas de IT, de la organización.

El Responsable de Sistema puede proponer en un futuro a la Dirección un Administrador de la Seguridad del Sistema (ASS) para la implementación, gestión y mantenimiento de las diferentes medidas de seguridad desde el punto de vista técnico.

FUNCIONES

- 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 de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- 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 el Responsable de la Seguridad, antes de ser ejecutada.
- Aplicación de la configuración de la seguridad junto con el Administrador de Seguridad del Sistema.
- Elaboración de los procedimientos operativos de seguridad.
- Monitorizar el estado de seguridad del sistema junto con el Administrador de Seguridad del Sistema.
- Participación en la elaboración de los planes de mejora de la seguridad.
- Elaboración de los planes de continuidad.
- Elaboración de los ciclos de vida: especificación, arquitectura, desarrollo, operación, cambios

5 DOCUMENTACIÓN, GESTIÓN DEL SISTEMA Y ACCESO.

5.1 Elementos del Sistema de Gestión

1) **Liderazgo y Compromiso:** La Dirección de NASERTIC demuestra liderazgo y compromiso con respecto al SGSI asegurando que la política y los objetivos de

seguridad son establecidos y compatibles con la dirección estratégica; asegurando la integración de los requisitos del SGSI en los procesos de la organización; asegurando la disponibilidad de recursos; comunicando la importancia de la gestión de la seguridad; asegurando que el SGSI logra sus resultados; dirigiendo y apoyando a las personas; y promoviendo la mejora continua.

2) **Objetivos de Seguridad de la Información:** NASERTIC establecerá objetivos de seguridad de la información en las funciones y niveles pertinentes. Estos objetivos serán coherentes con la política de seguridad, medibles (si es posible), tendrán en cuenta los requisitos aplicables y los resultados de la evaluación de riesgos, serán monitorizados, comunicados y actualizados según sea apropiado.
3) **Categorización de Sistemas y Medidas de Seguridad:** Los sistemas de información de NASERTIC serán categorizados (Bajo, Medio o Alto) según lo establecido en el Anexo I del ENS, en función del impacto valorado para las dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad, Autenticidad, Trazabilidad). Las medidas de seguridad a implantar, incluyendo los refuerzos que correspondan, se seleccionarán del Anexo II del ENS en función de dicha categorización y del resultado del análisis de riesgos.
4) **Declaración de Aplicabilidad:** Se elaborará y mantendrá una Declaración de Aplicabilidad (SoA) que contenga los controles necesarios (seleccionados del Anexo A de la ISO/IEC 27001 y el Anexo II del ENS), la justificación para su inclusión, si están implementados o no, y la justificación para cualquier exclusión de controles.
5) **Auditoría, Revisión por la Dirección y Mejora Continua:** El SGSI será sometido a auditorías internas a intervalos planificados para determinar si cumple con los requisitos propios de NASERTIC, de esta política, del ENS y de la norma ISO/IEC 27001, y si está implementado y mantenido eficazmente. La Dirección revisará el SGSI de NASERTIC a intervalos planificados para asegurar su continua idoneidad, adecuación y eficacia. Esta revisión incluirá la consideración de los resultados de las auditorías, el estado de los riesgos, los incidentes de seguridad, y las oportunidades de mejora. NASERTIC mejorará continuamente la idoneidad, adecuación y eficacia del SGSI.

5.2 Documentación de Seguridad de la Información

Esta política de seguridad de la información se desarrolla en la documentación del sistema de gestión integrado de NASERTIC.

5.3 Responsabilidad de la Dirección

La Dirección es responsable de asignar los medios técnicos y humanos necesarios para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos de información.

Para ello, aprobará las políticas, normativas, medidas técnicas y organizativas que sean requeridos, y se compromete a distribuirlas a todas las personas afectadas.

Adicionalmente, siempre que sea de obligado cumplimiento, se tratará cualquier elemento introducido en los sistemas de información gestionados por NASERTIC, según los requisitos establecidos por la legislación vigente sobre propiedad intelectual.

5.4 Responsabilidades de las personas usuarias

Cada persona usuaria es responsable del equipamiento que NASERTIC le ha confiado para el desarrollo de sus funciones laborales, y de cumplir las políticas, normativas, medidas técnicas y organizativas en materia de seguridad de la información.

Igualmente, la persona usuaria es responsable de proteger y mantener la confidencialidad de la información perteneciente o confiada a NASERTIC, y deberá contribuir de manera activa al secreto de esta. Esta obligación subsistirá incluso después de finalizar los servicios en NASERTIC.

En caso de detectar algún posible incidente de seguridad de la información, la persona usuaria deberá comunicarlo siguiendo el procedimiento establecido.

El incumplimiento de las citadas responsabilidades puede desencadenar un procedimiento disciplinario, además de consecuencias civiles o penales.

5.5 Comité de Seguridad de la información y Protección de Datos.

El comité de seguridad de la información está formado por:

a) Gerente, que ostentará la presidencia del Comité.

b) Responsable de los servicios

c) Responsable de Seguridad

d) Responsable del sistema

e) Responsable del área jurídica

f) Delegado de Protección de Datos

El comité de seguridad de la información y protección de datos es responsable de:

1) Elaborar propuestas de modificación y actualización permanente de la Política de Seguridad de la Información y Protección de Datos (PPDSI) de la organización.
2) Promover recursos y medios para la mejora en materia de protección de datos y seguridad de la información.
3) Buscar la eficiencia al compartir experiencias, trabajos realizados y lecciones aprendidas que pueden ser aprovechadas por otras sociedades públicas adscritas a CPEN. 4) Promover decisiones conjuntas para la búsqueda de la homogeneidad y eficiencia en el uso de recursos.
4) Elaborar, al menos con una periodicidad anual, un informe conjunto del estado de situación, relativo a protección de datos y seguridad de la información de NASERTIC, que sirva de entrada para la revisión por la Dirección.
5) Supervisar la elaboración y mantenimiento de la Declaración de Aplicabilidad (SoA).

6) Proponer y promover acciones de mejora continua del SGSI.
7) Proponer y promover acciones de mejora continua del SGSI.

6 TRATAMIENTO DE LOS DATOS PERSONALES

6.1 Principios de actuación:

NASERTIC tratará la información y los datos personales conforme a los siguientes principios de protección de datos y seguridad de la información:

1) **Licitud, lealtad y transparencia**: los datos personales serán tratados de manera lícita, leal y transparente en relación con la persona interesada.
2) **Legitimación en el tratamiento de datos personales**: solo se tratarán los datos personales cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.
3) **Limitación de la finalidad**: los datos personales serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
4) **Minimización de datos**: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
5) **Exactitud**: los datos personales serán exactos y, si fuera necesario, actualizarlos; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.
6) **Limitación del plazo de conservación**: los datos personales serán mantenidos de forma que se permita la identificación de las personas interesadas durante no más tiempo del necesario para los fines que justificaron su tratamiento.
7) **Integridad y confidencialidad**: los datos personales serán tratados de tal manera que se garantice su seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Quienes intervengan en el tratamiento de los datos estarán sujetos al deber de secreto incluso después de haber concluido la relación que justificaba su intervención.
8) **Responsabilidad proactiva**: NASERTIC será responsable del cumplimiento de los principios anteriormente señalados y adoptarán las medidas técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.
9) **Atención de los derechos de las personas afectadas**: se adoptarán medidas en NASERTIC que garanticen el adecuado ejercicio por las personas afectadas, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos personales.
10) **Alcance estratégico**: la protección de datos y la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de NASERTIC para conformar un todo coherente y eficaz.

11) **Responsabilidad diferenciada**: en los sistemas de información responsabilidad de NASERTIC se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles:
    a. Responsable del tratamiento: la persona que determina los fines y medios del tratamiento.
    b. Encargado del tratamiento: la persona que trata datos personales por cuenta del responsable del tratamiento según sus requerimientos
    c. Delegada o delegado de protección de datos: la persona que informa y asesora al responsable del tratamiento de las obligaciones en materia de cumplimiento del RGPD.
    d. Responsable de la información: la persona que determina los requisitos de seguridad de la información tratada.
    e. Responsable del servicio: la persona que determina los requisitos funcionales y de seguridad de los servicios prestados a partir de la información.
    f. Responsable de seguridad de la información: la persona que determina las decisiones para satisfacer los requisitos de seguridad.
    g. Responsable del sistema: la persona que tiene la responsabilidad sobre los requisitos no funcionales y de diseño, construcción, operación y soporte de los sistemas de información utilizados en la prestación de los servicios.
12) **Seguridad integral**: la seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, debiendo, además, abarcar otras propiedades, como la autenticidad y la trazabilidad. La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural.
13) **Análisis y gestión de riesgos:** el análisis y gestión del riesgo es el conjunto de actividades coordinadas que se desarrollan para identificar los riesgos y el impacto o consecuencias sobre un activo, cuando una amenaza se materializa y puede afectar al tratamiento de los datos o de la información debido a la existencia de una debilidad o vulnerabilidad del sistema, tanto de protección de datos como de gestión de la información. El análisis y gestión de riesgos es parte esencial del proceso de protección de datos y de seguridad de la información, de forma que permita el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad organizativas y técnicas, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo, NASERTIC tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.
14) **Proporcionalidad**: NASERTIC establecerá medidas de protección, detección y recuperación que resulten proporcionales a los potenciales riesgos y a la criticidad y el valor de la información, de los tratamientos de datos personales y de los servicios afectados.

15) **Proceso de verificación**: NASERTIC implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad de los tratamientos.
16) **Protección de datos y seguridad desde el diseño**: NASERTIC promoverá la implantación del principio de protección de datos desde el diseño, con el objetivo de cumplir los requisitos definidos en el RGPD y garantizar los derechos de las personas interesadas, de forma que la protección de datos se encuentre presente desde las primeras fases de concepción de un proyecto. Asimismo, la seguridad de la información se aplicará desde el diseño inicial de los sistemas de información.
17) **Seguridad por defecto**: NASERTIC promoverá que los sistemas de información de su titularidad se diseñen y configuren de forma que garanticen la protección de datos por defecto, en especial en lo que hace referencia a la minimización de los datos y del acceso a la información.
18) **Seguridad ligada a las personas**: se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder, a los activos de información y a los datos personales conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
19) **Seguridad física**: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
20) **Seguridad en la gestión de comunicaciones y operaciones**: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad. El sistema ha de proteger el perímetro, en particular si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.
21) **Autorización y control de acceso**: se limitará el acceso a los activos de información por parte de las personas usuarias, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de NASERTIC. Para corregir, o exigir responsabilidades en su caso, cada persona que acceda a la información del sistema debe estar identificada de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos y quién ha realizado determinada actividad. En caso de existir indicios de actividades delictivas o que comprometan la seguridad de la información tratada por NASERTIC, éstos deberán ser comunicados a la autoridad competente para su persecución.
22) **Adquisición, desarrollo y mantenimiento de los sistemas de información**: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por

defecto, incluyendo al control de cambios (p.e. Ante actualizaciones) para garantizar su integridad.

23) **Gestión de los incidentes de seguridad**: se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en la normativa de protección de datos y seguridad de la información, de los incidentes de seguridad.
24) **Gestión de la continuidad**: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener l continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de NASERTIC.
25) **Cumplimiento**: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información y protección de datos personales.
26) **Profesionalidad**: la seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento. El personal de NASERTIC recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de NASERTIC. NASERTIC exigirá que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
27) **Uso aceptable de los sistemas de información**: en el caso del personal al servicio de NASERTIC, los medios y equipos informáticos a utilizar serán directamente provistos e instalados por las unidades de la propia Organización o por los proveedores de servicios, como parte del acuerdo de prestación que se establezca, con conocimiento y autorización de las unidades técnicas encargadas a tal efecto, siendo el único uso aceptable de los mismos el adecuado desempeño de las funciones propias de su puesto de trabajo y quedando prohibida toda alteración no autorizada de los mismos.
28) **Mejora continua**: NASERTIC se enfoca a la mejora continua del proceso de seguridad a partir de la medición y análisis de la información y del Sistema de Gestión de Seguridad de la Información (SGSI) en su conjunto.
29) **Existencia de líneas de defensa:** El sistema de información dispondrá de una estrategia de protección constituida por múltiples capas de seguridad, de naturaleza organizativa, física y lógica.
30) **Vigilancia continua y reevaluación periódica:** La seguridad se reevaluará y actualizará periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección.
31) **Mínimo Privilegio:** Los sistemas de información se diseñarán y configurarán otorgando los mínimos privilegios necesarios para su correcto desempeño. Las funciones de operación, administración y registro serán las mínimas necesarias y realizadas por personal autorizado.
32) **Registro de actividad y detección de código dañino:** Se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas. Se implementarán mecanismos para la detección de código dañino

6.2 Privacidad desde el diseño

Desde el diseño de todos los tratamientos de datos se tendrá en consideración la privacidad, para ello y con carácter previo, se elaborará un registro de operaciones de tratamiento, conforme lo establecido en el RGPD, se analizará la necesidad de llevar a cabo una evaluación de impacto y en su caso un análisis de riesgos valorando el ciclo de vida del tratamiento, los elementos relevantes, la proporcionalidad y la base de legitimación del tratamiento.

Así mismo se implantará la privacidad por defecto, valorando:

- la minimización de los datos necesarios para el tratamiento,
- que las funciones sean las necesarias para el uso o finalidad de los datos,
- que las funciones solamente puedan ser realizadas por personal autorizado,
- configurado el sistema para que solamente esté disponible y accesible en determinados lugares y momentos,
- que el sistema no esté disponible ni accesible para las funciones que no sean estrictamente necesarias.

7 Proveedores

Cuando NASERTIC utiliza servicios de terceros o ceda información a terceros (principalmente proveedores), se les hace partícipes de esta política y de la documentación relevante en materia de seguridad de la información.

Dicha tercera parte queda sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando proceda, se establecerán procedimientos específicos de reporte y resolución de incidentes.

La tercera parte garantizará que su personal, propio y subcontratado terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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.

Aprobado por:

LUIS CAMPOS ITURRALDE

DIRECTOR GENERAL

72697437A LUIS CAMPOS (R: A31098064)

Firmado digitalmente por 72697437A LUIS CAMPOS (R: A31098064)
Fecha: 2026.05.21 09:53:38 +02'00'