PREÁMBULO

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.

Índice:

PREÁMBULO 1
1.1 Objetivo 3
1.2 Alcance 3
1.3 Principios de protección de datos y seguridad de la información 3
1.4 Privacidad desde el diseño 7
1.5 Responsabilidad de la Dirección 7
1.6 Responsabilidades de las personas usuarias 7
1.7 Comité de seguridad de la información y Protección de Datos 8
1.8 Clientes 8
1.9 Proveedores 9
1.10 Elementos adicionales del Sistema de Gestión 9
1.11 Documentación de Seguridad de la Información 10

1.1 Objetivo

El objetivo de la presente política es establecer las directrices generales que garanticen la seguridad de los sistemas de información de NASERTIC, así como el cumplimiento de las obligaciones derivadas del tratamiento de datos de carácter personal.

1.2 Alcance

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.

1.3 Principios de protección de datos y seguridad de la información

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 a 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

1.4 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.

1.5 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.

1.6 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 la misma. 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.

1.7 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.
5) 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.
6) Supervisar la elaboración y mantenimiento de la Declaración de Aplicabilidad (SoA).
7) Proponer y promover acciones de mejora continua del SGSI.

1.8 Clientes

Cuando NASERTIC presta servicios a otros organismos o maneja información de otros organismos, se les hace partícipes de esta política y se establecen canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecen procedimientos de actuación para la reacción ante incidentes de seguridad.

1.9 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.

1.10 Elementos adicionales 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.

1.11 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.

Aprobado por:

72697437A LUIS CAMPOS (R: A31098064)

Firmado digitalmente por 72697437A LUIS CAMPOS (R: A31098064)
Fecha: 2025.05.26 15:30:15 +02'00'