POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (ENS)

ERITEA SISTEMAS S.L.U.

Las copias controladas de este documento son actualizadas y distribuidas cada vez que se realice una modificación o revisión. Las copias no controladas no son actualizadas.

Este documento es propiedad de ERITEA SISTEMAS S.L.U. Queda prohibida la realización de fotocopias, o la reproducción por cualquier otro medio, total o parcialmente, sin la autorización de ERITEA SISTEMAS S.L.U. o su representante legal.

Índice

1. Introducción

El presente documento tiene por objeto establecer la Política de Seguridad de la Información para ERITEA SISTEMAS S.L.U. en base a los requisitos dispuestos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad; asegurando así la confidencialidad, integridad y disponibilidad de los sistemas de información de la empresa y, por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

ERITEA SISTEMAS S.L.U. es una empresa que presta servicios de consultoría avanzada de sistemas, soporte IT, suministro de infraestructura hardware e instalación, configuración, mantenimiento y puesta en marcha de sistemas informáticos, prestados tanto a empresas privadas como a Administraciones y organismos públicos.

ERITEA SISTEMAS S.L.U. tiene personalidad jurídica propia y plena capacidad de obrar para administrar, adquirir, contratar, asumir obligaciones, así como renunciar y ejercer libremente toda clase de derechos y acciones ante las Administraciones públicas.

ERITEA SISTEMAS S.L.U. establece objetivos de seguridad de la información encaminados a proteger con las mayores garantías, la integridad, la confidencialidad, la disponibilidad, la trazabilidad y la autenticidad de la información objeto de tratamiento dentro de sus competencias.

Para garantizar una apropiada seguridad de la información, ERITEA SISTEMAS S.L.U. aplica las más adecuadas medidas de seguridad en todos los Departamentos, reforzando la prevención, detección y respuesta de incidentes de seguridad.

Los sistemas de información y comunicación de ERITEA SISTEMAS S.L.U. están protegidos contra potenciales amenazas que puedan poner en peligro la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información. A tal fin, la empresa adopta una estrategia de seguridad de la información que permite cumplir con los requisitos establecidos por el Esquema Nacional de Seguridad; aplica un sistema de mejora continua, supervisa y garantiza unos adecuados niveles de servicios; sigue y analiza las vulnerabilidades reportadas y prepara una respuesta efectiva a los incidentes de seguridad con el fin de garantizar la continuidad de los servicios.

Dentro del enfoque de la seguridad de la información como parte integral de los servicios prestados por ERITEA SISTEMAS S.L.U. y de su funcionamiento interno, tiene una especial importancia la protección de datos personales, por lo que muchas de las medidas implantadas están encaminadas a proteger proactivamente dichos datos, velando por el cumplimiento de

lo dispuesto en la legislación vigente en materia de protección de datos personales dentro del marco normativo europeo y español.

2. Alcance

Esta política es aplicable a:

- Todos los activos, sistemas de información y comunicación y actividades de tratamiento de datos de carácter personal de los que ERITEA SISTEMAS S.L.U. sea titular o responsable, tenga encomendada su gestión o sean usados para el ejercicio de las competencias que le son propias en el ámbito de sus actividades profesionales.
- Todos los Departamentos.
- Todo el personal de ERITEA SISTEMAS S.L.U.
- Todo el personal externo que preste servicios a ERITEA SISTEMAS S.L.U.
- Todo el personal externo que pueda acceder a los sistemas de información de ERITEA SISTEMAS S.L.U.

3. Misión

La misión de ERITEA SISTEMAS S.L.U. es ayudar a empresas y organizaciones a desarrollar su actividad comercial dentro de la sociedad, a través de medios tecnológicos que favorezcan, a su vez, el desarrollo de las personas que las conforman.

Los objetivos de servicio de la empresa son los siguientes:

I. Ofrecer servicios de valor a nuestros clientes, abarcando consultorías en Sistema en Virtualización, Consolidación de CPD, Soluciones de alta disponibilidad e hiperconvergencia. Soluciones de almacenamiento enterprise y redundancia, así como almacenamiento de alto rendimiento FLASH.
II. Aportar soluciones a nivel de operador: VPNs, doble factor de autenticación, Firewalls y reglas de enrutamiento, tanto simple como avanzado con protocolos BGP, OSPF, etc.
III. Prestar a nuestros clientes de naturaleza tanto pública como privada, servicios de externalización completa de sus sistemas: help desk, consultoría y asesoramiento, dejando al cliente las labores de coordinación del servicio.

IV. Proporcionar soluciones de ciberseguridad, descubriendo nuevas técnicas y tácticas de ataques informáticos y evasión para proteger rápidamente a nuestros clientes.
V. Acometer proyectos de servicio completos: consultoría, planificación, despliegue, instalación, configuración, migración, puesta en marcha y mantenimiento posventa; suministrando además la infraestructura hardware/software necesaria (puestos de trabajo, servidores, almacenamiento, electrónica de comunicaciones, etc.).
VI. Ofrecer transparencia al cliente en la prestación de cualquier servicio, pudiendo ver en todo momento la trazabilidad de los proyectos en curso, así como las incidencias resueltas, cerradas o en curso con personal interno.

ERITEA SISTEMAS S.L.U. asume los siguientes objetivos en materia de seguridad de la información:

VII. Reforzar la cultura de la organización en materia de seguridad de la información y protección de datos.
VIII. Asegurar que se cumpla la normativa vigente en materia de seguridad y protección de datos a las que la organización deba someterse.
IX. Establecer una estructura organizativa adecuada para la gestión de la seguridad de la información definiendo los roles y los comités necesarios, además de las funciones y las respectivas responsabilidades.
X. Situar a ERITEA SISTEMAS S.L.U. en el cuadrante de las entidades más avanzadas en materia de seguridad de la información en el ámbito de los servicios prestados a las Administraciones Públicas.
XI. Garantizar la disponibilidad de los servicios y la eficacia de las medidas de seguridad implantadas por medio de evaluaciones y auditorías.

4. Marco legal y regulatorio aplicable

Se evitará cualquier tipo de incumplimiento de las leyes u obligaciones legales, reglamentarias o contractuales y de los requisitos de seguridad que afecten a los sistemas de información de ERITEA SISTEMAS S.L.U.

La legislación aplicable a ERITEA SISTEMAS S.L.U. en el marco de la seguridad de la información es la siguiente:

A nivel europeo:

- **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).
- **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 de la Unión.

A nivel estatal:

- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **Ley Orgánica 3/2018**, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **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, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- **Real Decreto Legislativo 1/1996**, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- **Real Decreto-ley 14/2019** de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- **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

- **Real Decreto 1150/2021**, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021.
- **Real Decreto-ley 12/2018,** de 7 de septiembre, de seguridad de las redes y sistemas de información.
- **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.
- **Real Decreto 43/2021**, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.
- **Guías CCN-STIC** (800), **Abstracts** e **Instrucciones Técnicas de Seguridad**

5 Organización de la Seguridad

5.1 Comité de Seguridad

El Comité de Seguridad coordina la seguridad de la información en la organización y establece la estrategia. Está compuesto por el responsable de la Información y del Servicio, el Responsable de Seguridad y el Responsable del Sistema.

El Comité de Seguridad de la Información cuenta con los siguientes perfiles:

Perfiles a nivel de Gobierno:

- Responsable de la Dirección
- Responsable de Tratamiento de Datos
- Responsable de la Información
- Responsable del Servicio

Perfiles a nivel de Supervisión:

- Responsable de Seguridad

Perfiles a nivel Operativo:

- Responsable de Sistema.

El Comité tiene las siguientes funciones:

a) Promover la seguridad de los activos y servicios de ERITEA SISTEMAS S.L.U.
b) Diseñar la estructura de la documentación de seguridad.
c) Valorar y proponer la aprobación de toda la documentación de seguridad.
d) Vigilar el cumplimiento de las obligaciones del responsable del tratamiento, conforme las regula la normativa de protección de datos de carácter personal.
e) Difundir entre el personal al que se refiere el apartado 2 del presente documento, el conocimiento de las obligaciones que le atañen y las consecuencias en que pudiera incurrir en caso de incumplimiento.
f) Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
g) Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
h) Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección
i) Aprobar la Normativa de Seguridad de la información.
j) Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
k) Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
l) 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 tales incidentes.
m) Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
n) Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
o) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
p) 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.

5.2 Responsable de la Información y del Servicio

El responsable de la Información/Servicio es una persona situada en el nivel Directivo de la organización. Este cargo tiene la responsabilidad última del uso que se haga de cierta información o prestación de servicio y, por tanto, de su protección. El responsable de la Información/Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

El responsable de la Información/Servicio será designado por la dirección de ERITEA SISTEMAS S.L.U. y tiene como responsabilidad la ejecución de todas las medidas de seguridad adecuadas para ERITEA SISTEMAS S.L.U., incluida la elaboración de la documentación de seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección anuncie la sustitución de la persona que ocupa el cargo.

El responsable de la Información/Servicio dispone de la potestad de establecer los requisitos de la información o del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información o de los servicios.

La aprobación formal de los niveles corresponde al responsable de la Información/Servicio, que recibirá la propuesta del Responsable de la Seguridad y del Responsable del Sistema, dentro de la estructura creada en el comité correspondiente.

La Dirección de ERITEA SISTEMAS S.L.U. garantizará que el Responsable de la Información/Servicio participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

La Dirección de ERITEA SISTEMAS S.L.U. respaldará al Responsable de la Información/Servicio en el desempeño de las funciones mencionadas en el artículo 39 del RGPD, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

La Dirección de ERITEA SISTEMAS S.L.U. garantizará que el responsable de la Información/Servicio no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. El responsable de la Información/Servicio rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Las personas interesadas podrán ponerse en contacto con el responsable de la Información/Servicio por lo que respecta a todas las cuestiones relativas a la seguridad de la información y a la protección de datos personales.

El responsable de la Información/Servicio estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

El responsable de la Información/Servicio podrá desempeñar otras funciones y cometidos. La Dirección garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja (a veces se dice que 'se heredan los requisitos'), y suele añadir requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

El responsable de la Información/Servicio tendrá como mínimo las siguientes funciones:

a) Informar y asesorar a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del ENS y de otras disposiciones aplicables en materia de seguridad de la información y de protección de datos, vigentes en España o en la Unión o de los Estados miembros.
b) Supervisar el cumplimiento del Marco Regulador de la Privacidad y Seguridad de la Información, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
c) Proporcionar los recursos y medios adecuados para el cumplimiento de los principios básicos, requisitos mínimos y Marco regulador en materia de Privacidad y Seguridad de la Información.

d) Evaluar los niveles de seguridad de la Información tratada y de los servicios prestados.
e) Asumir las funciones explícitamente atribuidas a la figura del Responsable de la Información/Servicio en el ENS.
f) Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la seguridad de la información y supervisar su aplicación de conformidad con lo dispuesto en el ENS.
g) Informar al Responsable de Seguridad de la Información sobre el cumplimiento de los niveles de seguridad y resto de requerimientos que se definan.
h) Cooperar con las autoridades de control y los CERT (Computer Emergency Reaction Team).

El detalle de las funciones del responsable se encuentra en el documento "Fichas de Puestos".

El Responsable de la Información/Servicio desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

5.3 Responsable de Seguridad

El Responsable de Seguridad será designado por la dirección de ERITEA SISTEMAS S.L.U. y tiene como responsabilidad la determinación de las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Este cargo se irá renovando automáticamente hasta que la Dirección anuncie la sustitución de la persona que ocupa el cargo.

Con independencia de la obligación genérica referida a la implantación, coordinación y control de las medidas de seguridad, se enumeran a continuación, a título enunciativo, las funciones mínimas concretas del Responsable de Seguridad:

a) Colaborar, cooperar y asistir al Responsable de la Información/Servicios en el desarrollo de sus funciones con la asistencia técnica del órgano competente de los sistemas de información que soporten los servicios.
b) Desarrollar, operar y mantener el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, apoyado por todos los responsables.

c) Proponer el desarrollo de documentos técnicos del Marco Regulador y elevarlos a la persona titular competente para su aprobación. Proponer los planes de Privacidad y Seguridad de la Información, auditorías, continuidad de los servicios, formación y concienciación y observar su ejecución, así como su seguimiento.
d) Establecer y comprobar todos los procedimientos y estándares necesarios para la correcta aplicación de la normativa de seguridad.
e) Adoptar, con la mayor inmediatez, las medidas oportunas para subsanar cualquier anomalía que haya producido una incidencia e importar al Comité los impresos en que se hayan registrado las incidencias.
f) Cuando las incidencias hayan afectado a datos personales, el Responsable de Seguridad deberá comunicar inmediatamente la incidencia a la AEPD.
g) A intervalos planificados, recibir y revisar información sobre el desempeño y cumplimiento del sistema de gestión de la Seguridad de la Información.
h) Asumir las funciones explícitamente atribuidas a la figura del Responsable Seguridad de la Información en el ENS.

Adicionalmente, el Responsable de Seguridad será el Secretario del Comité de Seguridad de la Información, y como tal:

i) Convocará las reuniones del Comité de Seguridad de la Información.
j) Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
k) Elaborará el acta de las reuniones.
l) Convocará otros perfiles consultivos a las reuniones del comité sí fuera necesario.
m) Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El detalle de las funciones del responsable se encuentra en el documento "Fichas de Puestos".

5.4 Responsable de Sistema.

El Responsable del Sistema será designado por la dirección de ERITEA SISTEMAS S.L.U. La persona designada figurará en la documentación de seguridad del sistema de información.

El Responsable del Sistema tendrá como mínimo las siguientes funciones:

a) Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Definir la tipología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
c) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del 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 el Responsable de la Seguridad, antes de ser ejecutada.

El detalle de las funciones del responsable se encuentra en el documento "Fichas de Puestos".

5.5 Usuarios

El personal técnico y adminsitrativo accede a las aplicaciones con el perfil suficiente para desempeñar sus funciones profesionales, debido a la función asignada o del puesto de trabajo que desempeña y de la unidad administrativa en la que se encuadra.

El detalle de las funciones de los técnicos se encuentra en el documento "Fichas de Puestos".

5.6 Procedimiento de designación y renovación de perfiles

Es función de la Dirección de la organización, en este caso del CEO de ERITEA SISTEMAS S.L.U., designar los siguientes perfiles que se integrarán en la estructura definida para la seguridad de la información en la organización:

- ✓ Al **Responsable de la Información/Servicio.** Este cargo se irá renovando automáticamente hasta que la Dirección anuncie la sustitución de la persona que ocupa el cargo.
- ✓ Al **Responsable de Seguridad**, que debe reportar directamente a la Dirección y al Comité de Seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección anuncie la sustitución de la persona que ocupa el cargo.
- ✓ Al **responsable de Sistema**, que, en materia de seguridad, reportará al Responsable de la Seguridad. Este cargo se irá renovando automáticamente hasta que la Dirección anuncie la sustitución de la persona que ocupa el cargo.

El Comité de Seguridad analizará los candidatos propuestos para los diferentes perfiles y realizará una propuesta final a la dirección para que esta lleve a cabo los nombramientos.

5.7 Nombramientos

El CEO de ERITEA SISTEMAS S.L.U. ejercerá como **Responsable de la Información y de los Servicios**. Adicionalmente, ejercerá como Responsable de Tratamiento en representación de su organización.

El **Delegado de Protección de Datos** será nombrado por la persona titular de la empresa, con competencias en administración electrónica a fin de dar cumplimiento a lo requerido en el artículo 37 del RGPD, que llevará a cabo las tareas establecidas en el artículo 39 del citado RGPD, así como las que se deriven de la normativa española de protección de datos de carácter personal y de los documentos de buenas prácticas que se adopten por la propia organización.

Actualmente ERITEA SISTEMAS S.L.U no dispone de un DPD por no ser, en el caso de esta organización, obligatorio su nombramiento. Si que dispone de los servicios de una consultora externa especialista en Protección de Datos y Privacidad.

La consultora de Seguridad de la Información de ERITEA SISTEMAS S.L.U. ejercerá como **Responsable de Seguridad de la Información**.

El Responsable de Proyectos será el **Responsable del Sistema de Información**, seleccionado entre el personal técnico, con los conocimientos adecuados.

El **Comité de Seguridad** de la Información analizará los candidatos propuestos para los diferentes perfiles y realizará una propuesta final a la dirección para que esta lleve a cabo los nombramientos.

5.8 Compatibilidades

De acuerdo con los requerimientos señalados en los diferentes artículos del Esquema Nacional de Seguridad y al contenido de las guías CCN-STIC (Guía 801 Funciones y Responsabilidades) que lo desarrollan se pueden señalar, recogidas textualmente, las siguientes puntualizaciones respecto a los perfiles señalados en las páginas anteriores:

- Las figuras de **Responsable de la Información y Responsable del Servicio** pueden recaer en la misma persona, Comité u órgano colegiado, como ocurre en el caso de ERITEA SISTEMAS S.L.U., dependiendo de la naturaleza o tamaño de la organización.
- El **Responsable de Seguridad** es la persona designada por la Dirección de la organización, según el procedimiento descrito en su Política de Seguridad de la Información. De conformidad con el principio de "segregación de funciones y tareas" recogido en el art. 10 del ENS, **el Responsable de la Seguridad será una figura diferenciada del Responsable del Sistema, del responsable de la Información y del Responsable del Servicio**.
- El perfil de **Responsable del Sistema**, dado que es el encargado de llevar a la práctica, implementar y controlar las medidas de seguridad no es compatible con ningún otro perfil.

6 Estructuración de la documentación de seguridad

6.1 Clasificación de la documentación

La documentación de seguridad se clasifica en cuanto a su contenido del siguiente modo:

a) **Política de seguridad**: El presente documento, que establece las directrices generales de la seguridad en ERITEA SISTEMAS S.L.U. al más alto nivel.

b) **Normativa de seguridad**: Los documentos que establecen la obligatoriedad de la documentación de seguridad.
c) **Políticas particulares y planes específicos**: Documentación que establece directrices de actuación en áreas determinadas.
d) **Procedimientos**: Documentos que establecen maneras concretas de actuación.
e) **Registros**: Documentos que reflejan los resultados de los procedimientos.
f) **Inventarios**: Relación de ítems en un momento determinado.
g) **Otra documentación**: Cualquier otra documentación relevante a la seguridad de la información procesada por ERITEA SISTEMAS S.L.U.

6.2 Procedimiento para la clasificación

La clasificación la realiza el Responsable de Seguridad, bajo la supervisión del Comité de Seguridad de ERITEA SISTEMAS S.L.U.

6.3 Generación y aprobación de la documentación

La documentación la genera el Responsable de Seguridad, o personal bajo su dirección, la propuesta la realiza el Comité de Seguridad y la aprueba la dirección de ERITEA SISTEMAS S.L.U.

6.4 Acceso a la documentación

El acceso a esta documentación se autoriza por el Responsable de Seguridad, previa deliberación en el Comité de Seguridad. A cada usuario sólo se le conceden los privilegios mínimos para cumplir con estas obligaciones.

La difusión de determinada documentación está regulada en los correspondientes procedimientos de difusión.

6.5 Revisión de la documentación de seguridad

La revisión de la documentación de seguridad se realiza conforme a los procedimientos que se establezcan.

7 Principios Básicos y Requisitos Mínimos de Privacidad y Seguridad de la Información

7.1 Principios básicos

ERITEA SISTEMAS S.L.U. tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios de protección de datos y seguridad de la información:

a) **Licitud, lealtad y transparencia**: Los datos de carácter personal serán tratados de manera lícita, leal y transparente en relación con el interesado.
b) **Legitimación en el tratamiento de datos personales**: Solo se tratarán los datos de carácter personal cuando dicho tratamiento se encuentre amparado en alguna de las causas de legitimación establecidas en los artículos 6 y 9 del RGPD.
c) **Limitación de la finalidad**: Los datos de carácter personal serán tratados para el cumplimiento de fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.
d) **Minimización de datos**: Los datos de carácter personal serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
e) **Exactitud**: Los datos de carácter personal serán exactos y, si fuera necesario, actualizados; 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.
f) **Limitación del plazo de conservación**: Los datos de carácter personal serán mantenidos de forma que se permita la identificación de los interesaos durante no más tiempo del necesario para los fines que justificaron su tratamiento.
g) **Integridad y confidencialidad**: Los datos de carácter personal 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 aquel.
h) **Responsabilidad proactiva**: ERITEA SISTEMAS S.L.U. será responsable del cumplimiento de los principios anteriormente señalados y adoptará las medidas

técnicas y organizativas que le permitan estar en condiciones de demostrar dicho cumplimiento.

i) **Atención de los derechos de los afectados**: Se adoptarán medidas en la organización que garanticen el adecuado ejercicio por los afectados, cuando proceda, de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad respecto de sus datos de carácter personal.

j) **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 iniciativas estratégicas de ERITEA SISTEMAS S.L.U. para conformar un todo coherente y eficaz.

k) **Seguridad integral**: La seguridad tenderá a la preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. 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.

l) **Gestión de riesgos**: La gestión del riesgo es el conjunto de actividades coordinadas que ERITEA SISTEMAS S.L.U. desarrolla para dirigir y controlar el riesgo, entendiendo como riesgo el efecto de la incertidumbre sobre la consecución de los objetivos. El análisis y gestión de riesgos son parte esencial del proceso de protección de datos y de seguridad de la información de ERITEA SISTEMAS S.L.U., de forma que perita 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, 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 la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo ERITEA SISTEMAS S.L.U. tendrá en cuenta los riesgos que se derivan para los derechos de las personas con respecto al tratamiento de sus datos personales.

m) **Proceso de verificación**: ERITEA SISTEMAS S.L.U. implantará un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la privacidad y seguridad de la información.

n) **Protección de datos y seguridad desde el diseño**: ERITEA SISTEMAS S.L.U. promoverá la implantación del principio de protección de datos desde el diseño con el objetivo de cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados de forma que la protección de datos se encuentre

presente en 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.

o) **Prevención, reacción y recuperación**: La privacidad y seguridad de la información debe contemplar los aspectos de prevención, reacción y recuperación sobre los activos, para conseguir que las amenazas sobre los mismos no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.

p) **Líneas de defensa**: Los sistemas de información han de disponer de una estrategia de protección constituida por múltiples capas de seguridad.

q) **Reevaluación periódica**: La gestión de la Privacidad y Seguridad de la Información se revisarán, evaluará y actualizará periódicamente para mantener su eficacia de forma continuada, con la finalidad de hacer frente a la constante evolución de los riesgos y las medidas de seguridad.

r) **Responsabilidad diferenciada**: En los sistemas de información responsabilidad de ERITEA SISTEMAS S.L.U. se observará el principio de responsabilidad diferenciada de forma que se delimiten las diferentes responsabilidades y roles.

7.2 Requisitos mínimos

ERITEA SISTEMAS S.L.U. establece los siguientes requisitos mínimos, que han de regir su Marco Regulador:

a) **Organización e implantación del proceso de seguridad:** La seguridad compromete a todo el personal dentro del alcance definido en este documento.

b) **Análisis y gestión de los riesgos**: ERITEA SISTEMAS S.L.U. debe analizar y tratar sus riesgos empleando metodologías reconocidas. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos, en especial cuando se traten datos de carácter personal.

c) **Evaluación de impacto en la privacidad**: Cuando se traten datos de carácter personal que, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas, debe realizarse, antes del tratamiento, una evaluación del impacto en la privacidad.

d) **Gestión de Personal**: El personal de las entidades incluidas en el alcance serán informados de sus deberes y obligaciones en materia de seguridad.

e) **Profesionalidad**: El personal de las entidades incluidas en el alcance que desarrollen funciones en el ámbito de la Privacidad y Seguridad de la Información dispondrán de la capacitación adecuada para la ejecución de las tareas encomendadas.

f) **Autorización y control de los accesos**: El acceso a los sistemas de información estarán controlados y limitados. Cada usuario, proceso, dispositivo y otros sistemas de información que accedan a la información de los sistemas de ERITEA SISTEMAS S.L.U. debe estar identificado 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.

g) **Protección de las instalaciones**: Las instalaciones de ERITEA SISTEMAS S.L.U. contarán con medidas de seguridad física adecuadas a la información que tratan en su interior.

h) **Adquisición de productos**: Antes de la adquisición de cualquier producto de seguridad de la información aplicable al alcance incluido dentro del ENS, se seguirán las pautas descritas en la Guía del CCN 105 Versión febrero 2021. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

i) **Seguridad por defecto**: Los sistemas de información deben diseñarse y configurarse de forma que proporcionen las mínimas funcionalidades requeridas, incluidas aquellas relacionadas con la operación, administración y registro de actividad, asegurando su disponibilidad y de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

j) **Integridad y actualización del sistema**: Cualquier elemento físico o lógico requiere la autorización del Responsable de Seguridad de la Información para poder proceder a su instalación en los sistemas de información de ERITEA SISTEMAS S.L.U. Se mantendrá actualizado el estado de seguridad de los sistemas de información, en relación con las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que les afecten, de forma que dicho estado sirva como entrada a las actividades de gestión de riesgos.

k) **Protección de la información almacenada y en tránsito**: Se prestará especial atención a la información, en cualquier soporte, almacenada o en tránsito a través de entornos inseguros. Aplicándose las medidas de seguridad que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de estos.

l) **Prevención ante otros sistemas de información interconectados**: Se protegerán adecuadamente tanto las comunicaciones entre los sistemas de información y otros sistemas externos y en particular los puntos de interconexión entre las redes que soporten dichas comunicaciones, especialmente aquellas que se realicen a través de redes públicas.

m) **Registro de actividad**: Con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona, entidad o proceso que actúa.

n) **Incidentes de seguridad**: Se implantarán los mecanismos apropiados para la correcta identificación, registro, resolución y notificación, en los términos previstos en el RGPD y el ENS, de los incidentes de seguridad.

o) **Continuidad de la actividad**: Se desarrollarán planes de continuidad de negocio y actividades de recuperación para garantizar la disponibilidad de los servicios.

p) **Mejora continua del proceso de seguridad**: La gestión de Privacidad y Seguridad de la Información estará sometida a un ciclo de mejora continua como resultado de la aplicación del principio de reevaluación periódica.

8 Relación con terceras partes

Cuando un tercero preste servicios a ERITEA SISTEMAS S.L.U. en el que deba acceder a datos personales de los que ERITEA SISTEMAS S.L.U. es Responsable del Tratamiento, o se cedan activos de información a éstos, se le debe hacer partícipe del Marco Regulador de Privacidad y Seguridad de la Información que ataña a dichos servicios o activos.

Las terceras partes quedan sujetas a las obligaciones establecidas en dicho Marco.

Los contratos, encargos o convenios que se suscriban a partir de la entrada en vigor de este acuerdo deben incluir la obligación de cumplir esta Política.

Las subcontrataciones requerirán el consentimiento expreso del Responsable de la Información/Servicio para el acceso a los activos de la información.

Cualquier tercero adjudicatario de un contrato, encargo o convenio que conlleve el tratamiento de datos de carácter personal en nombre de ERITEA SISTEMAS S.L.U. deberá ser constituido como Encargado de Tratamiento y firmar el correspondiente contrato como anexo a los contratos suscritos para la prestación de los servicios contratados, además de los correspondientes acuerdos de confidencialidad con la empresa proveedora y con los trabajadores externos que vayan a acceder a la información de ERITEA SISTEMAS S.L.U.

Cuando ERITEA SISTEMAS S.L.U. preste servicios a otras organizaciones o maneje información de otras organizaciones, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de las respectivas unidades de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando ERITEA SISTEMAS S.L.U. utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Si un tercero no puede cumplir algún aspecto de la Política de Seguridad de la Información según lo que se requiere en los párrafos anteriores, será preciso obtener un informe del responsable de seguridad competente que precise los riesgos en que se incurre y la manera de tratarlos. Con anterioridad a su continuación, también será necesario que los responsables de la información y los responsables de los servicios afectados aprueben dicho informe antes de seguir adelante.

9 Resolución de conflictos

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa definida para la gestión de la seguridad de la información, lo resolverá su superior jerárquico; en su ausencia, prevalece la decisión del Comité de Seguridad de la Información.

En caso de conflicto entre los responsables que componen la estructura organizativa para la gestión de la seguridad de la información y los definidos en la normativa de

protección de datos de carácter personal, prevalece la decisión que implique el nivel más alto de protección.

10 Obligaciones del personal

Todos los miembros de ERITEA SISTEMAS S.L.U. tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, siendo responsabilidad del Comité de Seguridad de la Información de la empresa disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la empresa atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Para ello, ERITEA SISTEMAS S.L.U. garantizará la definición y la ejecución de las acciones necesarias para concienciar y fomentar el cumplimiento de las obligaciones por parte del personal con relación a los riesgos y las amenazas relativos a la seguridad de la información.

La gestión y preservación de la seguridad de la información y el cumplimiento de los objetivos citados en esta Política deben ser el fin común de todas las personas que presten servicio directa o indirectamente en la organización, de tal manera que son responsables del uso correcto de los activos de tecnologías de la información y de las comunicaciones puestos a su disposición.

El incumplimiento de esta política de seguridad de la información podrá suponer el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales que correspondan.

Los usuarios de ERITEA SISTEMAS S.L.U. serán responsables de aquella información que manejen y/o a la que accedan, en función de los permisos que les sean asignados dentro de la organización, en el desarrollo de sus actividades profesionales. Dicha información tendrá asignados los niveles de seguridad requeridos.

11 Revisión de la política

El Responsable de Seguridad asegurará la revisión de la Política de Seguridad de la Información cuando se produzcan cambios significativos en el contexto y/o la organización de ERITEA SISTEMAS S.L.U., la cual se elevará, para su revisión y aprobación, al Comité de Seguridad de la Información.

Su revisión debe garantizar que ésta se encuentra alineada con la estrategia, la misión y visión del organismo en materia de Privacidad y Seguridad de la Información.

En último término, la Política de Seguridad de la Información, y sus revisiones, será aprobada formalmente por la Dirección de la Organización y tendrá carácter imperativo sobre toda la organización.

12 Aprobación y entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde el día siguiente de su aprobación y hasta que no sea reemplazada por otra versión posterior.