POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

ENS

USO PÚBLICO

INDICE

16 de mayo de 2023

Aprobado por:

Comité de Seguridad

Firmado:

Raúl García	Antonio Narváez
Resp. Seguridad	Dir. Técnico

1. OBJETO Y CAMPO DE APLICACIÓN

Este documento describe la política de seguridad de la información seguida por Serval Networks para dar cumplimiento a los requisitos establecidos en el Esquema Nacional de Seguridad.

Se aplica a todos los sistemas de Serval Networks para las siguientes actividades desarrolladas: Comercialización, diseño, desarrollo, planificación, integración, instalación, mantenimiento y soporte de sistemas integrales de telecomunicaciones, IT, y seguridad.

2. REFERENCIAS

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

3.1. MISIÓN DE LA ORGANIZACIÓN.

Somos una compañía especialista dentro del sector de la Ciberseguridad y el Networking enfocada en el segmento de las Grandes Cuentas, cuyas señas de identidad se definen a través de la innovación continua, la pasión por la Ciberseguridad, y la unidad de toda la compañía como una gran familia independientemente del rol de cada uno.

Somos muy apreciados por nuestros clientes, pero también por los fabricantes y mayoristas con los que trabajamos, pues procuramos prestar nuestros servicios siempre dentro de unos niveles de excelencia que cumplan con las expectativas de todos ellos.

Esto nos permite estar siempre a la vanguardia tecnológica, especializando a los técnicos en las mejores soluciones del mundo, impulsando su crecimiento personal, y ayudándoles a permanecer también dentro de la excelencia profesional con el paso de los años.

Por este motivo, en Serval Networks establecemos objetivos encaminados a mejorar la confidencialidad, integridad, disponibilidad, autenticidad, y trazabilidad de la información que tratamos, evaluando los riesgos a los que se encuentra sometida la información, y estableciendo planes de tratamiento de riesgos para su mejora.

Esta política de seguridad de la información se ha desarrollado hasta completar un sistema de gestión que cumple con los requisitos establecidos en la norma UNE-EN ISO/IEC 27001 y con el Esquema Nacional de Seguridad, y que incluye los siguientes apartados:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Continuidad de la actividad.

o) Mejora continua del proceso de seguridad.

3.2. EL MARCO REGULATORIO EN EL QUE SE DESARROLLAMOS NUESTRAS LAS ACTIVIDADES.

Serval Networks desarrolla su actividad en un marco regulatorio marcado por el cumplimiento de los requisitos establecidos en materia de protección de datos, telecomunicaciones, y propiedad intelectual.

En el desarrollo de nuestras actividades, estamos comprometidos con el cumplimiento de los requisitos legales establecidos en:

- 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD)
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 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.
- 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.
- DIRECTIVA 2014/26/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 26 de febrero de 2014 relativa a la gestión colectiva de los derechos de autor y derechos afines y a la concesión de licencias multiterritoriales de derechos sobre obras musicales para su utilización en línea en mercado interior
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

3.3. LOS ROLES O FUNCIONES DE SEGURIDAD, DEFINIENDO PARA CADA UNO, SUS DEBERES Y RESPONSABILIDADES, ASÍ COMO EL PROCEDIMIENTO PARA SU DESIGNACIÓN Y RENOVACIÓN.

La información comercial y el saber hacer de las personas son factores decisivos para la competitividad de Serval Networks, y constituyen activos esenciales para el crecimiento y desarrollo de nuestra organización.

Por este motivo, se han establecido los siguientes roles de seguridad:

- **Responsable de la información**. Esta figura recae en el Comité de Seguridad de la Información. Es el órgano encargado de determinar los requisitos de seguridad de la información tratada, aprobando los niveles de seguridad de la información. Entre sus funciones se incluye la aprobación de esta política de seguridad.
- **Responsable de cada servicio**. Al frente de cada servicio ofrecido por Serval Networks, se ha designado un director, que es el responsable del servicio, determinando los requisitos de seguridad del servicio, las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

  Valora las consecuencias de un impacto negativo sobre la seguridad de los servicios. Esta valoración se efectúa atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.
- **Responsable de seguridad**. Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Se trata de una persona jerárquicamente independiente del responsable del sistema.

  Participa en la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones seleccionando, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a su juicio.

  Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

  Es el responsable de aprobar la declaración de aplicabilidad que incluya las medidas del Anexo II del Esquema Nacional de Seguridad.

  Es el responsable de analizar y determinar las medidas compensatorias de forma justificada mediante su aprobación formal.

  Analizar y supervisar los supuestos concretos de utilización de las infraestructuras y servicios comunes de la organización.

  Analizar los informes de auditoría, y encargarse de que se adopten las medidas correctivas adecuadas.
- **Responsable de cada sistema de información**. Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
- **Responsable de sistemas de gestión**. Se encarga de la coordinación de las actividades necesarias para el mantenimiento del sistema de gestión de seguridad de la información. Garantiza que el sistema de gestión cumple con los requisitos establecidos en el Esquema Nacional de Seguridad, y que la documentación no entra en conflicto con otros sistemas de gestión de la organización.
- **Responsable de protección de datos.** Es la persona encargada de determinar los fines y los medios del tratamiento de la información que contenga datos de carácter personal, y se asegura de que se cumplen los requisitos establecidos en el reglamento general de protección de datos y la ley orgánica de protección de datos y garantía de los derechos digitales.

Estos roles son desempeñados por los miembros de la organización designados por el Comité de Seguridad sin una duración determinada hasta que decida su renovación.

En el caso de que durante la realización de alguna actividad se requiriese su coordinación o mediación en la resolución de un conflicto, éste será elevado al Comité de Seguridad para su resolución.

Para los demás puestos de trabajo se han establecido sus funciones y responsabilidades en sus perfiles de puesto de trabajo.

3.4. LA ESTRUCTURA Y COMPOSICIÓN DEL COMITÉ PARA LA GESTIÓN Y COORDINACIÓN DE LA SEGURIDAD.

El Comité de Seguridad de la Información se encuentra compuesto por:

- Director General.
- Responsable de Seguridad.

El Comité de Seguridad realiza las funciones de responsable de la información, coordinación de las actividades desarrolladas por los cargos nombrados para garantizar la seguridad y actúa como máximo órgano de decisión con los otros miembros de la organización.

3.5. LAS DIRECTRICES PARA LA ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO.

La documentación del sistema de gestión está estructurada de forma piramidal, en cuya parte superior se encuentra esta política.

Un Manual, que describe cómo se da cumplimiento a los diferentes puntos del Esquema Nacional de Seguridad y que referencia a los documentos que desarrollan cada apartado.

Instrucciones Técnicas de Seguridad, que describen las políticas de seguridad aplicadas a los sistemas de la organización.

Por último los registros que sirven como evidencia para demostrar el cumplimiento de los requisitos establecidos en el Esquema Nacional de Seguridad.

Los documentos se encuentran compartidos con los miembros pertinentes de la organización a través de las carpetas de red a las que pueden acceder en modo solo lectura y que administra el responsable de sistemas de gestión.

3.6. LOS RIESGOS QUE SE DERIVAN DEL TRATAMIENTO DE LOS DATOS PERSONALES.

Durante el desarrollo de su actividad, Serval Networks accede a información personal que es tratada conforme a los requisitos legales establecidos tanto en el reglamento general de protección de datos, como en la ley orgánica de protección de datos y garantía de derechos digitales.

En aquellos casos en los que se cuenta con un encargado de tratamiento, se establecen los acuerdos y condiciones que rigen la forma en la que deben ser tratados acorde a los riesgos detectados por el responsable de protección de protección, que evalúa el tratamiento que debe aplicarse en cada caso, y al que puede acceder para ejercer los derechos contemplados en la legislación a través de la dirección de correo electrónico rrhh@servalnetwoks.com

4. CONTROL DE EDICIONES

EDICION	MOTIVO DEL CAMBIO	FECHA
1	Primera elaboración de la política	16/05/2023