POLÍTICA:
SEGURIDAD DE LA INFORMACIÓN
(VERSIÓN 05)

1. OBJETIVO

Sharf considera a la información como un activo valioso para el cumplimiento de sus funciones, alcance de su propuesta de valor ("Crear conexiones de alto valor a través de la cadena logística") y de sus objetivos. Por ello, se compromete a gestionar la seguridad de la información, la ciberseguridad y la protección de datos personales a través de medidas que aseguren su confidencialidad, integridad y disponibilidad, que permitan:

- Cumplir los requisitos legales, regulatorios, contractuales y organizacionales aplicables en materia de seguridad de la información, ciberseguridad y protección de datos personales.
- Proteger la confidencialidad, integridad y disponibilidad de la información y de los activos que la soportan.
- Gestionar y controlar los riesgos e incidentes de seguridad de la información y ciberseguridad.
- Proteger la información y la plataforma tecnológica que la soporta, como parte de una estrategia orientada a la continuidad del negocio.
- Fortalecer continuamente las capacidades de ciberseguridad para prevenir, detectar, responder y recuperarse frente a amenazas digitales que puedan afectar los activos de información, servicios tecnológicos y operaciones de la organización.
- Promover una cultura organizacional basada en la seguridad, privacidad, gestión responsable de la información y resiliencia digital, fomentando la participación activa de todos los colaboradores y partes interesadas.
- Mejorar continuamente la eficacia del SGSI.
- Garantizar la aplicación responsable de sistemas de automatización e inteligencia artificial, asegurando siempre la transparencia, explicabilidad, supervisión humana y la no discriminación en los procesos donde se utilicen.

2. ALCANCE

Esta política aplica a colaboradores, practicantes, clientes, proveedores, contratistas, consultores, terceros y cualquier otra parte interesada que tenga acceso, procese, almacene, transmita o gestione información o activos de información de Sharf.

3. DIRECTRICES

- Toda información clasificada como Confidencial, Restringida o que contenga datos personales deberá protegerse mediante controles de seguridad apropiados de acuerdo con su nivel de criticidad y clasificación.
- Todos los colaboradores, proveedores y terceros son responsables de proteger la información a la que acceden y cumplir las políticas, procedimientos y controles establecidos por la organización.
- Sharf contará con capacidades y procedimientos para la gestión de incidentes de seguridad de la información y ciberseguridad, asegurando su detección, análisis,

respuesta, recuperación y mejora continua, con el fin de minimizar su impacto sobre las operaciones y los activos de información.

- Sharf promoverá permanentemente la concientización y capacitación en seguridad de la información, ciberseguridad, privacidad y protección de datos personales.
- Sharf gestionará de forma continua los riesgos de seguridad de la información y ciberseguridad mediante una metodología corporativa aprobada y mantendrá capacidades de detección, respuesta, recuperación y mejora continua frente a incidentes de seguridad.
- La Política de Seguridad de la Información se soporta en una serie de políticas específicas o directivas que proporcionan lineamientos sobre tópicos específicos, las cuales buscan complementar la presente política.
- Los proveedores, contratistas y terceros que accedan, almacenen, procesen o transmitan información de Sharf deberán cumplir los requisitos de seguridad de la información establecidos por la organización.
- Sharf realizará evaluaciones periódicas de seguridad sobre sus procesos, aplicaciones, infraestructura tecnológica y servicios críticos mediante auditorías, análisis de vulnerabilidades, pruebas de seguridad y otras actividades orientadas a verificar la eficacia de los controles implementados.
- El uso de sistemas automatizados e inteligencia artificial deberá realizarse bajo principios de seguridad, transparencia, supervisión humana, trazabilidad, explicabilidad y protección de la información.
- Asimismo, queda prohibido ingresar información confidencial, datos personales o información crítica en herramientas de inteligencia artificial no autorizadas por la organización.
- La presente Política de Seguridad de la Información será revisada al menos una vez al año o cuando se produzcan cambios significativos en el entorno legal, regulatorio, tecnológico, organizacional o de riesgos que puedan afectar al Sistema de Gestión de Seguridad de la Información.

4. DOCUMENTOS DE REFERENCIA

- ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información
- Decreto de Urgencia N° 007-2020 – Marco de Confianza Digital.
- Ley N° 31814 – Ley que promueve el uso responsable de la Inteligencia Artificial.
- Ley N° 29733 - Ley de Protección de Datos Personales - Perú

5. RESPONSABILIDADES

- Es responsabilidad del Gerente de TI aprobar la presente política. Asimismo, asumir o designar a un responsable para las funciones y responsabilidades en la gestión de seguridad de la información ante la ausencia del Analista de Seguridad de la Información.

- El Analista de Seguridad de la Información es responsable de verificar y hacer de conocimiento al personal involucrado los lineamientos establecidos en el presente procedimiento.
- Es responsabilidad de los colaboradores cumplir con los lineamientos especificados en la presente política.
- Es responsabilidad de los proveedores cumplir con los lineamientos especificados en la presente política.

6. REGISTROS

- No aplica

7. ANEXOS

- No aplica

8. CONTROL DE CAMBIOS

Versión	Descripción	Autor	Aprobado por	Fecha Aprobación
V5	- Se actualizaron los apartados de: Objetivo, Alcance, Directrices y Documentos de Referencia.	Luis Rivera	Daniel Vidaurre	26/08/2026
V4	- Se agregó en el item 5: "…Asimismo, asumir o designar a un responsable para las funciones y responsabilidades en la gestión de seguridad de la información ante la ausencia del Analista de Seguridad de la Información."	Luis Rivera / Leslie Salazar	Daniel Vidaurre	03/02/2026
V3	- Se agregaron lineamientos en el documento referentes a la inclusión de normativa en el punto 4 de documentos de referencia. Se agregaron Decreto de Urgencia N° 007-2020 – Marco de Confianza Digital y la Ley N° 31814 – Ley que promueve el uso responsable de la Inteligencia Artificial. - En el punto 1 de objetivos se agregó el último lineamiento. - En el punto 3 se agregaron las 3 últimas directrices.	Luis Rivera / Julyanna Sandoval	Daniel Vidaurre	29/08/2025
V2	- Se actualizo el apartado de alcance, objetivo y directrices.	Jackelyn A/Luis R	Daniel Vidaurre	12/03/2025

V1	- Creación del documento	Diana Huiza	Daniel Vidaurre	14/02/2023