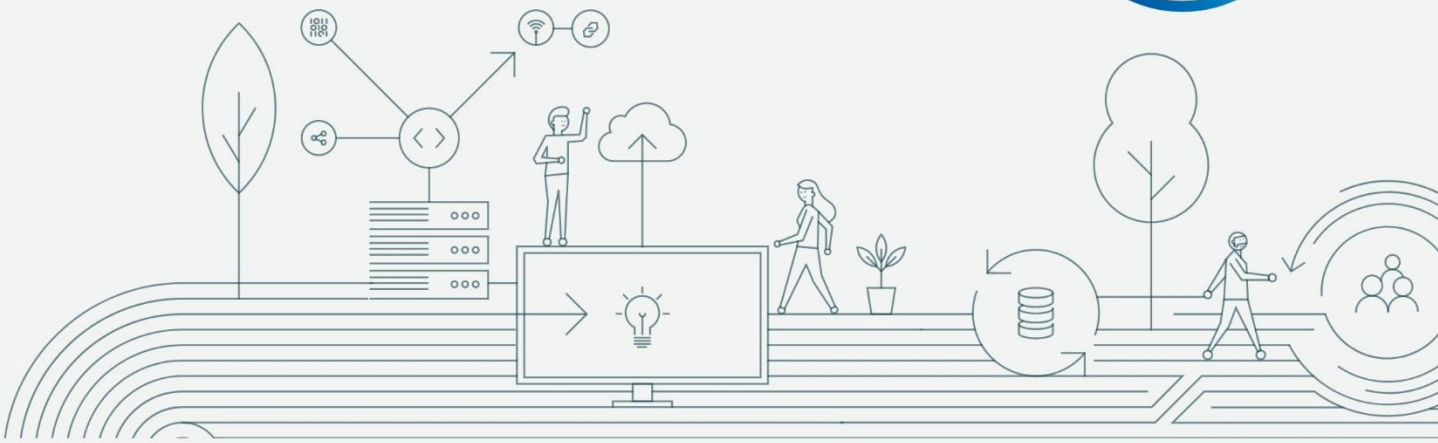

Política de Seguridad de la Información

Código:	GDE-PO-01
Versión:	1.0
Fecha de la versión:	06.10.2025
Elaborado por:	Oficial de Seguridad de la Información
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Director General
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
05.09.2022	0.1	Equipo de proyecto SGSI	Creación del documento
20.11.2024	0.2	Oficial de Seguridad de la Información	Modificación del documento en cuanto al comité por cambio de miembro del SGSI.
27.08.2025	1.0	Oficial de Seguridad de la Información	Inclusión de los apartados 2 y 3 Actualización del apartado 4

Tabla de contenido

1. Introducción

Este documento define la política de seguridad de la información de COMWARE.

COMWARE como una empresa moderna y con visión de futuro, reconoce a nivel directivo, la necesidad de asegurar que su operación se desarrolle de manera fluida y sin interrupciones, en beneficio de sus clientes, accionistas y demás partes interesadas.

Con el fin de proporcionar este nivel de operación continua, COMWARE implementó un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al documento internacional ISO/IEC 27001:2022.

Este documento define los requisitos para un SGSI basado en las mejores prácticas reconocidas internacionalmente.

El funcionamiento del SGSI aporta múltiples beneficios para la empresa, entre ellos:

- Garantiza la seguridad de la información de sus partes interesadas.
- Protección de las fuentes de ingresos y la rentabilidad de la compañía.
- Garantía en el suministro de bienes y servicios a los clientes.
- Mantenimiento y mejora del valor para los accionistas.
- Cumplimiento de los requisitos legales y regulatorios.

COMWARE mantiene su Sistema de Gestión de Seguridad de la Información (SGSI) certificado conforme al documento internacional ISO/IEC 27001. Esto permite que la adopción efectiva de las mejores prácticas en seguridad de la información sea validada continuamente por una tercera parte independiente, Organismo de Certificación registrado.

Esta política se aplica a todos los sistemas, personas y procesos que constituyen los sistemas de información de la organización, incluidos directores, colaboradores, proveedores y otras terceras partes que tengan acceso a los sistemas de COMWARE.

Los siguientes documentos complementarios son relevantes para esta política de seguridad de la información y proporcionan información adicional sobre cómo se aplica:

- GDE-PR-01 Procedimiento de evaluación y tratamiento de riesgos

- GDE-MN-01 Declaración de Aplicabilidad (SoA)
- GSI-PN-04 Objetivos de seguridad de la información y planificación para alcanzarlos.
- GDE-MN-02-Contexto, requisitos y alcance de la seguridad de la información.
- GSI-PR-07 Procedimiento para la gestión de eventos e incidentes de seguridad de la información.
- GSI-PO-01 Política de uso de dispositivos.
- GSI-PN-02 Plan de recuperación ante desastres.

Los detalles sobre el número de la última versión de cada uno de estos documentos están disponibles en el registro GSI-RG-36 Lista Maestra de Documentos.

2. Documentos de referencia

- ISO/IEC 27001:2022 cláusula 5.2

3. Términos y Definiciones

- **Política:** conjunto de principios, directrices y normas establecidas por una organización o entidad, que guían la toma de decisiones y el comportamiento dentro de un marco determinado.

- **Seguridad de la información:** se refiere a la protección de la información de una organización contra accesos no autorizados, alteraciones, destrucción, divulgación o interrupciones, asegurando que se mantengan la confidencialidad, integridad y disponibilidad de los datos.

- **Sistema de Gestión de Seguridad de la Información - SGSI:** enfoque estructurado para gestionar la seguridad de la información dentro de una organización. Su propósito principal es proteger los activos de información mediante un conjunto de políticas, procedimientos, controles y recursos, garantizando la confidencialidad, integridad y disponibilidad de los datos. El SGSI permite a las organizaciones identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información.

4. Política de Seguridad de la Información

4.1. Requisitos de seguridad de la información

COMWARE acordará y mantendrá una definición clara y documentada de los requisitos de seguridad de la información provenientes de sus líneas de negocio hacia los clientes.

Los requisitos legales, regulatorios y contractuales también se documentarán e incorporarán al proceso de planificación. Los requisitos específicos relacionados con la seguridad de nuevos sistemas o servicios, o aquellos que se modifiquen, se captarán como parte de la etapa de diseño de cada proyecto.

Es un principio fundamental del Sistema de Gestión de Seguridad de la Información de COMWARE que los controles implementados se basen en las necesidades del negocio, y esto se comunicará regularmente a todo el personal a través de reuniones de equipo y documentos informativos.

4.2. Objetivos de seguridad de la información

COMWARE estableció los siguientes objetivos de seguridad de la información:

- Reducir los incidentes de Seguridad de la Información.
- Lograr que los clientes recomienden los productos y servicios de Comware enfocados en Seguridad de la Información.
- Aplicar estándares de seguridad de la información que cumplan los requisitos de disponibilidad, integridad y confidencialidad.
- Asegurar cumplimiento de controles mínimos de configuración segura y protección de datos.
- Proteger la información de clientes y la propiedad intelectual en todos los servicios entregados.
- Garantizar la disponibilidad de los recursos de TI para la operación de los procesos de Comware.

Así también, de acuerdo con el documento internacional ISO/IEC 27001:2022, COMWARE adopta, cuando corresponda, los controles de referencia detallados en el Anexo A del documento internacional. Estos controles se revisan de manera regular con los resultados de las evaluaciones de riesgos y en línea con los planes de tratamiento de riesgos de seguridad de la información.

Además, se adoptan e implementan, según corresponda, controles mejorados y adicionales de los siguientes documentos internacionales:

- ISO/IEC 27002:2022 – Seguridad de la Información, ciberseguridad y protección de la privacidad: controles de seguridad de la información.

- ISO/IEC 27017 – Tecnología de la información - Técnicas de seguridad – Código de buenas prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube.

- ISO/IEC 27018 – Tecnología de la Información - Técnicas de seguridad – Código de buenas prácticas para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadoras de PII.

La adopción de estos códigos de práctica proporcionará garantías adicionales a nuestros clientes y contribuirá aún más al cumplimiento de la Ley de Protección de Datos Personales (LOPDP).

4.3. Mejora continua del SGSI

La política de COMWARE con respecto a la mejora continua es:

- Mejorar de manera continua la eficacia del SGSI.
- Fortalecer los procesos actuales para alinearlos con las buenas prácticas definidas en el documento internacional ISO/IEC 27001 y documentos relacionados.
- Mantenerla de manera continua la recertificación ISO/IEC 27001.
- Aumentar el nivel de proactividad (y la percepción de proactividad por parte de las partes interesadas) en materia de seguridad de la información.
- Hacer que los procesos y controles de seguridad de la información sean más medibles, a fin de proporcionar una base sólida para la toma de decisiones informadas.
- Revisar anualmente los indicadores y métricas relevantes para evaluar si es apropiado modificarlos, en base a los datos históricos recopilados.
- Obtener ideas de mejora mediante reuniones periódicas y otras formas de comunicación con las partes interesadas, incluidos los clientes de servicios en la nube.

- Revisar las ideas de mejora en las reuniones regulares de la dirección, con el fin de priorizarlas y evaluar los plazos y beneficios.

Las ideas de mejora pueden obtenerse de cualquier fuente, incluyendo empleados, clientes, proveedores, personal de TI, evaluaciones de riesgos e informes de servicio. Una vez identificadas, se registrarán y evaluarán como parte de las revisiones por la alta dirección.

4.4. Áreas de la política de seguridad de la información

COMWARE definió políticas en una amplia variedad de áreas relacionadas con la seguridad de la información, las cuales se describen en detalle en un conjunto integral de documentos de política que acompañan a esta política general de seguridad de la información.

Cada una de estas políticas fue definida y acordada por una o más personas con competencia en el área correspondiente y, una vez aprobada formalmente, se comunicó a las partes interesadas, tanto dentro como fuera de la organización.

En la Tabla 1 se muestra las políticas individuales que conforman el conjunto documental y resume el contenido de cada política, así como el público objetivo de las partes interesadas.

Título de la Política	Áreas abordadas	Público objetivo
Política de uso de activos	Seguridad de dispositivos móviles y portátiles; protección de la información fuera de las instalaciones.	Colaboradores con trabajo remoto; personal con dispositivos móviles y portátiles.
Política trae tu propio dispositivo (BYOD)	Permisos y restricciones para uso de dispositivos personales en actividades de la organización, seguridad de la información y	Empleados que utilicen dispositivos personales para actividades laborales.

Título de la Política	Áreas abordadas	Público objetivo
	requisitos de protección de datos.	
Política de clasificación y etiquetado de la información	Clasificación y etiquetado de la información según su sensibilidad; niveles de confidencialidad y requisitos de manejo.	Todos los empleados y contratistas que manejen información de la organización.
Política de uso aceptable	Define los comportamientos permitidos y prohibidos en el uso de recursos tecnológicos de la organización.	Todos los empleados, contratistas, consultores, proveedores y cualquier usuario autorizado que acceda a los recursos tecnológicos de la organización
Política de claves	Gestión de ciclo de vida de claves criptográficas, generación, distribución, almacenamiento, uso y eliminación.	Personal de TI, seguridad de la información y usuarios que utilicen cifrado o certificados digitales.
Política de control de acceso	Gestión de acceso de usuarios, privilegios mínimos, revisión de accesos, alta y baja de usuarios.	Todo el personal; principalmente TI y responsables de gestión de accesos.
Política del uso de criptografía	Directrices para el uso de cifrado, gestión de claves, algoritmos aprobados y protección de datos cifrados.	Personal de TI, seguridad de la información y usuarios que manejen información cifrada.
Política de pantalla y escritorio limpios	Prácticas para mantener áreas de trabajo libres de información confidencial	Todo el personal en oficinas, espacios compartidos o áreas públicas.

Título de la Política	Áreas abordadas	Público objetivo
	y bloqueo de pantallas cuando no se utilicen.	
Política de seguridad de equipos	Seguridad física y lógica de equipos de TI, manejo adecuado, ubicación y protección contra daños o robos.	Todo el personal que utilice equipos informáticos.
Política de creación de copias de seguridad	Directrices de respaldo, frecuencia, almacenamiento, protección y recuperación de copias de seguridad.	Equipos de TI, usuarios de sistemas críticos y gestión de continuidad.
Política de eliminación y destrucción	Lineamientos para eliminación segura y destrucción de información y activos, incluyendo dispositivos de almacenamiento.	Personal de TI, gestión documental y usuarios que gestionen información sensible.
Política para la protección contra malware	Medidas de prevención, detección y respuesta ante software malicioso, actualizaciones de antivirus y prácticas seguras de uso de dispositivos.	Todos los usuarios de equipos informáticos y dispositivos conectados a la red.
Política de transferencia de información	Seguridad en la transferencia de información dentro y fuera de la organización, incluyendo cifrado y autorizaciones.	Personal que comparta información internamente o con terceros.

Título de la Política	Áreas abordadas	Público objetivo
Política de gestión de cambios	Controles para la implementación de cambios en sistemas, infraestructura y aplicaciones de TI.	Equipos de TI, desarrollo, infraestructura y gestión de proyectos.
Política de Seguridad de la Información para las Relaciones con Proveedores	Requisitos de seguridad para proveedores y terceros; gestión de contratos y evaluación de seguridad de la información.	Áreas de compras, TI, seguridad de la información y responsables de contratos con proveedores.
Política de concientización	Establece directrices para capacitar y sensibilizar a los empleados sobre riesgos de seguridad de la información, buenas prácticas y cumplimiento normativo.	Todo el personal de la organización, especialmente nuevos empleados, usuarios con acceso a sistemas críticos y responsables de áreas operativas.
Política de seguridad de la información para el uso de servicios en la nube	Define los requisitos de seguridad para la adopción, uso y gestión de servicios en la nube, incluyendo protección de datos, acceso seguro y evaluación de proveedores.	quipos de TI, responsables de seguridad de la información, usuarios que gestionan o consumen servicios en la nube, y áreas que almacenan datos sensibles.
Política uso de la inteligencia artificial	Regula el desarrollo, implementación y uso ético de soluciones basadas en IA, asegurando transparencia,	Analistas de datos, responsables de innovación tecnológica, áreas legales y cualquier usuario que interactúe con sistemas de IA.

Título de la Política	Áreas abordadas	Público objetivo
	protección de datos y mitigación de sesgos.	
Política de líneas base de configuración	Establece configuraciones mínimas seguras para sistemas, redes y dispositivos, con el fin de reducir vulnerabilidades y asegurar la integridad de los activos tecnológicos.	Administradores de sistemas, personal de infraestructura, equipos de ciberseguridad y auditores técnicos.

Tabla 1. Políticas complementarias de Seguridad de la Información

4.5. Aplicación de la Política de Seguridad de la Información

Las declaraciones de política establecidas en este documento y en el conjunto de políticas de apoyo listadas en la Tabla 1 fueron revisadas y aprobadas por la alta dirección de COMWARE y deben ser cumplidas. El incumplimiento de estas políticas por parte de un colaborador puede resultar en la aplicación de medidas disciplinarias, de acuerdo con el Reglamento interno de Trabajo y el Código de Ética y Conducta de la compañía establecido por la organización.

Las preguntas relacionadas con cualquier política de COMWARE deben dirigirse, en primera instancia al Oficial de Seguridad de la Información.

5. Validez y gestión de documentos

En el caso de que se identifique un incumplimiento de las disposiciones establecidas en la presente Política, COMWARE se reserva el derecho de tomar las medidas necesarias para asegurar su cabal cumplimiento. Las infracciones de esta Política pueden dar lugar a acciones legales de índole disciplinario, de conformidad con lo establecido en el Reglamento interno de Trabajo y el Código de Ética y Conducta de la compañía.

El presente documento será revisado al menos una vez al año durante las revisiones por parte de la alta dirección.

Este documento es válido hasta la siguiente actualización.

El propietario de este documento es el Comité de Seguridad de la Información, quien debe verificar, y si es necesario actualizar el documento por lo menos una vez al año, tomando en consideración la conveniencia, adecuación y eficacia del SGSI y/o a través de las auditorías internas.

La alta dirección comunica a la Junta General de Accionistas el estatus del SGSI.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Conformidad del SGSI con la norma y con los demás documentos internos de la compañía.
- Ineficacia de la implementación y mantenimiento del SGSI de acuerdo con los informes de auditorías.