POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

La alta dirección de **WEARE DEV** entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus servicios con sus clientes y proveedores, todo enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
El objetivo de este documento es establecer las políticas, prácticas y lineamientos internos aplicables para el Sistema de Gestión de Seguridad de la Información (de ahora en más SGSI) para **WEARE DEV.**

2. ALCANCE

Esta política aplica a todos los procesos, activos de información, sistemas, empleados, contratistas y terceros que accedan o gestionen información de **WEARE DEV**.

3. LINEAMIENTOS

Contexto de la organización

3.1 Comprender a la organización y su contexto

WEARE DEV es una compañia dedicada al desarrollo, implementación y mantenimiento de soluciones de software diseñadas para optimizar los procesos de negocio de sus clientes en diversos sectores. La organización opera desde Medellín, Antioquia, y se caracteriza por su enfoque innovador, el uso de metodologías ágiles y su capacidad para integrar tecnologías emergentes en sus productos y servicios.

WEARE DEV reconoce que la información y los sistemas que la soportan son activos críticos para su operación y reputación. Por ello, ha establecido un **Sistema de Gestión de Seguridad de la Información (SGSI)** con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información frente a amenazas internas y externas.

Entre los factores internos y externos que influyen en el SGSI se incluyen:

- La evolución constante de las tecnologías utilizadas en el desarrollo de software.
- El aumento de las amenazas cibernéticas y las vulnerabilidades asociadas.
- Los cambios en la legislación sobre protección de datos y ciberseguridad.
- Las expectativas de los clientes sobre la seguridad y confiabilidad de los servicios.
- La cultura organizacional, las competencias del personal y el uso de infraestructura en la nube.

3.2 Comprender a las partes interesadas

WEARE DEV ha identificado las partes interesadas relevantes y sus requisitos en materia de seguridad de la información. Estos requisitos se analizan y revisan periódicamente para asegurar su cumplimiento dentro del alcance del SGSI.

Parte interesada	**Requisitos relevantes en materia de seguridad de la información**
Clientes	Confidencialidad de la información de negocio, cumplimiento de acuerdos contractuales y de nivel de servicio (SLA), disponibilidad de las plataformas de software.
Colaboradores y contratistas	Acceso seguro a los sistemas, capacitación en buenas prácticas de seguridad, cumplimiento de las políticas internas.
Proveedores y aliados tecnológicos	Cumplimiento de cláusulas contractuales de seguridad, uso seguro de información compartida, controles sobre servicios en la nube.
Entidades regulatorias	Cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales, así como otras regulaciones nacionales e internacionales aplicables.
Alta Dirección	Protección de la reputación corporativa, cumplimiento normativo, continuidad del negocio y retorno sostenible de la inversión.

Los requisitos de estas partes interesadas se consideran en el diseño, implementación y mejora del SGSI para garantizar su eficacia y alineación con los objetivos estratégicos de **WEARE DEV.**

3.3 Determinar el alcance del SGSI

El **Sistema de Gestión de Seguridad de la Información (SGSI)** de **WEARE DEV** abarca los procesos de:

- Desarrollo, implementación, despliegue y mantenimiento de software.
- Administración de infraestructura tecnológica y servicios alojados en la nube.
- Soporte técnico y atención a clientes.
- Gestión de la información interna y de terceros.

El SGSI aplica a todos los procesos de la organización y a todo el personal que maneje información o tenga acceso a los sistemas bajo control de **WEARE DEV.**
El alcance incluye las operaciones realizadas en la sede principal en Medellín, Antioquia, y en los entornos tecnológicos gestionados por la empresa o sus proveedores autorizados.

3.4 Sistema de gestión de la seguridad de la información

WEARE DEV ha implementado un **SGSI** conforme a los requisitos de la norma ISO/IEC 27001:2022.
El sistema proporciona un marco estructurado para identificar, evaluar y tratar los riesgos de seguridad de la información, aplicar controles adecuados, medir su desempeño y asegurar la mejora continua.
El SGSI se basa en el ciclo **Planificar – Hacer – Verificar – Actuar (PHVA)**, integrando la gestión de la seguridad con los procesos estratégicos y operativos de la empresa. Este sistema garantiza la protección de la información corporativa, la de los clientes y la de los aliados estratégicos.

Liderazgo

3.5 Liderazgo y compromiso

La **Alta Dirección de WEARE DEV** demuestra liderazgo y compromiso con el SGSI mediante:

- La definición y comunicación de la política de seguridad de la información.

- La asignación de recursos humanos, tecnológicos y financieros necesarios.
- El establecimiento de responsabilidades y autoridad para roles clave del SGSI.
- La integración de los requisitos de seguridad en los procesos de negocio.
- El impulso de una cultura organizacional orientada a la protección de la información.

La Alta Dirección designa un **responsable del SGSI** encargado de coordinar las actividades del sistema, liderar la gestión de riesgos, asegurar la ejecución de auditorías internas, y promover la mejora continua del SGSI.

3.6 Componentes claves de gestión de seguridad de la información

Gestión de Activos

- Identificación, inventario y clasificación de todos los activos de información.
- Asignación de responsables por cada activo.
- Etiquetado según niveles de confidencialidad: confidencial, organizacional o pública.

Control de Accesos

- Aplicación del principio de mínimo privilegio.
- Autenticación robusta (incluye multifactor).
- Revisión periódica de permisos y monitoreo de accesos.
- Gestión segura de contraseñas y solicitudes de acceso.

Protección de Datos Personales

- Cumplimiento de la Ley 1581 de 2012.
- Cifrado, anonimización y técnicas de enmascaramiento.
- Tratamiento autorizado y controlado de datos sensibles.

Dispositivos Móviles y Teletrabajo

- Uso exclusivo para fines laborales.
- Prohibición de aplicaciones no autorizadas.
- Conexión a redes seguras y reporte de incidentes.
- Capacitación en buenas prácticas de seguridad móvil.

Seguridad Física

- Control de acceso a instalaciones mediante credenciales y biometría.
- Videovigilancia, señalización y monitoreo continuo.
- Separación de procesos críticas y mantenimiento de infraestructura.

Seguridad en Sistemas y Aplicaciones

- Uso de herramientas como antivirus, firewall y antimalware.
- Aplicación de medidas de hardening.
- Validación periódica de sistemas críticos.

Filtrado Web

- Bloqueo de sitios maliciosos, inapropiados o no alineados con la cultura organizacional.
- Control sobre el uso de internet corporativo.

Gestión de Contraseñas

- Requisitos de complejidad y cambio periódico.
- Prohibición de almacenamiento inseguro.
- Uso de autenticación multifactorial.

Criptografía

- Cifrado de datos en tránsito y en reposo.
- Uso de protocolos como HTTPS, VPN, OpenPGP y AES256.
- Gestión de claves públicas y privadas.

Gestión de Riesgos

- Identificación, evaluación y tratamiento de riesgos.
- Revisión anual o ante cambios significativos.
- Integración de riesgos en proyectos y operaciones.

Continuidad del Negocio

- Planes de recuperación ante desastres.
- Asignación de responsables y recursos.
- Pruebas periódicas y mejora continua.

Gestión de Incidentes

- Registro, análisis y resolución de incidentes.
- Canales de reporte y seguimiento.
- Creación de base de conocimiento para eventos futuros.

Cumplimiento Normativo

- Identificación de requisitos legales y contractuales.
- Auditorías internas y revisión de políticas.
- Alineación con normativas locales e internacionales.

Relación con Proveedores

- Evaluación periódica de servicios.
- Contratos con cláusulas de seguridad y confidencialidad.
- Gestión de accesos y comunicación de requisitos.

Servicios en la Nube

- Uso exclusivo para funciones laborales.
- Cifrado de información sensible.
- Evaluación de riesgos y cumplimiento de políticas de respaldo y cambios.

Ciclo de Vida del Desarrollo

- Seguridad en todas las fases del desarrollo de software.
- Segregación de ambientes (desarrollo, pruebas, producción).
- Control de cambios y uso de datos no productivos.

Gestión de Logs

- Registro y monitoreo de actividades en sistemas.
- Detección de accesos no autorizados o comportamientos inusuales.

Gestión de Vulnerabilidades Técnicas

- Ethical hacking y escaneo de vulnerabilidades.
- Priorización y remediación de riesgos técnicos.
- Actualización constante de sistemas y parches.

Seguridad en Redes

- Segregación de redes y uso de VPN.
- Protección de datos en tránsito.
- Políticas para medios extraíbles y comunicación segura.

Inteligencia de Amenazas

- Análisis de amenazas emergentes.
- Uso de servicios SOC para detección y respuesta.
- Compartición de información relevante para prevención.

3.7 Roles, responsabilidades y autoridades

La alta dirección de **WEARE DEV** ha definido los roles y asignado sus responsabilidades asociadas al SGSI dentro del documento de Descriptivo de Roles y Responsabilidades que establece, entre otras cosas, lo siguiente:

- Todos los roles necesarios para llevar a cabo las actividades requeridas por la ISO 27001.
- Las responsabilidades que asume cada uno de los roles involucrados en el SGSI.
- La responsabilidad del Oficial de Seguridad de la Información (OSI), en conjunto con el Comité de Seguridad es, entre otras, velar por el cumplimiento del SGSI y de informar sobre su desempeño a la alta dirección y a la organización.
- Así como también dentro de la Política del Comité de Seguridad de la Información donde se establecen las funciones de los integrantes del comité definido por la organización.

Planificación

3.8 Acciones para tratar los riesgos y oportunidades

WEARE DEV implementa un proceso de gestión de riesgos que incluye:

- **Identificación:** detección de amenazas y vulnerabilidades.
- **Evaluación:** análisis del impacto y probabilidad.
- **Tratamiento:** selección e implementación de controles según la declaración de aplicabilidad (SoA).
- **Monitoreo:** seguimiento continuo y actualización de riesgos.

Las oportunidades identificadas se integran en planes de mejora continua del SGSI.

3.9 Objetivos de seguridad de la información y planificación para alcanzarlos

WEARE DEV establece sus objetivos de seguridad bajo un enfoque de alto nivel, pero estrechamente relacionados a los objetivos organizacionales. Los objetivos del SGSI deben:

- Ser consistentes con la Política de Seguridad de la Información.
- Contemplar los resultados de la evaluación y los planes de tratamiento de los riesgos.
- Estar disponibles y documentados.
- Ser actualizados, cuando sea requerido.

WEARE DEV declara los siguientes objetivos de seguridad de la información alineados al SGSI y a su estrategia, para el año 2025:

1. Asegurar y mantener la confidencialidad y disponibilidad de la información de la compañía.

2. Velar por el cumplimiento hacia la prevención de las amenazas de vulnerabilidad mitigando y/o eliminar los casos presentados.

3. Garantizar la integridad de la información en los sistemas que procesan datos corporativos

4. Asegurar y mantener la confidencialidad y disponibilidad de la información de la compañía.

3.10 Planificación de cambios

WEARE DEV determina que cualquier cambio que se considere necesario para el SGSI, éste debe llevarse a cabo de manera planificada. Además, debe ser aprobado por la alta dirección y comunicado a la organización y partes interesadas.

Soporte

3.11 Recursos

WEARE DEV dedica un presupuesto que le permita asegurar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, el cual debe ser aprobado por la alta dirección.
Este presupuesto y su aprobación permanecen como información documentada.
Asimismo, se garantiza la participación del recurso humano necesario para el SGSI y se dispone de los recursos de infraestructura tecnológica que soportan la operación.

3.12 Competencia

WEARE DEV garantiza que el personal que desempeña funciones que afectan la seguridad de la información sea competente, con base en educación, formación, habilidades y experiencia verificable.
Se mantienen registros de capacitación y evaluación de competencias relacionadas con el SGSI.

3.13 Concientización

Todos los colaboradores y contratistas reciben formación y campañas periódicas sobre seguridad de la información, orientadas a fomentar la responsabilidad en el manejo de los activos y la prevención de incidentes.

3.14 Comunicación

WEARE DEV define y mantiene un plan de comunicación interna y externa relacionado con el SGSI, asegurando que:

- La información se comunique de manera oportuna y precisa.
- Se definan responsables, canales y frecuencias de comunicación.
- Se preserve la confidencialidad de los mensajes relacionados con seguridad

3.15 Información documentada

3.15.1 General

Toda la documentación del SGSI, incluyendo políticas, procedimientos, registros y evidencias, se gestiona bajo control documental.
Cada documento tiene un código, versión, responsable, fecha de emisión y revisión.
Se utilizan repositorios seguros para asegurar la integridad, disponibilidad y confidencialidad de la información.

Operación

3.16 Control y planificación operacional

WEARE DEV planifica, implementa y controla los procesos necesarios para cumplir los requisitos del SGSI, asegurando que:

- Se definan criterios de operación segura.
- Se implementen controles técnicos y administrativos adecuados.
- Se mantengan evidencias documentadas de la ejecución.

- Se tomen acciones correctivas cuando los resultados no cumplan con los objetivos planificados.

El control operacional incluye la gestión de incidentes, continuidad del negocio, control de accesos, y mantenimiento de la infraestructura tecnológica.

3.17 Evaluación de los riesgos de seguridad de la información

La evaluación de riesgos debe ser periódica por lo que WeAre Dev SAS ha definido aplicarla cada año, o cuando se produzcan modificaciones importantes.
Las condiciones para la aplicación adecuada de estas evaluaciones son especificadas en la Metodología de Gestión de Riesgos.
Asimismo, los resultados de las evaluaciones de riesgos se encuentran disponibles como información documentada en los repositorios autorizados

3.18 Tratamiento de los riesgos de seguridad de la información

WEARE DEV implementa el plan de tratamiento de riesgos, para cada riesgo identificado se tienen medidas de tratamiento que pueden incluir:

- Mitigación mediante controles técnicos u organizaciones
- Transferencia mediante seguros o acuerdos con terceros
- Aceptación con justificación documentada.

Los resultados se documentan en la matriz de tratamiento de riesgos y en la declaración de aplicabilidad.

Evaluación del desempeño

3.19 Seguimiento, medición, análisis y evaluación

WEARE DEV evalúa el desempeño del SGSI mediante:

- Indicadores de cumplimiento de objetivos
- Revisión de incidentes y medidas preventivas
- Evaluaciones periódicas de eficacia de controles

Los resultados se documentan y se utilizan para la mejora continua.

3.20 Auditorías internas

WEARE DEV realiza auditorías internas planificadas al menos una vez al año, con el fin de verificar:

- Verificar la conformidad del SGSI con los requisitos de ISO 27000:2022
- Evaluar la eficacia de los controles implementados
- Identificar oportunidades de mejora

Las auditorias son realizadas por el personal competente e independiente de los procesos auditados. Los hallazgos se documentan y se gestionan acciones correctivas.

3.21 Revisión por la alta dirección

3.21.1 General (Requisito 9.3.1)

La alta dirección y el comité que conforman a **WEARE DEV** realizan una rendición de cuentas mensual y una revisión anual del SGSI para garantizar su conveniencia, continuidad, vigencia, adecuación y efectividad.

3.21.2 Insumos para la revisión por la dirección

La revisión por la dirección comprende lo siguiente:

- El seguimiento de las acciones de revisiones previas.
- Cambios significativos internos y externos de la organización, relevantes para el SGSI.
- Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI.
- Los resultados de la retroalimentación sobre el desempeño de la Seguridad de la Información en la empresa:
- No conformidades y acciones correctivas.
- Resultados de auditorías internas y externas.
- Resultados de métricas e indicadores.
- Cumplimiento de los objetivos.
- Retroalimentación de las partes interesadas.

Esta información se obtiene por medio de encuestas de clima laboral para la retroalimentación de los colaboradores, actas de comité de seguridad, formato de reportes HSEQ y un correo electrónico habilitado en la página web para cualquier parte interesada externa, por medio del siguiente correo electrónico: **info@WEARE DEV.co.**
Los resultados de la valoración y gestión de riesgos del SGSI y el estado del plan de tratamiento.

Oportunidades de mejora continua.

3.21.3 Resultados de la revisión por la dirección

WEARE DEV genera la minuta de sesión de comité como información documentada donde incluye los resultados de la revisión y las decisiones para el mantenimiento y mejora continua del SGSI.

Mejora

3.22 Mejora continua

WEARE DEV realiza acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSI y deja registro de esto en los siguientes documentos:

Procedimiento de Acciones Correctivas y de Mejora
Plan de Tratamiento de Acciones Correctivas y de Mejora

3.23 No conformidad y acción correctiva

Al presentarse una no conformidad, la compañía:

- Toma las acciones para controlarla, corregirla y atender las consecuencias de ésta.
- Evalúa si es posible eliminar la causa de la no conformidad, mediante su revisión, determinación de sus causas y verificación de no conformidades similares.
- Implementa las acciones necesarias.
- Revisa la efectividad de las acciones realizadas.
- Realiza cambios sobre el SGSI, si es requerido.

La organización deja registro de esto en los siguientes documentos:

- Procedimiento de Acciones Correctivas y de Mejora
- Plan de Tratamiento de Acciones Correctivas y de Mejora
- Análisis Causa Raíz

WEARE DEV asegura que las acciones correctivas aplicadas son acordes y proporcionales a las no conformidades que se encontraron.

5. CONTROL DE CAMBIOS

CONTROL DE DOCUMENTOS				
FECHA	**ELABORADO**	**REVISADO**	**APROBADO**	**CONTROL DE CAMBIOS**
15/04/2024	Directora HSEQ	Comité de Seguridad de la información	CEO	Versión 01 Creación del documento
07/02/2025	Directora HSEQ	Comité de Seguridad de la información	CEO	Versión 02 Clasificación de la información
27/10/2025	OSI	Comité de seguridad de la información	CEO	Versión 03 modificación de documento e integración con política de seguridad