

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

1. DECLARACIÓN DE LA POLÍTICA

En Bigfive B5 S.R.L., empresa dominicana con presencia regional en Centro y Sudamérica especializada en servicios integrales de ciberseguridad, implementamos nuestro Sistema de Gestión de Seguridad de la Información (SGSI) conforme a los requisitos en seguridad de la norma ISO/IEC 27001:2022, con el compromiso de garantizar la confidencialidad, integridad y disponibilidad de la información de nuestros clientes y de la organización.

La Dirección establece este marco de seguridad para sustentar la excelencia en la prestación de nuestros servicios especializados seguridad de la información, asignando los recursos necesarios y definiendo objetivos alineados con la estrategia del negocio.

Nuestro SGSI se fundamenta en la aplicación sistemática de mejores prácticas de seguridad que integran principios, procesos y responsabilidades claramente definidas, implementando un enfoque proactivo de gestión de riesgos que permite identificar, evaluar y tratar las amenazas a los activos de información. Mediante este enfoque, aseguramos el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables, minimizando los riesgos asociados al uso, almacenamiento, procesamiento y transmisión de la información en nuestros procesos internos.

2. ALCANCE

Esta política es aplicable a:

- Todos los sistemas, redes y activos de información involucrados en la prestación de Servicios de Monitoreo y Alertamiento SOC, Servicio de Ciberinteligencia CTI y entrega de Servicio de Análisis y Respuesta a Incidentes CSIRT.
- Todo el personal permanente, temporal y contratistas o proveedores relacionados con los procesos de Entrega del Servicios de Monitoreo y Alertamiento SOC, Servicio de Ciberinteligencia CTI y entrega de Servicio de Análisis y Respuesta a Incidentes CSIRT.
- Todos los procesos operativos y de apoyo relacionados con la gestión de seguridad de la información y la entrega de Servicios de Monitoreo y Alertamiento SOC, Servicio de Ciberinteligencia CTI y entrega de Servicio de Análisis y Respuesta a Incidentes CSIRT.



- Todas las ubicaciones físicas donde se procesa información relacionada con los servicios mencionados.

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Esta política establece el marco para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001:2022, alineado con nuestros objetivos de negocio:

3.1. Objetivos:

3.1.1. **Objetivo 1: Fortalecer la cultura de seguridad de la información en los equipos SOC, CTI y CSIRT.**

Este objetivo se encuentra alineado al O.E. 7 “Mantener la sostenibilidad operacional y rentabilidad del negocio”. Promoviendo una cultura organizacional basada en la seguridad de la información a través de programas de capacitación continua, simulaciones de incidentes y adopción de mejores prácticas, reduciendo los incidentes derivados del factor humano y asegurando la correcta aplicación de los controles técnicos especializados requeridos para la prestación de servicios de seguridad gestionada.

3.1.2. **Objetivo 2: Gestionar adecuadamente los riesgos de seguridad para fortalecer la resiliencia operacional y continuidad operativa de los servicios del alcance del SGSI, y salvaguardar la disponibilidad, integridad y seguridad de los activos de información del alcance del SGSI.**

Este objetivo se encuentra alineado al O.E. 7 “Mantener la sostenibilidad operacional y rentabilidad del negocio”. Implementando un proceso continuo de gestión de riesgos de seguridad de la información, mediante la identificación, evaluación y mitigación de amenazas avanzadas, asegurando la aplicación de controles alineados con los requerimientos de clientes y estándares del sector para proteger la infraestructura crítica de monitoreo y respuesta.

3.1.3. **Objetivo 3: Garantizar la excelencia operacional mediante la gestión efectiva de incidentes de seguridad.**

Este objetivo se encuentra alineado al OE4 “Fortalecer soluciones propias y desarrollar capacidades técnicas especializadas para la excelencia en servicios de seguridad”. Asegurando la implementación de procesos de gestión de incidentes de clase mundial que mantengan la disponibilidad, integridad y confidencialidad de



los servicios, enfocándose en cumplir y superar los SLAs establecidos, y manteniendo capacidades de respuesta inmediata y análisis forense de alta precisión.

3.1.4. **Objetivo 4: Obtener y mantener la certificación ISO 27001 y otras certificaciones relevantes del sector.**

Este objetivo se encuentra alineado al OE3 “Obtener certificación ISO 27001 en la sede principal para los servicios críticos para el primer semestre del 2026 y posicionarse como proveedor de referencia en el sector de seguridad de la información en el sector local y regional”. Garantizando el cumplimiento continuo con el estándar ISO 27001:2022 y otros marcos regulatorios aplicables, para demostrar a clientes y partes interesadas el compromiso con los más altos estándares de seguridad y la mejora continua del SGSI.

3.1.5. **Objetivo 5: Retener 70% talento y fortalecer el plan de capacitación y desarrollo para perfiles con alto potencial.**

Este objetivo se encuentra alineado al OE8: “Retener 70% talento y fortalecer el plan de capacitación y desarrollo para perfiles con alto potencial”. Asegura la mejora continua de las capacidades de detección y respuesta mediante la formación especializada, la actualización constante del personal y el desarrollo de habilidades especializadas en el equipo técnico, para enfrentar de manera efectiva el panorama moderno de amenazas.

3.2 Compromisos:

En fiel cumplimiento de estos objetivos, la empresa se compromete a:

- Proporcionar los recursos económicos, humanos e infraestructura necesarios para la adecuada gestión y funcionamiento del SGSI.
- Capacitar al personal en el sistema de gestión SGSI, fortaleciendo su gestión mediante la evaluación y motivación a los colaboradores.
- Dar cumplimiento a la legislación y normativa vigente en Seguridad de la Información, de tal manera que se cumplan los objetivos empresariales en este ámbito.
- Dar a conocer y difundir esta política y publicarla para nuestros colaboradores, proveedores, clientes, y entes de control, siendo expuesta en los sitios más relevantes de la empresa.



- Promover la mejora continua de esta política y del sistema de gestión, acorde a los procesos internos y a la legislación vigente, actualizándose frecuentemente.

Esta política ha sido revisada y aprobada por la Gerencia General de Bigfive B5 S.R.L. y entra en vigor a partir del 12 de noviembre de 2025.

Aprobado por:

Gerencia General Bigfive
11/11/2025

4. REVISIÓN Y ACTUALIZACIÓN

El presente documento será revisado al menos una vez al año o cuando se requiera.

4.1 Historial de revisión y aprobación

| Ver. | Fecha | Razón de actualización | Preparado por | Revisado por | Aprobado por |
|------|------------|--------------------------------|---------------------------|--------------|-----------------|
| 1.0 | 12/11/2025 | Creación inicial del documento | Coordinadora Regional GRC | Gerente CTO | Gerente General |

