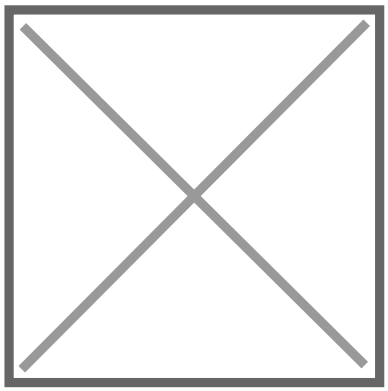
Política de Seguridad, Ciberseguridad y Continuidad del Servicio

- POL-TI-SEC-01: Política de Ciberseguridad y Continuidad del Servicio

POL-TI-SEC-01: Política de Ciberseguridad y Continuidad del Servicio

	**Política Corporativa de Seguridad de la Información, Ciberseguridad y Continuidad del Servicio.**	Fecha de elaboración: 2026/05/22
	InterServicios S.A.S.	Código: POL-TI-SEC-01
		Versión: 1.0

1. Objetivo de la Política

Establecer las directrices, lineamientos y controles formales destinados a proteger los activos de información, plataformas de software y la infraestructura tecnológica administrada por **INTERSERVICIOS S.A.S.**, garantizando de forma estricta los principios de confidencialidad, integridad y disponibilidad de la información, así como la resiliencia y continuidad de los servicios prestados ante contingencias o incidentes de ciberseguridad.

2. Alcance

Esta política es de cumplimiento obligatorio y aplica a todas las soluciones de software desarrolladas, contratadas o alojadas por la organización, las plataformas tecnológicas en producción, los servicios dedicados, así como al personal técnico, administrativo y proveedores externos de infraestructura involucrados en la cadena de entrega del servicio a nuestros clientes.

3. Marco Institucional de Infraestructura (Capa Data Center)

INTERSERVICIOS S.A.S. delega el alojamiento físico y de conectividad perimetral de sus servidores dedicados en un proveedor global de primer nivel, el cual cuenta con la certificación internacional

Type 2 SOC 2 con cumplimiento HIPAA/HITECH. Los controles mínimos exigidos y validados en esta capa comprenden:

- **Seguridad Física Corporativa:** Restricción estricta de acceso mediante biometría de huella dactilar, tarjetas de proximidad, sistemas cerrados de televisión (CCTV) con vigilancia activa 24/7 y racks independientes bajo llave.
- **Seguridad Ambiental y de Hardware:** Infraestructura con redundancia N+1 en suministro eléctrico (sistemas UPS autónomos y generadores diésel de emergencia), climatización HVAC de precisión, sistemas de supresión de incendios por tubería seca y sensores automatizados de inundación.
- **Protección de Red Perimetral:** Despliegue de firewalls de alta disponibilidad a nivel de capa de red (Juniper) con políticas restrictivas *"Deny All"* por defecto y sistemas integrados de mitigación proactiva contra ataques de denegación de servicio distribuidos (DDoS).

4. Controles Técnicos, Administrativos y Operativos (Capa Servidor y Aplicación)

Como administradores del software e infraestructura lógica, el área de TI de INTERSERVICIOS S.A.S. implementa de forma permanente los siguientes controles de seguridad:

4.1 Control de Acceso Lógico y Administrativo

Todo acceso a los entornos de gestión y bases de datos está restringido bajo el principio de privilegio mínimo y la segregación de funciones. El acceso al servidor está estrictamente limitado a personal autorizado vía llaves SSH cifradas y restringido explícitamente por direccionamiento IP.

4.2 Gestión de Parches y Vulnerabilidades

Se mantiene un ciclo de actualización y remediación proactiva que incluye la aplicación periódica de parches críticos de seguridad sobre los sistemas operativos y dependencias de software. Anualmente se programan escaneos de vulnerabilidades y pruebas de penetración (*pentesting*) con firmas de auditoría externas autorizadas. El software del servidor cuenta con la protección activa de **CSF (ConfigServer Security & Firewall)**.

4.3 Gestión Humana y Confidencialidad

Todo el personal técnico con acceso a datos o código firma acuerdos estrictos de confidencialidad y no divulgación (NDA), complementados con rigurosas validaciones de antecedentes previas a la contratación laboral.

5. Prevención, Detección y Respuesta a Incidentes de Ciberseguridad

La organización mantiene una postura de monitoreo continuo para identificar anomalías operativas de manera temprana:

- **Sistemas de Detección:** Despliegue de herramientas automatizadas para la detección de intrusos (IDS) y el monitoreo de integridad de archivos (FIM) mediante plataformas de monitoreo como Zabbix y OSSEC, alertando sobre cualquier intento de intrusión o modificación no autorizada de archivos.
- **Plan de Respuesta a Incidentes (IRP):** En caso de detectarse una anomalía, se activa de inmediato el protocolo de aislamiento de la amenaza, análisis forense y remediación.
- **Protocolo de Notificación:** Las incidencias de seguridad que afecten potencialmente la operación o datos de los clientes se notificarán de forma inmediata una vez detectadas, utilizando canales formales de soporte mediante la plataforma de tickets con copia automatizada al correo electrónico del cliente.

6. Continuidad de Negocio y Recuperación ante Desastres (BCP / DRP)

En concordancia con el Plan de Continuidad del Negocio institucional, INTERSERVICIOS S.A.S. fundamenta su gobernanza TIC bajo las buenas prácticas internacionales de las normas **ISO 22301 e ISO 27001**.

6.1 Estrategia de Copias de Seguridad (Backups)

Para asegurar la integridad de la información histórica y transaccional, se definen las siguientes directrices obligatorias:

- **Frecuencia de Ejecución:** Se ejecutan de manera automatizada respaldos programados bajo la periodicidad de **1 diario, 1 semanal y 1 mensual**.
- **Retención y Resguardo:** Las copias de seguridad se almacenan de forma segura bajo cifrado AES con una retención mínima de 2 respaldos diarios, 1 respaldo semanal y 1 respaldo mensual.

6.2 Métricas Objetivas de Resiliencia (RTO y RPO)

Ante un evento de contingencia o desastre crítico que afecte el funcionamiento del software, la organización se compromete a mantener los servicios dentro de los siguientes umbrales tolerables:

- **RPO (Punto Objetivo de Recuperación):** Máximo de **24 horas**, garantizando que ante un fallo total de hardware la pérdida máxima de datos no superará dicho período.
- **RTO (Tiempo Objetivo de Recuperación):** Tiempo estimado para restablecer y poner en línea el servicio operativo de un máximo de **12 horas** a partir del diagnóstico y declaración del incidente.

6.3 Gobernanza, Pruebas del Plan y Emisión

La gestión de crisis tecnológicas está a cargo del **Comité de Desastres TIC**, coliderado por la Gerencia de Proyectos (Dirección de Continuidad) y el Líder de TI. Este comité tiene la responsabilidad de coordinar ejercicios de entrenamiento y simulacros de restauración de datos como mínimo una (1) vez al año para certificar la efectividad de las copias de respaldo.

La presente política será revisada de forma anual por el Área de TI para garantizar su alineación frente a nuevas amenazas. Para constancia de su obligatoriedad y entrada en vigencia formal.

Elaborado por: Karen Cano	Revisado por: Diego Tobón	Aprobado por: Jorge Tobón
Fecha de elaboración: 2026/05/22	Fecha Revisión: 2026/05/22	Fecha Aprobación: 2026/05/25