



POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022

COBPE-SGSI-PO-04
Versión: 02
Fecha: 02/10/2026
Página 1 de 2

1. PROPÓSITO Y ALCANCE

Cobranzas Perú S.A.C. establece la presente Política de Seguridad de la Información con el propósito de proteger la confidencialidad, integridad y disponibilidad de la información que recibe, procesa, almacena, utiliza y transmite durante la prestación de sus servicios de gestión integral de cobranzas.

La organización reconoce que la información personal y financiera de los deudores es proporcionada por sus clientes, principalmente entidades bancarias y financieras, para su tratamiento en el marco de los servicios de cobranza contratados. En consecuencia, Cobranzas Perú S.A.C. actúa como encargado del tratamiento de dichos datos, conforme a las instrucciones, finalidades autorizadas y obligaciones contractuales establecidas por sus clientes, sin asumir la titularidad de la información recibida.

La presente política comprende los procesos, actividades, sistemas de información, infraestructura tecnológica y recursos relacionados con la gestión integral de cobranzas, desde la recepción de las carteras de clientes hasta la generación de reportería estratégica, considerando los canales de gestión **Call Center, SMS, IVR y Mailing**, así como los ambientes tecnológicos **Transaccional y VICIdial**.

Su aplicación comprende las sedes ubicadas en Av. Petit Thouars 3638 y Calle Las Casas 165, San Isidro, Lima, y alcanza al personal, responsables de procesos y terceros que intervienen en las actividades comprendidas dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a ISO/IEC 27001:2022 y a los requisitos legales y contractuales aplicables.

2. PRINCIPIOS DE SEGURIDAD

- **Confidencialidad:** Garantizar que la información sensible solo sea accesible por personas autorizadas mediante controles de acceso, cifrado y clasificación.
- **Integridad:** Asegurar exactitud y veracidad de la información evitando modificaciones no autorizadas en bases de datos y registros.

- **Disponibilidad:** Garantizar que sistemas críticos estén disponibles mediante continuidad del negocio, copias de seguridad y gestión de incidentes.
- **Trazabilidad:** Mantener registros auditables de accesos, modificaciones y gestiones para cumplimiento legal.

3. COMPROMISOS DE LA ALTA DIRECCIÓN

La Alta Dirección se compromete a:

- Proporcionar recursos necesarios para implementar, mantener y mejorar continuamente el SGSI.
- **Cumplir requisitos legales (Ley Nro. 29733, INDECOPI, OSIPTEL, SBS).**
- Establecer y revisar objetivos de seguridad alineados con objetivos estratégicos.
- Promover cultura de seguridad mediante capacitación continua.
- Gestionar proactivamente riesgos mediante análisis periódicos y controles.
- Mejorar continuamente mediante auditorías y acciones correctivas.
- Garantizar privacidad y protección de datos personales respetando derechos ARCO.

4. RESPONSABILIDADES

- **Alta Dirección:** Aprobar, comunicar y garantizar cumplimiento, asignando recursos.
- **Jefatura de Sistemas/CISO:** Coordinar implementación, mantenimiento y gestión de riesgos.
- **jefes de Área:** Garantizar cumplimiento en sus áreas y promover concientización.
- **Colaboradores:** Conocer, cumplir y reportar incidentes de seguridad.
- **Proveedores:** Cumplir requisitos de seguridad contractuales.

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2022

COBPE-SGSI-PO-04
Versión: 02
Fecha: 02/10/2026
Página 2 de 2

5. GESTIÓN DE RIESGOS

Se implementará metodología sistemática para identificar, analizar, evaluar y tratar riesgos de seguridad que afecten confidencialidad, integridad y disponibilidad de activos críticos, considerando amenazas internas, externas, tecnológicas, humanas y de procesos. Los riesgos serán revisados periódicamente y tratados mediante controles del Anexo A de ISO 27001:2022.

Como parte del análisis del contexto del SGSI, la organización determinará la pertinencia del cambio climático y sus posibles efectos sobre la seguridad de la información, disponibilidad de los servicios y continuidad de las operaciones.

6. INCIDENTES DE SEGURIDAD

Todos los colaboradores deben reportar inmediatamente cualquier incidente (accesos no autorizados, pérdida de datos, malware, brechas) a la Jefatura de Sistemas. La organización responderá rápida y efectivamente, realizará análisis de causa raíz e implementará acciones correctivas, cumpliendo obligaciones legales de notificación cuando corresponda.

7. CUMPLIMIENTO Y MEJORA CONTINUA

Esta política será revisada anualmente o ante cambios significativos en el contexto organizacional, requisitos legales, tecnología o riesgos. Se realizarán auditorías internas periódicas para verificar cumplimiento y eficacia de controles. Los resultados serán utilizados para la mejora continua del SGSI.

8. COMUNICACIÓN Y TOMA DE CONCIENCIA

Esta política será comunicada a todos los colaboradores, proveedores y partes interesadas relevantes, estando disponible en la plataforma interna. Se implementarán programas de capacitación y concienciación continua para garantizar su comprensión y cumplimiento.

CONTROL DE VERSIONES

Versión	Fecha	Descripción del cambio	Elaborado por	Revisado por	Aprobado por
01	10/12/2025	Emisión inicial de la Política del SGSI	Responsable SGSI	Jefatura de Sistemas/CISO	Gerencia General
02	02/10/2026	Incorporación de la consideración del cambio climático conforme a ISO/IEC 27001:2022/Amd 1:2024.	Responsable SGSI	Jefatura de Sistemas/CISO	Gerencia General



FRANKLIN CISNEROS SOLÍS
Gerente General
Cobranzas Perú SAC