POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Documento redactado por:	Felipe Dittus	Gerente SGI / CISO
Documento revisado por:	Andres Pozo	Asesor TI
Documento aprobado por:	Verónica Gajardo	Gerente General

1. DECLARACIÓN INSTITUCIONAL

COBRANZAS ASSETS LTDA, enfocados en brindar servicios de gestión y asesoría de cuentas por cobrar (Cobranzas), tiene entre sus objetivos organizacionales consolidarse como empresa líder del mercado, construyendo relaciones comerciales perdurables con sus clientes, sustentadas en soluciones tecnológicas innovadoras con altos estándares de calidad y seguridad.

Los negocios de **COBRANZAS ASSETS LTDA** se basan en la confianza y dependen estrechamente de la información que emana de la propia organización y que le confían sus clientes, de allí que su gestión de manera segura y responsable sea un requisito indispensable para el logro de los objetivos organizacionales, implicando un factor estratégico para la rentabilidad, continuidad operacional, reputación empresarial y, por tanto, para la sustentabilidad a largo plazo.

Reconociendo la importancia que implica la información para la organización, **COBRANZAS ASSETS LTDA** ha asumido el compromiso de establecer una estructura corporativa responsable de garantizar el cumplimiento de los objetivos de seguridad de la información con fundamento en las leyes, regulaciones, normas, acuerdos contractuales, políticas y procedimientos aplicables y en concordancia con los objetivos estratégicos.

Asimismo, la alta dirección se ha comprometido en implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) sustentado en la norma ISO/IEC 27001:2022, teniendo en la Política General de Seguridad de la Información y demás políticas complementarias, el marco aplicable para la ejecución de medidas que permitan identificar, evaluar y analizar de manera estructurada y eficiente los riesgos que pudieran afectar a los activos de información relevantes. Lo anterior hará posible implementar controles adecuados para la mitigación de dichos riesgos, garantizado con ello la confidencialidad, integridad y disponibilidad de la información. Esta integración junto a Sistema de Gestión de calidad (SGC) sustentado en la norma ISO/IEC 9001:2015 conforman el Sistema de Gestión Integrado de **COBRANZAS ASSETS LTDA.**

2. OBJETIVO

El propósito de esta Política General de Seguridad de la Información es definir los lineamientos y requisitos generales aplicables a fin de garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por **COBRANZAS ASSETS LTDA** Lo anterior incluye:

a.- Cumplir con los requisitos de nuestros clientes
b.- Resolver oportunamente los reclamos de nuestros clientes
c.- Implementar anualmente a lo menos 3 mejoras al sistema de gestión de la seguridad de la información

d.- Mantener en 0 la cantidad de incidentes de seguridad de la información relacionadas con pérdidas de confidencialidad reflejados en reportes de incidentes
e.- Mantener en 0 la cantidad de incidentes de seguridad física relacionadas con pérdidas de integridad reflejados en reportes de incidentes
f.- Mantener en un 95% las vulnerabilidades técnicas de sistemas y aplicaciones y a las acciones implementadas para corregirlas
g.- Mantener en cero las multas o sanciones por incumplimiento legal y contractual
h.- Mantener en 100% el cumplimiento de la Matriz de Requisitos Legales en forma anual

3. ALCANCE

Considerando la cadena de valor de **COBRANZAS ASSETS LTDA**, su contexto interno y externo, así como los requisitos de seguridad de la información de las partes interesadas, se establece que en el Sistema de Gestión Integrado y, en consecuencia, la Política General de Seguridad de la Información, aplica a todos los procesos relacionados con la generación del servicio.

La Política General de Seguridad de la Información debe ser aplicada por todos los colaboradores, contratistas y proveedores que usen activos de información que se encuentren dentro del alcance antes mencionado.

Asimismo, la Política General de Seguridad de la Información cubre la información durante todo su ciclo de vida, desde su recopilación, almacenamiento, uso y transferencia, hasta su disposición final, indistintamente de que se trate de información escrita, impresa, en formato digital o que sea compartida verbalmente.

4. REFERENCIAS NORMATIVAS

Norma ISO 9001:2015. Sistema de gestión de la calidad.
Norma ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información

5. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACION

Confidencialidad: La información gestionada por **COBRANZAS ASSETS LTDA** solo debe estar al alcance de las personas o sistemas autorizados para acceder a ella.

Integridad: La información debe ser exacta y completa, para lo cual debe ser protegida de modificaciones o eliminación no autorizadas.

Disponibilidad: La información debe ser accesible cuando personas o sistemas autorizados lo requieran.

6. REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) se sustenta en los siguientes requisitos:

6.1 Compromiso de la dirección

La dirección apoyará a los roles relevantes y dispondrá de los recursos necesarios para la gestión de riesgos e implementación de controles de seguridad de la información.

6.2 Gestión de riesgos

Se administrarán los riesgos en materia de seguridad de la información, vinculados con los procesos incluidos dentro del alcance del SGI y con los sistemas de aplicaciones e infraestructura tecnológica que los soportan. Lo anterior incluye la identificación, evaluación y tratamientos de los riesgos.

6.3 Responsabilidad de colaboradores

Toda información de **COBRANZAS ASSETS LTDA** o confiada por sus clientes deberá ser protegida por todos los colaboradores, contratistas y proveedores con quienes la organización realice negocios y que tengan acceso a la misma.

Los colaboradores deberán tener el cuidado y diligencia que se esperaría de una persona razonablemente prudente al tratar información sensible y deberán informar a través de los canales formales de denuncia interna que establezca la organización cualquier infracción o sospecha de infracción a las políticas y reglas de seguridad de la información.
Asimismo, los colaboradores deben reportar los eventos o incidentes de seguridad de información de los que tengan conocimiento.

6.4 Concientización y capacitación

Se implementarán mecanismos para la concientización y capacitación periódica de los colaboradores de **COBRANZAS ASSETS LTDA**, a fin de que éstos conozcan sus responsabilidades, de acuerdo con los roles desempeñados, así como la importancia del cumplimiento de las leyes, regulaciones, normas, acuerdos, políticas y procedimientos de seguridad de la información.

6.5 Gestión de activos de información

Los activos de información de la organización deberán ser identificados y tener designado un propietario, quien será responsable de su correcta administración durante todo su ciclo de vida. Adicionalmente, podrán designarse custodios de activos, quienes serán responsables de su resguardo. Los activos deben ser protegidos y usados para fines permitidos por la organización.

6.6 Clasificación de la información

La información se clasificará según los criterios establecidos por la organización, atendiendo al grado de confidencialidad y riesgo asociado, a fin de garantizar que se implementen los controles adecuados para su protección.

6.7 Control de accesibilidad

Se establecerán criterios para definir el derecho de acceso a la información, instalaciones, a los sistemas de aplicaciones de apoyo e infraestructura tecnológica por parte de colaboradores, contratistas y proveedores. El acceso se basará en el principio del mínimo derecho de accesibilidad.

6.8 Uso de tecnología autorizada

COBRANZAS ASSETS LTDA sólo se permitirá el uso de programas, aplicaciones y equipos informáticos de la manera y con la finalidad autorizada por la organización.

Los programas o aplicaciones deben estar correctamente licenciados.

6.9 Acuerdos con proveedores

Se exigirá a los proveedores implementar y cumplir las políticas, procedimientos y prácticas de seguridad de la información de **COBRANZAS ASSETS LTDA**, cuando tengan acceso a la misma, garantizando su confidencialidad. Se controlará a los proveedores de servicios a fin de confirmar que cumplan sus obligaciones contractuales en materia de seguridad.

6.10 Gestión de incidentes de seguridad de la información y continuidad

Se establecerán mecanismos para gestionar oportuna y eficientemente incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información administrada por **COBRANZAS ASSETS LTDA**, garantizando la continuidad de los servicios prestados y minimizando sus consecuencias.

6.11 Evaluación, revisión y mejoramiento

El Comité Estratégico Seguridad y Gestión de Riesgos evaluará continuamente el funcionamiento y efectividad del Sistema de Gestión de Seguridad de la información.

Asimismo, **COBRANZAS ASSETS LTDA** diseñará y ejecutará un plan de auditoría interna de seguridad de la información, a fin de verificar que las políticas, procedimientos y controles cumplan con los requisitos aplicables, generando un programa para corregir eventuales no conformidades desde sus causas y para la implementación de acciones de mejora.

Los resultados serán documentados y revisados por la Gerencia General.

6.12 Cumplimiento

Todos los colaboradores de **COBRANZAS ASSETS LTDA** deberán cumplir los requisitos legales, normativos, contractuales y procedimentales aplicables en materia de seguridad de la información.

Cada jefatura velará por el cumplimiento de las políticas y procedimientos de seguridad internos, incorporando en sus procesos los controles necesarios para ello.

Políticas Complementarias de Seguridad de la Información

Para cumplir con los objetivos, principios y requisitos de seguridad de la información, **COBRANZAS ASSETS LTDA** implementará las siguientes políticas complementarias:

Código	Nombre	Objetivo
F-500-001-002	Política integrada de SGC y SGSI	Establecer un marco estratégico que permita a la organización garantizar la calidad de sus productos y servicios, al mismo tiempo que protege la confidencialidad, integridad y disponibilidad de la información.
F-500-001-004	Política General de Ciberseguridad	Establecer los principios fundamentales de Seguridad que aseguren la salvaguarda de la integridad, la confidencialidad y la disponibilidad de sus activos tecnológicos y de la Información generada y utilizada en todos los procesos y operaciones de su negocio.

F-500-001-005	Política de Organización de Seguridad de la Información	Establecer las directrices para configurar la estructura de roles y responsabilidades necesarias para gestionar la seguridad de la información, estableciendo un marco para su implementación, coordinación y control.
F-500-001-006	Política de Transferencia de Información	Establecer lineamientos para garantizar la seguridad de la información que se transfiere dentro de Assets y con cualquier entidad externa a la misma, haciendo uso de cualquier recurso de comunicación.
F-500-001-007	Política de Seguridad para los Servicios en la Nube	Establecer los requisitos de seguridad de la información en los procesos de adquisición, uso, gestión y salida de los servicios en la nube, con el fin de administrar la seguridad de la información en su uso.
F-500-001-008	Política de Control Criptográfico	Establecer reglas para el uso efectivo de la criptografía dentro de Assets, incluyendo la gestión de claves criptográficas para proteger la confidencialidad, la autenticidad o la integridad de la información de acuerdo con los requisitos comerciales y de seguridad de la información. Teniendo en cuenta los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con la criptografía.
F-500-001-009	Política de Amenazas	Establece el marco para la recopilación, análisis y difusión de inteligencia de amenazas, con el objetivo de proteger los activos de información de la organización y minimizar el riesgo de incidentes de seguridad.
F-500-001-010	Política de Seguridad Física y del Entorno	Establecer los controles de acceso físico a las oficinas Assets, para evitar accesos no autorizados, daños o interferencias contra las instalaciones y la información. Igualmente busca proteger el equipamiento para reducir los riesgos ocasionados por

		amenazas y peligros ambientales y oportunidades de acceso no autorizado.
F-500-001-011	Política de Respaldo de la Información	Establecer normas y políticas para el resguardo de la información, para posibilitar la recuperación de ésta en el menor tiempo posible, a través de la restauración del respaldo.
F-500-001-012	Política de Puesto de trabajo despejado y pantalla limpia	Establecer lineamientos y normas generales que regulen la protección y el uso de pantallas y escritorios no supervisados, durante y después de la jornada laboral, entendiendo éstos como pantallas de computador y/o escritorios que permanecen sin uso y sin un colaborador que esté vigilando y ejerciendo supervisión sobre la información que éstos contienen.
F-500-001-013	Política de Privacidad	Identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la de la información de identificación (PII) de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
F-500-001-014	Política de Desarrollo Seguro	Garantizar que la seguridad de la información se incorpore y mantenga en todas las etapas del ciclo de vida del desarrollo de software. Mediante el uso de herramientas y metodologías.
F-500-001-015	Política Gestión de Activos	Establecer las directrices para la gestión de activos que son propiedad de Assets, incluyendo los servicios de cómputo y almacenamiento en la nube, con el fin de controlar los riesgos de seguridad de la información asociados a dichos activos.

F-500-001-016	Política de Dispositivos de Punto Final de Usuario	Establecer las directrices de seguridad para los dispositivos de punto final de usuario, que son propiedad de Assets**,** de tal manera que se encuentre protegida la información almacenada, procesada o accedida a través de dichos dispositivos.
F-500-001-017	Política de Control de Acceso	Establecer las directrices de control de acceso a los activos, controlar el acceso a la información y a la infraestructura de procesamiento de dicha información. Evitar accesos no autorizados, daños o interferencias contra las instalaciones y la información de la compañía o de sus clientes.
F-500-001-018	Política de Teletrabajo	Establecer las directrices para regular el trabajo remoto para los colaboradores y controlar los riesgos de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.
F-601-001-001	Política Comite de SGSI Assets	Establecer la estructura, funciones y responsabilidades del Comité del Sistema de Gestión de Seguridad de la Información con el objetivo de garantizar la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001:2022.

COBRANZAS ASSETS LTDA. reconoce como parte integrante de esta Política General de Seguridad de la Información a las políticas anteriormente mencionadas, así como a todas las normas y procedimientos que se desprendan de éstas.

Adicionalmente, podrán establecerse políticas distintas a las señaladas cuando las circunstancias lo hagan necesario para el adecuado tratamiento de riesgos de seguridad de la información.

7. SANCIONES APLICABLES

El incumplimiento comprobado a la Política General de Seguridad de la Información, demás políticas complementarias o procedimientos por parte de colaboradores de **COBRANZAS ASSETS LTDA**, conllevará la aplicación de las medidas disciplinarias previstas en el Reglamento Interno de Orden, Higiene y Seguridad.
Cuando se trate de terceros, podrá dar lugar al término anticipado del contrato por incumplimiento de obligaciones.

Adicionalmente, **COBRANZAS ASSETS LTDA** se reserva el derecho a iniciar acciones legales a fin de establecer las responsabilidades civiles y penales que hubiere lugar por parte de colaboradores o terceros que incumplan esta política y demás normativas de seguridad de la información.

8. DIFUSIÓN, VIGENCIA DE POLITICA

El Gerente SGI/CISO será responsable de coordinar la difusión de esta política a las partes interesadas, así como su actualización periódica, proponiendo al Comité Estratégico de Seguridad y Gestión de Riesgos los cambios que sean necesarios para su aprobación.

Esta política tendrá vigencia desde la fecha en la que sea oficializada por la Gerencia General, hasta el momento en que se oficialice una nueva versión. Se revisará cada dos años o antes, si circunstancias excepcionales lo justifican, y estará disponible en ISOCheck para todos los miembros de la organización que necesiten leerla. La totalidad de las políticas deben ser informadas a las Jefaturas para que las difundan según el nivel de acceso permitido a cada colaborador.

El mecanismo formal de comunicación es el correo institucional de la Compañía.

9. REVISIONES

REV.	SECCIÓN	SUB-SEC.	*PÁRRAFO*	# SOLICITUD DE CAMBIO	FECHA	AUTORIZADO POR
00	Creación del documento				17-12-2024	Verónica Gajardo Gerente General

Santiago, Chile – Enero 2025

p.p. COBRANZAS ASSETS LTDA.
R.U.T.: 77.049.120-7

GERENTE GENERAL
COBRANZAS ASSETS LIMITADA.