POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN & CIBERSEGURIDAD

Riesgo y Ciberseguridad

Versión 8.2

21 de enero 2026



Cristian Krauss
Oficial de Seguridad de la Información y Ciberdefensa

KLP-SEI-POL-001

Contenido

1. Objetivo 4
2. Alcance 4
3. Definiciones generales 4
4. Actores involucrados 5
5. Directrices y normativas 7
5.1 Principios de Seguridad de la información 7
5.2 Disponibilidad 8
5.3 Directrices de Seguridad de la Información 8
5.4 Objetivos de Seguridad de la información 9
5.5 Tratamiento de la Información 10
5.6 Gestión de Seguridad de la Información 10
5.6.1 Política de Seguridad de los Recursos Humanos 10
5.6.2 Política de Gestión de Activos 10
5.6.3 Política de Control de Acceso 11
5.6.4 Política de Encriptación 11
5.6.5 Política de Seguridad Física y del Ambiente 11
5.7 Política de Seguridad en las Operaciones 12
5.7.1 Política de Seguridad en las Comunicaciones 12
5.7.2 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información 12
5.7.3 Política de Gestión de Proveedores de Servicio 13
5.7.4 Política de Gestión de Incidentes de Seguridad de la Información & Ciberseguridad 13
5.7.5 Política de Continuidad de Negocio 13
5.7.6 Política de Trabajo Remoto y Dispositivos Móviles 13
6. Documentos de referencia 14
7. Regulaciones Externas 16
8. Cumplimiento 17

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

8.1 Mecanismos de seguimiento 17
8.2 Consecuencias del incumplimiento 17
9. Revisión y actualización 18
9.1 Criterios de actualización 18
9.2 Responsable de mantención 18
9.3 Control de cambios 18

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

1. Objetivo

Esta política forma parte integral del Sistema de Gestión de Seguridad de la Información (SGSI) de KLAP, y su contenido está alineado con el alcance, contexto, objetivos y controles establecidos en dicho sistema, conforme a la norma ISO/IEC 27001:2022. Su objetivo es establecer los requisitos de seguridad de la información de KLAP y sus filiales para todos los empleados, contratistas y socios de negocio. El Gobierno Corporativo de KLAP adoptó esta política de seguridad para proteger la información con el fin de alcanzar sus objetivos de negocio y/o el cumplimiento de las leyes o reglamentos aplicables.

Todos los activos de información son propiedad intelectual de KLAP, independientemente de su forma o medio de almacenamiento (digital o impreso). Por lo tanto, el uso de este recurso sólo debe ocurrir dentro de las actividades de negocio que el Gobierno Corporativo de KLAP estime oportuno.

2. Alcance

Esta política es de aplicación obligatoria para todos los colaboradores de KLAP, sin importar el tipo de contrato (indefinido, plazo fijo u honorarios), el área de trabajo o el nivel jerárquico. Asimismo, aplica a personal externo, proveedores de servicios y socios de negocio, remunerados o no, que utilicen, mantengan o tengan acceso privilegiado a activos de información de KLAP o sus filiales.

3. Definiciones generales

Concepto	Definición
Seguridad de la información	Conjunto de prácticas y medidas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información. Esto implica proteger los datos contra accesos no autorizados, alteraciones, pérdidas o daños, tanto en formato digital como físico. Incluye controles técnicos, como el cifrado y las contraseñas; procedimientos organizativos, como políticas y auditorías; y la concienciación del personal para garantizar que la información se maneje de manera segura.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

Información	Conjunto de datos organizados en poder de una entidad que poseen valor para la misma.
Activo de información	Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para KLAP.
Protección de Datos Personales	Conjunto de principios que los responsables y encargados del tratamiento deben considerar al tratar datos personales. Se trata del control de la propia información frente a su tratamiento automatizado o no, es decir, no solo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

4. Actores involucrados

Actor involucrado	Responsabilidad
Directorio	Establecer, implementar, mantener, aprobar y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI). Cumplir con los requisitos legales, regulatorios y contractuales aplicables. Asegurar la confidencialidad, integridad, disponibilidad y resiliencia de la información. Proveer los recursos necesarios para cumplir con los objetivos de seguridad establecidos. Fomentar una cultura de concienciación en seguridad a todos los niveles de la organización.
Oficial de Seguridad de la Información & Ciberseguridad CISO	Asegurar la aplicación efectiva de la presente Política en KLAP. Esto incluye liderar su implementación, coordinar su comunicación interna, supervisar su cumplimiento y proponer actualizaciones cuando existan

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

	Cambios en el entorno de amenazas, normativas, procesos o tecnologías que lo requieran. Velar porque todas las áreas de KLAP comprendan y apliquen los lineamientos establecidos en esta política, así como asesorar a la alta dirección en la toma de decisiones relacionadas con su alcance, excepciones y ajustes. Coordinar las actividades de capacitación, monitoreo y auditoría necesarias para garantizar la efectividad y pertinencia continua de esta política.
Comité de Riesgos Operacionales y Seguridad de la Información (CROSI)	Asegurar la validación, respaldo y alineación estratégica de la presente política, actuando como órgano rector que garantiza su aplicabilidad corporativa y transversal en todo KLAP. Revisar y aprobar las actualizaciones de esta política, velando por su coherencia con los objetivos de negocio, las prioridades de gestión de riesgos, el marco regulatorio aplicable y el entorno tecnológico. Supervisar que la política se mantenga vigente, relevante y efectiva a través del monitoreo de indicadores, revisión de reportes de cumplimiento y resultados de auditorías internas o externas.
Gerencia de Operaciones / Subgerente de Operaciones TI	Aplicación de políticas y procedimientos de seguridad de la información en función de su aplicabilidada todos los activos de información.
Control de Ciberseguridad y Ciberdefensa	Apoyar al Oficial de seguridad de la Información y Ciberseguridad en la definición de controles y asegurar la implementación o despliegue técnico. Dar seguimiento a los planes de acción para mitigar vulnerabilidades.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

	Detectar e informar desviaciones o incumplimientos de los controles Implementar en conjunto a Operaciones TI las herramientas de ciberseguridad. Gestionar a los equipos SOC ante incidentes de seguridad de la información y ciberseguridad. Dar cumplimiento a las políticas de SGSI.
Auditoría Interna	Responsable del Programa de Auditoría del SGSI: planifica y ejecuta auditorías, genera informes y promueve mejoras continuas del SGSI a partir de no conformidades y observaciones encontradas.
Usuarios	Cumplir con lo establecido en esta política actuando de forma diligente, ética y conforme a los principios de confidencialidad, integridad y disponibilidad de la información. Participar en las actividades de capacitación y concienciación definidas por la organización, firmar los compromisos de aceptación cuando corresponda, y colaborar activamente con las medidas de seguridad implementadas, reconociendo que la protección de la información es una responsabilidad compartida.

5. Directrices y normativas

5.1 Principios de Seguridad de la información

El Sistema de Gestión de Seguridad de la Información – SGSI establecerá distintos controles a nivel de gestión, con el objeto de garantizar que los activos de información cumplan con los siguientes principios:

- **Confidencialidad:** Los activos de información se encuentran protegidos de personas/usuarios no autorizados.
- **Integridad:** Los activos de información se encuentran completos, actualizados y son veraces, sin modificaciones inapropiadas o corruptas.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

- **Disponibilidad:** Los usuarios autorizados pueden acceder a los activos de información cuando requiera utilizarlos para desempeñar sus funciones.
- **Licitud, transparencia y lealtad:** Garantizar que los datos son tratados de manera lícita, leal y transparente para el interesado.
- **Limitación de la finalidad:** Garantizar, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines

5.2 Disponibilidad

La política y normativas de seguridad de la información necesitan estar disponibles para el acceso de los colaboradores y protegidas frente a cambios.

La política se encontrará disponible para las partes interesadas según corresponda cada caso. Para el personal interno de KLAP se encuentra comunicada y compartida mediante el SharePoint de la organización (Repositorio KLAP).

La política representa la seguridad y el tratamiento de la información de carácter organizacional y de carácter personal, englobando todo tipo de información sensible y crítica de KLAP y de sus partes interesadas.

5.3 Directrices de Seguridad de la Información

La Organización considera que la información, los sistemas asociados e infraestructura crítica son activos que deben ser protegidos para asegurar el correcto funcionamiento de Klap.

- La Seguridad de la Información en la Organización establece los principales controles, denominados directrices:
- La información de la Organización y de sus clientes se debe tratar de forma ética y sigilosa, de acuerdo con las leyes vigentes y normas internas, evitándose el mal uso y la exposición indebida.
- La información se debe utilizar de forma transparente y solamente para la finalidad para la cual se obtuvo.
- Todo el proceso, durante su ciclo de vida, debe garantizar la segregación de funciones, por medio de la participación de más de un colaborador o equipo de colaboradores.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

- El acceso a la información y recursos sólo aplica en usuarios que se encuentren debidamente autorizados.
- La identificación de cualquier colaborador debe ser única, personal e intransferible, calificándolo como responsable por las acciones realizadas.
- La concesión de accesos debe obedecer el criterio de menor privilegio, en el cual los usuarios tienen acceso solamente a los recursos de información imprescindibles para el pleno desempeño de sus actividades a no ser que la Gerencia General autorice el otorgamiento de privilegios de administrador al usuario por alguna gestión específica.
- Los riesgos asociados a la información de la Organización se deben informar al Oficial de Seguridad de la Información & Ciberseguridad quien lo canalizará al CROSI o a la Alta Dirección para su evaluación y tratamiento.
- Las observaciones derivadas de auditorías, incidentes, nuevas amenazas o sugerencias de usuarios serán consideradas en la revisión de esta política como parte del ciclo de mejora continua del SGSI.
- Las responsabilidades en lo que se refiere a la Seguridad de la Información se deben divulgar ampliamente a los colaboradores, que deben entender y asegurar estas directrices.
- Se debe tener un correcto tratamiento de los riesgos asociados a vulnerabilidades técnicas y actualizaciones de los sistemas.
- Se debe tener el compromiso de satisfacer los requisitos aplicables concernientes a la seguridad de la información.
- Se debe gestionar periódicamente el mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información

5.4 Objetivos de Seguridad de la información

- Asegurar que todos los colaboradores comprendan las expectativas y el compromiso de KLAP con respecto al uso responsable y seguro de los recursos de información.
- Concientizar a las partes interesadas respecto al uso responsable y seguro de los recursos de información.
- Promover el conocimiento de amenazas y buenas prácticas para proteger la seguridad de la información entre los colaboradores.
- Implementar un sistema de gestión de accesos y privilegios para eliminar accesos no autorizados.
- Registrar el 100% de los incidentes de Seguridad de la Información que se materialicen y se reporten por intermedio del SOC

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

5.5 Tratamiento de la Información

Toda información debe recibir una protección adecuada durante todas las etapas de su ciclo de vida, incluyendo su generación, manejo, almacenamiento y desecho. Esta protección debe estar alineada con los principios y directrices de Seguridad de la Información definidos por la organización.

Los contratos establecidos con terceros, proveedores, aliados estratégicos o cualquier parte externa deberán incluir cláusulas específicas que establezcan las responsabilidades y obligaciones legales respecto al uso, protección y confidencialidad de la información proporcionada por la organización. Estos contratos deben contemplar acuerdos de confidencialidad y de transferencia de información, garantizando que no se permita el uso o divulgación no autorizada de la misma.

La organización garantizará la protección de los derechos y libertades de las personas en lo relativo al tratamiento de sus datos personales, desde el mismo momento de su recolección o definición de uso. Toda persona interesada podrá, en cualquier momento, ejercer sus derechos de acceso, rectificación y eliminación de los datos personales que obren en poder de la organización. El tratamiento de estos datos se realizará conforme a los principios establecidos en esta política.

5.6 Gestión de Seguridad de la Información

Para asegurar que la Información tratada esté adecuadamente protegida, la Organización adopta los siguientes procesos:

5.6.1 Política de Seguridad de los Recursos Humanos

El Área de Recursos Humanos deberá establecer y mantener criterios de selección actualizados para los solicitantes (empleados o contratistas) que tienen como objetivo garantizar la veracidad y la honestidad de la información proporcionada, y estos criterios debe respetar y cumplir las normas y leyes vigentes. Además, acuerdos de confidencialidad deben adjuntarse al contrato de trabajo o la prestación de servicios, que debe ser firmado y devuelto a sus representantes legales. Para obtener más información, consulte la Política de Seguridad en Recursos Humanos.

5.6.2 Política de Gestión de Activos

Todos los activos de información de KLAP deben ser clasificados de acuerdo con su nivel de confidencialidad, disponibilidad, integridad y controles legales. Una

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

vez clasificados, se debe establecer la forma en que se accede, almacenan, manipulan y finalmente son eliminados. Todos los activos de información en forma de medios extraíbles deben ser encriptados o si son impresos deben tener su clasificación y claramente visible para que podamos proporcionar el nivel apropiado de tratamiento. Para obtener más información, consulte la Política de Gestión de Activos.

5.6.3 Política de Control de Acceso

Todos los sistemas de información de KLAP deben integrarse en un sistema de control de acceso aprobado por el Área de Tecnología y el Área de Seguridad de la Información & Ciberseguridad. La concesión de acceso (recursos o sistemas) debe ser aprobado por el Oficial de seguridad de la información & ciberseguridad y por el de sistemas. Además de ser instituido la función de segregación en función del nivel o responsabilidad funcional, así como una revisión periódica de la concesión de acceso, con el fin de evitar el acceso no autorizado. Para obtener más información, consulte la política de control de acceso.

Están prohibidos los accesos de carácter administrador a las estaciones de trabajo para todos los usuarios exceptuando aquellos que a modo de excepción cuente con la aprobación o excepciones validadas por el Oficial de Seguridad de la Información & Ciberseguridad.

5.6.4 Política de Encriptación

Toda la Información de KLAP, que necesite ser protegida de un acceso no autorizado o establecido por las regulaciones de cumplimiento internos o externos, debe utilizar criptografía fuerte de acuerdo con las normas aceptadas por el mercado con el fin de garantizar la confidencialidad, autenticidad e integridad de la información.

También todas las claves de cifrado utilizados, deben ser gestionados por un proceso que determina las directrices del ciclo de vida clave y otros aspectos relevantes. Para obtener más información, consulte la Política de cifrado.

5.6.5 Política de Seguridad Física y del Ambiente

Es responsabilidad de sus respectivos dueños proteger los activos de información contra el daño, robo o cualquier evento que pueda generar la falta de disponibilidad de esta.

Es necesario establecer el perímetro de seguridad física con el fin de preservar el acceso sólo a personas autorizadas. También se debe instituir manera obligatoria la identificación funcional de uso (divisa), por lo que es posible para controlar los

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

distintos niveles de acceso para los empleados, contratistas, socios de negocios y visitas. Para obtener más información, consulte la Política de Seguridad Física y del Ambiente.

5.7 Política de Seguridad en las Operaciones

El Área de Tecnología con el apoyo del área de seguridad de la información & Ciberseguridad, debe establecer directrices para garantizar un funcionamiento seguro y adecuado de los recursos y del procesamiento de la información. Para esto es necesario establecer procedimientos operativos documentados y accesibles a los usuarios que los requieran.

Los procedimientos operativos deben incluir, pero no se limitan a, los procedimientos de instalación y los procedimientos de configuración del sistema para el manejo de información, procedimientos de copia de seguridad (backup), los procedimientos para la gestión de pistas de auditoría y procedimientos de evento de monitoreo. Para obtener más información, consulte la Política de Seguridad en las Operaciones.

5.7.1 Política de Seguridad en las Comunicaciones

El área de Tecnología con el apoyo del área de Seguridad de la Información & Ciberseguridad debe establecer directrices para garantizar la protección de la información en las redes y recursos de procesamiento de la información que los apoyan. Para esto es necesario establecer procedimientos operativos documentados y accesibles a los usuarios necesarios y establecer las responsabilidades y procedimientos de la gestión de los equipos de red. Para obtener más información, consulte la Política de Seguridad en las comunicaciones.

5.7.2 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Todos los procesos que implican la adquisición, desarrollo y mantenimiento de sistemas de información, sólo deben ser realizadas por las áreas custodias, con permisos del área de Tecnología y el área de Seguridad de la Información Ciberseguridad. También en cada proceso, se deben realizar de pruebas de seguridad, con el objetivo de asegurar que los riesgos relacionados se conocen y se tratan oportunamente. Para obtener más información, consulte la Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

5.7.3 Política de Gestión de Proveedores de Servicio

Todas las relaciones con los proveedores de servicios deben seguir los lineamientos establecidos de seguridad de la información & Ciberseguridad, con el fin de garantizar la protección de los activos de KLAP, que son accedidos por estos proveedores. También cada relación con los proveedores de servicio debe ser formalizada y aceptada entre las partes. Para todos los efectos se aplicarán las cláusulas de confidencialidad y responsabilidad en el manejo de información. Para obtener más información, consulte la Política de Gestión de Proveedor de Servicios.

5.7.4 Política de Gestión de Incidentes de Seguridad de la Información & Ciberseguridad

Todos los incidentes y eventos de seguridad que afecten a los activos de información de KLAP, se reportan oportunamente al Área de Seguridad de la Información. Es responsabilidad del área de Seguridad de la Información & Ciberseguridad, coordinar todas las actividades relacionadas con el proceso de gestión de incidentes de seguridad de la información & Ciberseguridad. Es deber de todos los usuarios, informar un incidente relacionado con seguridad de información & Ciberseguridad y comunicar al área responsable. Para obtener más información, consulte la Política General de Gestión de Incidentes.

5.7.5 Política de Continuidad de Negocio

El proceso de gestión de la continuidad del negocio debe ser implementado con el fin de reducir el impacto sobre el negocio de KLAP y sus filiales. Es responsabilidad del gerente de la unidad de negocios para estos efectos, solicitar la conducción del área de Tecnología y el apoyo de ésta, en la generación y ejecución de planes de continuidad de negocio. Para obtener más información, consulte la Política de Continuidad de Negocio.

5.7.6 Política de Trabajo Remoto y Dispositivos Móviles

El área de Tecnología y de Recursos Humanos con el apoyo del área de Seguridad de la Información & Ciberseguridad, establecerá directrices para garantizar la seguridad de la información en el teletrabajo y el uso de dispositivos móviles en KLAP y sus filiales. Para ello debe establecer una política formal y asequible con las condiciones y restricciones.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

Esta política debe incluir, pero no se limitan a, los procedimientos de registro de los dispositivos móviles, la seguridad física, la instalación del software, el acceso a información clasificada, control de acceso, la desactivación o de bloqueo y copias de seguridad remotas. Para obtener más información, consulte la Política de trabajo remoto y dispositivos móviles

6. Documentos de referencia

Nombre del documento	Contenido
Política de Seguridad de los Recursos Humanos	Establece los requisitos de seguridad con respecto al ciclo de colaborador en KLAP, desde la selección, concientización, uso responsable de los activos asignados entre otros.
Política de Gestión de Activos	Establece los requisitos a nivel de seguridad de la información con respecto a la gestión de activo al momento de adquirir un activo en la organización, su tratamiento y uso adecuado con el fin de resguardar la confidencialidad, integridad y disponibilidad de los datos.
Política de Control de Acceso	Establece los requisitos de seguridad de la información y ciberseguridad para: identificar los activos de KLAP y sus filiales y definir las responsabilidades adecuadas para la protección de éstos, para que la información reciba un nivel adecuado de protección de acuerdo con su importancia para KLAP en base a la CIA de información.
Política de Encriptación	Establece los requisitos para el uso de la encriptación en KLAP y sus filiales para todos los empleados, contratistas, proveedores y socios de negocio. El Gobierno Corporativo de KLAP adoptó esta política de seguridad para garantizar que las funciones de cifrado se utilizan adecuadamente para proteger la

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

	confidencialidad, disponibilidad y integridad de la información.
Política de Seguridad Física y del Ambiente.	Establece los requisitos de seguridad de la información con el fin de proteger los accesos no autorizados a zonas críticas de la organización, tales como; datacenter, oficinas de operaciones TI, áreas de configuración de POS, entre otros.
Política de Seguridad en las Operaciones	Establece los requisitos de seguridad de la información con el cual deben operar los sistemas. Mantener siempre configuraciones robustas y seguras a nivel de sistemas operativos, configuración de reloj, respaldos entre otras.
Política de Seguridad en las Comunicaciones	Establece los requisitos de seguridad de la información con respecto a los canales de comunicación y sus niveles de cifrados para resguardar la integridad y disponibilidad de la información.
Política de Seguridad en la clasificación y manejo de la información	Garantizar que toda la información de la organización se identifique, clasifique y gestione de forma coherente con su nivel de sensibilidad, asegurando su confidencialidad, integridad y disponibilidad.
Política de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información	Establece los requisitos de seguridad de la información para la adquisición de nuevos productos que dan soporte a la operación. Ya sean desarrollos realizados por la organización o externos.
Política de Gestión de Proveedores de Servicio	Establece los requisitos de seguridad de la información para poder gestionar a los proveedores que prestan servicios a KLAP.
Política de Gestión de Incidentes de Seguridad de la Información & Ciberseguridad	Establece los requisitos de seguridad de la información para atender los incidentes según las definiciones de los eventos nivel 1 2 y 3, además establece las acciones que

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

	se deben realizar para realizar la gestión, desde la notificación de un evento hasta el cierre del evento.
Política de Continuidad del Negocio	Garantizar que la organización pueda mantener o restablecer rápidamente sus operaciones críticas ante interrupciones, minimizando el impacto en clientes, colaboradores y resultados.
Política de Trabajo Remoto y Dispositivos Móviles	Establece los alineamientos para garantizar un trabajo remoto y de dispositivos Móviles de forma segura.
Programa de Concientización de Seguridad y uso aceptable.	Conjunto estructurado de actividades y recursos diseñados para que todos los colaboradores comprendan los riesgos de seguridad de la información y ciberseguridad, adopten comportamientos seguros y conozcan sus responsabilidades en la protección de la información de la organización.
Matrices de Riesgo de Seguridad de la Información.	Herramienta visual que combina la probabilidad de ocurrencia de un evento con el impacto que tendría, permitiendo clasificar los riesgos en niveles (por ejemplo, bajo, medio, alto o critico) para priorizar acciones de mitigación.

7. Regulaciones Externas

Nombre del documento	Contenido
PCI-DSS V3.2.1	PCI-DSS V3.2.1 estándar de seguridad para proteger la información de tarjetas de pago. A nivel de confidencialidad de los datos sensibles del tarjetahabiente.
PCI-DSS V4.0.1	PCI-DSS V4.0.1 estándar de seguridad para proteger la información de tarjetas

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

	de pago. A nivel de confidencialidad de los datos sensibles del tarjetahabiente.
ISO/IEC 27001:2022	Norma internacional que proporciona una guía de buenas prácticas para implementar los controles de seguridad de la información.
PCI-PIN SECURITY V3.1	Estándar de seguridad que se enfoca en proteger la información de los números de identificación personal (PIN) durante las transacciones de pago.

8. Cumplimiento

8.1 Mecanismos de seguimiento

El cumplimiento de la política de seguridad de la información y ciberseguridad se llevará a cabo mediante la definición y seguimiento de Indicadores Clave de Rendimiento (KPI) establecidos por el Oficial de Seguridad de la Información y Ciberseguridad.

8.2 Consecuencias del incumplimiento

Cualquier violación de la presente Política puede resultar en la toma de las acciones disciplinarias correspondientes de acuerdo con el Reglamento interno KLAP. Es responsabilidad de todos los colaboradores del KLAP notificar al Oficial de Seguridad de la Información y Ciberseguridad cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política.

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

9. Revisión y actualización

9.1 Criterios de actualización

La presente política, así como sus versiones futuras, deberá ser comunicada de manera oportuna a todas las áreas y al personal de KLAP a través de medios accesibles, confiables y eficaces. Se deberá asegurar su correcta recepción, comprensión y cumplimiento, conforme a lo establecido en el punto 5 del presente documento.

Esta política deberá revisarse, como mínimo, una vez al año o cuando se produzcan cambios significativos en el entorno de negocios, la estructura organizacional o por cualquier otro motivo que lo justifique. La revisión será responsabilidad del Comité de Riesgos Operacionales y Seguridad de la Información (CROSI), y deberá contar con la aprobación formal de la Alta Dirección.

9.2 Responsable de mantención

Responsable de Mantención	Oficial de Seguridad de la Información y Ciberdefensa
Periodicidad	12 meses y/o bajo demanda
Clasificación de la Información	Público
Fecha de Aprobación	12-01-2026

9.3 Control de cambios

Versión	Fecha	Tipo de Cambio	Descripción de la modificación	Autor
1.0	13-09-2016	Creación	Creación del documento	Sandra Ferrada
2.0	30-09-2016	Mayor	Versión Actualizada	Sandra Ferrada
2.1	29-12-2017	Menor	Versión Actualizada	Sandra Ferrada
2.2	27-12-2018	Menor	Versión Actualizada	Sandra Ferrada

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

3.0	31-07-2019	Mayor	Versión Actualizada	Sandra Ferrada
3.1	03-09-2020	Menor	Versión Ratificada	Sandra Ferrada
4.0	01-03-2021	Mayor	Versión Actualizada	Gabriel Gonzalez
5.0	19-01-2022	Mayor	Versión Actualizada	Felipe Miranda
6.0	28-02-2023	Mayor	Versión Actualizada	Felipe Miranda
7.0	02-01-2024	Mayor	Versión Actualizada	Felipe Miranda
7.1	25-02-2025	Menor	Versión Actualizada	Cristian Krauss
8.0	25-09-2025	Mayor	Versión Actualizada con: - Cumplimiento del SGSI - Se agregan los roles y responsabilidades de forma detallada. Se agregan columnas en historial de versiones tales como fecha de aprobación.	Cristian Krauss
8.1	20-11-2025	Mayor	- Cambio de Formato Versión Actualizada	Cristian Krauss
8.2	12-01-2026	Menor	- Actualización Objetivos del SGSI	Cristian Krauss

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*

APROBADORES

VERSIÓN 8.2

Raúl Sapunar
Gerencia General
Gerente General

Raúl Sapunar K. (22 ene.. 2026 11:47:23 GMT-3)
Firma

Rafael Osorio
Operaciones & Tecnología
Gerente

Rafael Osorio P. (22 ene.. 2026 11:58:57 GMT-3)
Firma

Sandra Ferrada
Riesgo & Ciberseguridad
Gerente

Sandra Ferrada (22 ene.. 2026 11:13:45 GMT-3)
Firma

Leon Paul
Administración & Finanzas
Gerente

Leon Paul C. (21 ene.. 2026 19:00:18 GMT-3)
Firma

Patricio Martinez
Personas
Gerente

Patricio M. (22 ene.. 2026 10:53:10 GMT-3)
Firma

Validado por
Catalina Valdés
Jefa de Procesos

CValdésR. - (22 ene.. 2026 10:54:44 GMT-3)
Firma

*Este documento se almacena de forma centralizada. Cualquier reproducción total o parcial del mismo se considerará una "**Copia no Controlada**".*