Código: POL-01 Nombre: Política integral de seguridad de la información Versión: 1.0	Aprobado por: Gerencia de S.I Fecha: 02/12/2025

Tabla de contenido

1. OBJETIVO....2
2. ALCANCE....2
3. MARCO NORMATIVO APLICABLE....2
4. ROLES Y RESPONSABILIDADES....3
5. CLASIFICACIÓN DE LA INFORMACIÓN....4
6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN....5
7. GESTIÒN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÒN....5
8. PROTECCIÒN DE DATOS DE TARJETA DE CRÈDITO....6
9. PROTECCIÒN DE DATOS PERSONALES....7
10. CONTROL DE ACCESOS A LA INFORMACIÓN....7
11. REGISTRO MONITOREO Y TRAZABILIDAD....7
12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....8
13. CAPACITACIÓN Y CONCIENCIACIÓN....8
14. GESTIÓN DE TERCEROS Y PROVEEDORES....8
15. CONTINUIDAD DEL NEGOCIO....8
16. CUMPLIMIENTO, SANCIONES Y MEDIDAS DISCIPLINARIAS....8
17. REVISIÓN Y ACTUALIZACIÓN....9

Código: POL-01 Nombre: Política integral de seguridad de la información Versión: 1.0	Aprobado por: Gerencia de S.I Fecha: 02/12/2025

1. OBJETIVO

Definir los principios y directrices para la protección de la información de la organización, con el fin de preservar su confidencialidad, integridad y disponibilidad, gestionar de manera efectiva los riesgos asociados a la seguridad de la información y cumplir con los requisitos legales, regulatorios y técnicos vigentes.

2. ALCANCE

Esta política es de obligatorio cumplimiento para todos los colaboradores, contratistas y terceros que, directa o indirectamente, tengan acceso a información de la organización o participen en su procesamiento, almacenamiento o transmisión. Aplica a todos los procesos del negocio, plataformas tecnológicas, sistemas de información y activos relacionados con el tratamiento de datos de tarjetas de crédito y datos personales.

3. MARCO NORMATIVO APLICABLE.

La gestión de la seguridad de la información en la organización se rige por el cumplimiento obligatorio del estándar PCI DSS para la protección de datos de tarjetas de crédito y de la normativa colombiana vigente aplicable.

De manera complementaria, la organización toma como referencia las mejores prácticas establecidas en las normas y estándares de seguridad y ciberseguridad, con el fin de fortalecer la gestión de riesgos y los controles de seguridad de la información.

En caso de existir discrepancias entre los marcos de referencia, prevalecerán los requisitos obligatorios del estándar PCI DSS y de la legislación colombiana aplicable.

- **PCI DSS**: Estándar de cumplimiento obligatorio para la protección de datos de tarjetas de crédito, que define controles mínimos de seguridad.

- **ISO/IEC 27001 e ISO/IEC 27002**: Norma que establece los requisitos y controles para implementar y mantener un sistema de gestión de seguridad de la información basado en riesgos.

- **ISO 31000**: Norma que proporciona principios y directrices para la gestión integral de riesgos en las organizaciones.

- **ISO/IEC 27005**: Marco específico para la gestión del riesgo de seguridad de la información, complementario a ISO/IEC 27001.

- **ISO/IEC 27035**: Norma que define las buenas prácticas para la gestión y respuesta a incidentes de seguridad de la información.

- **NIST SP 800-61**: Guía técnica que orienta la preparación y respuesta ante incidentes de seguridad informática.

- **Ley 1581 de 2012**: Régimen general colombiano para la protección de datos personales y los derechos de los titulares de la información.

- **Habeas Data**: Principio constitucional que garantiza el derecho de las personas a conocer, actualizar y proteger su información personal.

- **Circular Externa 052 de la Superintendencia Financiera de Colombia**: Lineamientos en ciberseguridad, gestión del riesgo operativo y continuidad del negocio aplicables a organizaciones que interactúan con el sector financiero.

4. ROLES Y RESPONSABILIDADES

La organización definirá, documentará y mantendrá los roles y responsabilidades en materia de seguridad de la información con el fin de asegurar la correcta implementación, operación, supervisión y mejora continua de los controles de seguridad, en concordancia con los requisitos legales, regulatorios y técnicos aplicables.

Los roles, responsabilidades se encuentran formalmente establecidos en la **MAT-02 – Matriz RACI de Seguridad de la Información**, la cual define la participación de la Alta Dirección, el Responsable de Seguridad de la Información (CISO), el área de Tecnología

/ Seguridad, los dueños de la información, los colaboradores y los terceros, para cada uno de los procesos y actividades de seguridad de la información.

Las responsabilidades asignadas son de obligatorio cumplimiento para todas las partes involucradas. **(PCI DSS v4.0.1: Req. 12.1, 12.5 | ISO/IEC 27001:2022: 5.3 | ISO/IEC 27002:2022: 5.2, 5.3).**

5. CLASIFICACIÓN DE LA INFORMACIÓN

La información de la organización deberá ser clasificada teniendo en cuenta su nivel de sensibilidad, el impacto que su divulgación, alteración o pérdida pueda generar sobre la organización y los requisitos legales o regulatorios aplicables. Para efectos de esta política, la información se clasificará en las siguientes categorías:

- **Información pública:** Información cuyo acceso no genera riesgos para la organización y puede ser divulgada sin restricciones.
- **Información de uso interno:** Información destinada al uso interno de la organización, cuya divulgación no autorizada puede generar afectaciones operativas moderadas.
- **Información confidencial:** Información cuyo acceso, uso o divulgación no autorizada puede generar impactos significativos sobre la organización, los clientes o los procesos del negocio.
- **Información sensible:** Información crítica sujeta a requisitos legales o regulatorios estrictos, incluyendo datos de tarjetas de crédito y datos personales, cuya exposición no autorizada puede generar impactos legales, financieros o reputacionales graves.

Los dueños de la información serán responsables de asignar la clasificación correspondiente y de asegurar que se apliquen los controles de seguridad acordes con la clasificación definida. **(PCI DSS v4.0.1: Req. 3 | ISO/IEC 27001:2022: 5.12, 5.13 | ISO/IEC 27002:2022: 5.12, 5.13 | Ley 1581 de 2012).**

6. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La organización orienta su gestión de seguridad de la información bajo los siguientes principios:

- **Confidencialidad, integridad y disponibilidad:** La información debe ser protegida de accesos no autorizados, alteraciones indebidas y pérdidas.

- **Cultura de responsabilidad compartida:** La seguridad de la información es responsabilidad de todos los usuarios que tengan acceso a los activos de información.

- **Prevención del riesgo:** La organización prioriza la gestión de riesgos de seguridad de la información de manera preventiva, reduciendo la probabilidad y el impacto de incidentes.

- **Cumplimiento regulatorio:** La gestión de la seguridad de la información se desarrolla en concordancia con las normas, leyes y regulaciones aplicables.

- **Mínimo privilegio y necesidad de conocer:** Accesos limitados a lo estrictamente necesario.

- **Trazabilidad:** Las actividades relacionadas con el acceso y uso de la información deben ser registradas y monitoreadas, permitiendo su seguimiento y auditoría.

- **Mejora continua:** La organización promueve la revisión y el fortalecimiento permanente de sus prácticas de seguridad de la información, en respuesta a cambios en el entorno, en los riesgos y en los requisitos normativos.

7. GESTIÒN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÒN.

La organización establecerá y mantendrá un proceso documentado de gestión de riesgos de seguridad de la información. Dicho proceso será revisado al menos una vez al

año, así como cuando se presenten cambios significativos en el entorno, los procesos o las tecnologías.

El análisis de riesgos considerará amenazas, vulnerabilidades, probabilidad e impacto, priorizando aquellos riesgos asociados a activos críticos, al entorno de datos de tarjetas (CDE) y al tratamiento de datos personales.

Los controles definidos como resultado de la gestión de riesgos serán implementados de manera proporcional al nivel de riesgo identificado y deberán contar con la aprobación de la Alta Dirección cuando implique la aceptación de riesgos residuales significativos. **(PCI DSS v4.0.1: Req. 12.3.1, 12.3.2 | ISO/IEC 27001:2022: 6.1 | ISO/IEC 27002:2022: 5.4 | ISO 31000 | ISO/IEC 27005).**

8. PROTECCIÒN DE DATOS DE TARJETA DE CRÈDITO

La organización protegerá los datos de tarjetas de crédito durante todo su ciclo de vida, garantizando que su procesamiento, almacenamiento y transmisión se realicen únicamente cuando sea necesario para la operación del negocio.

Se prohíbe expresamente el almacenamiento de datos sensibles de autenticación después de la autorización, tales como códigos de validación, datos de banda magnética u otra información equivalente.

La transmisión del PAN y de cualquier dato sensible deberá realizarse exclusivamente mediante cifrado fuerte, utilizando protocolos seguros y actualizados. Asimismo, se implementarán controles que prevengan la intercepción, alteración o divulgación no autorizada de la información en tránsito.

El PAN almacenado deberá estar protegido mediante cifrado fuerte, tokenización o truncamiento, y su acceso estará restringido estrictamente por necesidad de negocio. La organización establecerá mecanismos para la gestión y protección de las claves criptográficas, así como controles que eviten la exposición no autorizada de los datos almacenados.**(PCI DSS v4.0.1: Req. 3, Req. 4 | ISO/IEC 27002:2022: 8.24, 8.25, 8.26).**

9. PROTECCIÒN DE DATOS PERSONALES

El tratamiento de los datos personales se realizará conforme a la Ley 1581 de 2012 y demás disposiciones aplicables, respetando los derechos de los titulares.

La organización adoptará medidas administrativas, técnicas y organizativas proporcionales al nivel de riesgo, orientadas a prevenir accesos no autorizados, pérdida, alteración o uso indebido de los datos personales. **(ISO/IEC 27002:2022: 5.34 | Ley 1581 de 2012 | Habeas Data).**

10. CONTROL DE ACCESOS A LA INFORMACIÓN

El acceso a la información y a los sistemas se otorgará de acuerdo con las funciones del usuario, aplicando los principios de mínimo privilegio y necesidad de conocer.

Cada usuario contará con una identidad única, y sus accesos serán gestionados a lo largo de todo su ciclo de vida, incluyendo su creación, modificación y revocación oportuna cuando se presenten cambios en funciones, traslados, finalización de contratos u otras situaciones que lo requieran.Los accesos privilegiados estarán sujetos a controles adicionales, acordes con el nivel de riesgo asociado.

Los accesos otorgados serán revisados como mínimo semestralmente, o cuando se presenten cambios relevantes en las responsabilidades del usuario. **(PCI DSS v4.0.1: Req. 7, Req. 8 | ISO/IEC 27002:2022: 5.15, 5.16, 5.18, 8.2).**

11. REGISTRO MONITOREO Y TRAZABILIDAD

La organización implementará mecanismos de registro y monitoreo sobre sistemas y datos críticos.

Los registros de auditoría deberán permitir identificar, como mínimo, el usuario, la fecha y hora, el origen del evento y la acción realizada, y estarán protegidos contra accesos no autorizados, alteraciones o eliminación indebida. Estos registros se conservarán por un período mínimo de doce (12) meses, garantizando que al menos los últimos tres (3) meses estén disponibles de forma inmediata para análisis, monitoreo y atención de incidentes de seguridad.**(PCI DSS v4.0.1: Req. 10.2, 10.4, 10.5, 10.7 | ISO/IEC 27002:2022: 8.15).**

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La organización contará con un proceso formal y documentado para la detección, reporte, análisis, respuesta y recuperación ante incidentes de seguridad de la información. **(PCI DSS v4.0.1: Req. 12.10 | ISO/IEC 27035 | ISO/IEC 27002:2022: 5.24, 5.25 | NIST SP 800-61).**

13. CAPACITACIÓN Y CONCIENCIACIÓN

Todos los colaboradores y terceros relevantes deberán recibir al menos una vez al año capacitación y actividades de concienciación en seguridad de la información, protección de datos personales y manejo seguro de datos de tarjetas de crédito, de acuerdo con sus responsabilidades. **(PCI DSS v4.0.1: Req. 12.6 | ISO/IEC 27001:2022: 7.2 | ISO/IEC 27002:2022: 6.3).**

14. GESTIÓN DE TERCEROS Y PROVEEDORES

Los terceros que tengan acceso a datos de tarjetas de crédito o a información sensible deberán cumplir con los requisitos de seguridad establecidos por la organización, los cuales serán formalizados mediante acuerdos contractuales.

La evaluación y seguimiento a terceros se realizará de forma periódica y proporcional al nivel de riesgo que represente la relación contractual. **(PCI DSS v4.0.1: Req. 12.8 | ISO/IEC 27001:2022: 8.1 | ISO/IEC 27002:2022: 5.19).**

15. CONTINUIDAD DEL NEGOCIO

La organización adoptará medidas para garantizar la continuidad de los procesos críticos y la recuperación oportuna ante eventos que afecten la seguridad de la información y la operación del negocio, considerando el impacto y la criticidad de los servicios. **(PCI DSS v4.0.1: Req. 12.10.1 | ISO/IEC 27002:2022: 5.30 | Circular 052 SFC).**

16. CUMPLIMIENTO, SANCIONES Y MEDIDAS DISCIPLINARIAS.

El cumplimiento de la presente política será verificado mediante auditorías, revisiones y mecanismos de seguimiento.

El incumplimiento podrá dar lugar a sanciones disciplinarias, contractuales o legales, considerando la gravedad del evento y el impacto sobre la seguridad de la información. **(PCI DSS v4.0.1: Req. 12.5 | ISO/IEC 27001:2022: 9.1 | Ley 1581 | Circular 052 SFC).**

17. REVISIÓN Y ACTUALIZACIÓN

La presente política será revisada al menos una vez al año, o cuando se presenten cambios relevantes en los riesgos, la infraestructura tecnológica, los procesos del negocio o la normativa aplicable, asegurando su vigencia y efectividad. **(PCI DSS v4.0.1: Req. 12.1.1 | ISO/IEC 27001:2022: 10.2).**