VISIONAMOS
sistema de pago cooperativo

POLÍTICA SISTEMA DE GESTIÒN INTEGRADO

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
YCIBERSEGURIDAD

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

VISIONAMOS SISTEMA DE PAGO COOPERATIVO está comprometida con la generación de valor y su sostenibilidad. Para lograr este fin, la gestión Calidad, Riesgos, Auditoría Interna, Seguridad de la Información y Ciberseguridad son pilares fundamentales para los procesos y hace parte de la actuación de los colaboradores de la Entidad.

El propósito es prevenir, detectar y evaluar de forma ágil y proactiva los impactos favorables y desfavorables que pueden afectar el logro de los objetivos estratégicos y por ende el desempeño organizacional.

De esta manera el Sistema de Gestión Integrado (SGI) administrar los procesos, los riesgos, los activos de información y el cumplimiento de controles, previniendo y mitigando la materialización de eventos adversos; así mismo construyendo una cultura proactiva de conciencia y autocontrol.

2. OBJETIVO.

Establecer los elementos y el marco general de actuación para el Sistema de Gestión Integrado, el cual busca promover y asegurar el cumplimiento de los objetivos estratégicos, tácticos y operativos.

3. POLÍTICA DEL SISTEMA DE GESTIÓN INTEGRADO.

Somos una Administradora de Sistemas de Pago Bajo Valor de naturaleza cooperativa y solidario que presta servicios de compensación y liquidación, que busca ser un referente por su innovación, seguridad y agilidad en la prestación de sus servicios, generando valor y satisfacción a las partes interesadas siendo coherente con sus criterios de actuación y su direccionamiento estratégico, basados en la gestión por procesos, la gestión de riesgos, la protección de los activos de información a través del aseguramiento de la confidencialidad, integridad y disponibilidad de la información, el cumplimiento y compromiso de normas, regulaciones y requisitos aplicables a Seguridad de la Información, Ciberseguridad y Calidad, contando con canales de comunicación idóneos, eficientes y seguros con las partes interesadas; y el compromiso de aplicar la mejora continua, asegurando su viabilidad y sostenibilidad en el tiempo.

4. OBJETIVOS DEL SISTEMA DE GESTIÓN INTEGRADO

OBJETIVO	PROCESO/SISTEMA	INDICADOR	EVALUACIÓN
Asegurar que los activos de información están adecuadamente protegidos.	Sistema de Seguridad de la información y Ciberseguridad	• Actualización Control Anti Malware • Equipos Infectados en la entidad • Mitigación de vulnerabilidades • Cierre de incidentes • Ataques recibidos en los Firewalls	Se tiene programada la evaluación de este objetivo de manera mensual
Establecer controles (Políticas, procedimientos u otros) para la protección de la información ante los eventos que puedan resultar en divulgación o alteración indebida de la información,	Sistema de Seguridad de la información y Ciberseguridad	• Casos Gestionados en la Mesa de Ayuda. • Cierre de incidentes • Intento de Fraudes registrado por las entidades.	Se tiene programada la evaluación de este objetivo de manera mensual
Garantizar el cumplimiento de los requisitos legales y normativos aplicados a la actividad economía de la Entidad respecto a: respecto a calidad, seguridad, ciberseguridad y riesgos	Gestión Jurídica /Todos los procesos	S-GJ-F-01 Matriz de requisitos legales-01.	Se revisara de manera Anual, o en los casos que se requiera.
Capacitar y sensibilizar al personal en temas relacionados con el Sistema de Gestión Integrado,	Sistema de Gestión Integrado	• Curso interno para los colaboradores • Curso externo para las Entidades	Se tiene programado una evaluación anual.

OBJETIVO	PROCESO/SISTEMA	INDICADOR	EVALUACIÓN
Desarrollar y controla eficazmente los proceso y servicios que satisfagan las expectativas de las Entidades.	Gestión de Operaciones	• Encuesta de satisfacción a la Entidades/Clientes	Se tiene programado una encuesta de satisfacción anual
Mejorar la eficacia de los Procesos de la Organización, con la participación de todos los colaboradores.	Auditoria	• Total, de acciones de mejora(oportunidad de mejora)/total de acciones tomado de las solicitudes de planes de acción.	Se mide de manera Trimestral
Controlar los procesos a través del cumplimiento de indicadores de gestión	Gestión de Calidad	• Matriz de indicadores	Se miden según periodicidad de los indicadores de cada procesos (Caracterizaciones de procesos)
Alcanzar una rentabilidad financiera que le de sostenibilidad a largo plazo a la organización.	Gestión Financiera	• Indicador de activos • Indicador de patrimonio	Se mide de manera trimestral

5. RESPONSABILIDADES.

Las responsabilidades frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad se encuentran documentadas en el manual S-SI-M-03-Sistema de gestión de seguridad de la información y Ciberseguridad y DCSI-0003 Gestión de la Ciberseguridad.

6. FUNCIONES.

Las funciones frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad son definidas y administradas bajo el procedimiento T-AP-P-01-Selección de personal.

7. PRINCIPIOS Y LINEAMIENTOS.

7.1. GENERALES.

- ✓ Promover la cultura y gestión en temas de ciberseguridad que involucre actividades relacionadas con la prevención de posibles eventos o acciones que puedan afectar o influir en los procesos internos o externos de VISIONAMOS.
- ✓ Contar con lineamientos asociados a la gestión de ciberseguridad, que permitan. prevenir posibles afectaciones, a través de los diferentes medios.
- ✓ Informar al Consejo de Administración, así como a la Alta Gerencia, a través del Comité de Riesgo y/o Comité de Seguridad de la Información y Ciberseguridad, con la periodicidad que éste considere; cualquier tema relacionado a ciberseguridad, especialmente, en la identificación de ciber-amenazas, resultados de la evaluación, propuestas de mejora en materia de ciberseguridad, resumen de los incidentes de ciberseguridad, que hayan afectado de alguna manera el funcionamiento de la entidad, así como orientar sobre esta materia.
- ✓ Contar con la Estructura necesaria, que se encargue o realice la gestión, relacionada a temas de ciberseguridad, y que la misma cuente con los mecanismos y recursos necesarios para sus funciones.
- ✓ Considerar en los contratos que se celebren con terceros, las medidas y consideraciones pertinentes que permitan prevenir y/o mitigar que la entidad se vea afectada por temas de ciberseguridad y seguridad de la información.
- ✓ Gestionar la seguridad de la información y ciberseguridad en cualquier iniciativa que involucre cambios tecnológicos.

7.2. GESTIÓN DE PREVENCIÓN.

- ✓ Establecer, documentar y brindar seguimiento a los controles de entrada y salida de información y gestión de identidades, bajo la premisa que las personas solo pueden disponer de los recursos que demande sus funciones, durante el tiempo que ello sea necesario o por duración de sus servicios en la Entidad.
- ✓ Los colaboradores de VISIONAMOS deberán procurar el cumplimiento y aplicación de los lineamientos descritos en la presente política con lo cual se mitiga o se previene cualquier proceso de vulnerabilidad que afecte su gestión.
- ✓ Identificar e informar, en la medida de lo posible, una vez detectados, cualquier riesgo cibernético emergente que pueda llegar a afectar al Grupo Bancario.
- ✓ Considerar dentro de los Planes de Continuidad y Contingencia del Negocio, la respuesta y recuperación oportuna de la Entidad frente a ataques cibernéticos
- ✓ El proceso de Auditoría de deberá incluir dentro de sus procesos, la evaluación periódica de los procesos relacionados a ciberseguridad.
- ✓ Incluir en los planes de Continuidad del Negocio pruebas (de intrusión o de cualquier otra que consideren), que simulen la materialización de posibles ataques.
- ✓ Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.
- ✓ De acuerdo con la estructura, canales de atención, volumen transaccional y número de Entidades Participantes, monitorear diferentes fuentes de información; tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la Entidad.
- ✓ Informar periódicamente a las Entidades Participantes, sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

7.3. PROTECCIÓN Y DETECCIÓN.

La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos, considerando:

- ✓ Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.
- ✓ Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
- ✓ Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar posibles ciberataques contra VISIONAMOS.

1. NOVEDADES Y ACTUALIZACIONES			
FECHA	**NATURALEZA DEL CAMBIO**	**ELABORÓ (Nombre/Cargo)**	**REVISÓ Y APROBÓ (Nombre/Cargo)**
29-SEP-2022	Creación de la política (Req 27)	Yessica Taborda /Analista de Procesos Cristian Villada /Analista de Seguridad de la Información	Consejo de Administración (Acta 261)