POLÍTICA DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

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 compromiso para satisfacer los requisitos, normas y regulaciones aplicables relacionados con la seguridad de la información, Ciberseguridad y Protección de la privacidad, 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.

OBJETIVOS DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

ITEM	OBJETIVO	PROCESO/SISTEMA
1	Asegurar que los activos de información están adecuadamente protegidos.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad
2	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 Gestión de Seguridad de la Información y Ciberseguridad
3	Garantizar el cumplimiento de los requisitos legales y normativos aplicados a la actividad económica de la Entidad respecto a Calidad, Seguridad, Ciberseguridad y Riesgos.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad Sistema de Gestión de la Calidad Todos los procesos
4	Capacitar y sensibilizar al personal en temas relacionados con el Sistema de Gestión Seguridad de la Información.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad Gestión de Personas
5	Mejorar la eficacia de los Procesos de la Organización, con la participación de todos los colaboradores.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad Sistema de Control Interno
6	Gestionar los riesgos de Seguridad de la Información y Ciberseguridad por medio de la identificación, valoración y tratamiento.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad Sistema de Gestión de Riesgos
7	Gestionar las debilidades, eventos e incidentes de Seguridad de la Información y Ciberseguridad.	Sistema de Gestión de Seguridad de la Información y Ciberseguridad Gestión Tecnológica

RESPONSABILIDADES

Las responsabilidades frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad se encuentran en el numeral 6.1.1 del Manual del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

COMPETENCIAS

Las competencias frente al Sistema de Gestión de Seguridad de la Información y Ciberseguridad son definidas y administradas bajo el Formato Descripción y Perfil del Cargo.

PRINCIPIOS Y LINEAMIENTOS 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 la Ciberseguridad que permitan prevenir posibles afectaciones en la continuidad del negocio y tener una respuesta eficaz a incidentes de seguridad.

- 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, con la periodicidad que éste considere; cualquier tema relacionado a Seguridad de la Información y Ciberseguridad, especialmente, en la identificación de Ciberamenazas, resultados de la evaluación de los riesgos, propuestas de mejora continua, resumen de los incidentes de Seguridad de la Información y Ciberseguridad que hayan afectado de alguna manera la prestación de los servicios de la entidad.

- Contar con una estructura definida para realizar la Gestión de Seguridad de la Información y Ciberseguridad, que cuente con los mecanismos y recursos necesarios para su funcionamiento.

- Considerar en los contratos que se celebren con terceros las medidas y consideraciones pertinentes que permitan prevenir y/o mitigar afectaciones por la materialización de riesgos.

- Gestionar la Seguridad de la Información y Ciberseguridad en cualquier iniciativa que involucre cambios tecnológicos.

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 deben 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 a las Entidades Participante de la red.
- Considerar dentro de los Planes de Continuidad de Negocio la respuesta y recuperación oportuna de la Entidad frente a ataques Cibernéticos.

- En el proceso de Auditoría se debe incluir la evaluación periódica de los procesos relacionados a Seguridad de la Información y Ciberseguridad.

- Incluir en la Gestión de Seguridad de la Información pruebas de intrusión o pentesting simulados para identificar vulnerabilidades que puedan ser explotadas y afectar la Continuidad del Negocio.

- 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 de la Información y Ciberseguridad que se deben adoptar para protegerse de ataque cibernético.

PROTECCIÓN Y DETECCIÓN

La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de Seguridad de la Información y Ciberseguridad que permitan protegerse ante los mismos, considerando:

- Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de Seguridad de la Información y 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 las plataformas tecnológicas con el propósito de identificar comportamientos inusuales que puedan evidenciar posibles ciberataques contra Visionamos.

NOTA: Esta política hace parte y fue extraída del Manual del Sistema de Gestión de Seguridad de la Información y Ciberseguridad en su VERSIÓN: 05 con fecha del 08/MAY/2025 del numeral 5.2.