POL 011_24 GM

Política general de seguridad de la información y la ciberseguridad

Versión 2

Público

CONTENIDO

1. Historial de revisiones

Versión	Autor (es)	Descripción	Revisado por	Aprobado por	Fecha de aprobación
1.0	Oficial de Seguridad de la Información	Elaboración de documento que incluye los lineamientos generales con relación a seguridad de información y ciberseguridad.	Gerencia de Riesgos	Directorio	24.04.2024
2.0	Oficial de Seguridad de la Información	Se actualiza el documento en cumplimiento del nuevo formato establecido en el Manual del área de procesos. Deroga el documento POL 011_24 GM Política general de SI-C v1 aprobado el 24.04.2024	Gerencia de Riesgos	Directorio	20.12.2024

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

2. Objetivo

Establecer lineamientos que garanticen una adecuada gestión del sistema de seguridad de la información y la ciberseguridad en GMoney, que permita asegurar los criterios de confidencialidad, integridad y disponibilidad de la información, en conformidad con la NTP ISO/IEC 27001:2022.

3. Alcance

El contenido de la presente normativa es de aplicación obligatoria, en lo que corresponda, a los directores, funcionarios y personal involucrado en la gestión de seguridad de la información de GMoney.

4. Base Legal

a. ISO/IEC 27000:2018 "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Información general y vocabulario".

b. NTP-ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de privacidad. Sistema de Gestión de Seguridad de la Información. Requisitos".

c. NTP-ISO/IEC 27002:2022 "Seguridad de la información, ciberseguridad y protección de privacidad. Controles de seguridad de la información".

d. Resolución SBS Nº 504-2021 Reglamento para la gestión de la seguridad de la información y ciberseguridad.

5. Definición de Términos

a. **Activo:** Cualquier bien tangible o intangible que tenga valor para GMoney.

b. **Activo de información**: Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para GMoney y tiene un ciclo de vida.

c. **Amenaza**: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

d. **Alta dirección:** Persona o grupo de personas que dirige y controla a una organización al más alto nivel.

Nota 1: La alta dirección tiene la facultad de delegar la autoridad y proporcionar los recursos dentro de la organización.

Nota 2: Si el alcance del SGSI cubre sólo una parte de una organización entonces la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización.

Nota 3: La alta dirección se llama a veces dirección ejecutiva y puede incluir directores generales, directores financieros, directores de información, y a funciones similares.

e. **Ciberseguridad**: Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

f. **Continuidad del Negocio:** Es un proceso efectuado por el Directorio, la Gerencia y todo el personal, dirigido a implementar respuestas efectivas de operatividad del negocio, con el fin de salvaguardar los intereses de GMoney, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones.

g. **Confidencialidad:** La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.

h. **Disponibilidad:** La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

i. **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a GMoney, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

j. **Gestión de seguridad de la información:** Está orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

k. **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.

l. **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

m. **Integridad:** La información debe ser completa, exacta y válida.

n. **Riesgo:** la posibilidad de ocurrencia de eventos que impacten negativamente sobre los objetivos de la empresa o su situación financiera.

6. Roles y Responsabilidades

Todo el personal de GMoney debe participar activamente en la gestión de seguridad de la información, para lo cual se establece las siguientes responsabilidades:

6.1. Directorio, Gerencia General

a. Aprobar políticas y lineamientos para la implementación del Sistema de Gestión de Seguridad de la Información y la Ciberseguridad y su mejora continua.

b. Asignar los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento.

c. Aprobar la organización, roles y responsabilidades para el Sistema de Gestión de Seguridad de la Información y la Ciberseguridad incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados.

d. La gerencia general, es responsable de tomar las medidas necesarias para implementar el Sistema de Gestión de Seguridad de la Información y la Ciberseguridad de acuerdo con las disposiciones del directorio.

6.2. Gerencias y Jefes de Áreas

a. Apoyar el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

b. Administrar e implementar los controles de seguridad de la información en sus respectivas unidades.

c. Aplicar las medidas disciplinarias por los riesgos asociados al incumplimiento de los lineamientos de seguridad de la información, de acuerdo con el grado de responsabilidad.

d. La Gerencia de Finanzas y Staff, debe velar por el cumplimiento de los aspectos legales en el establecimiento de contratos, como los derechos de propiedad intelectual, ley de protección de datos personales y privacidad de la información.

6.3. Comité de Riesgos

a. Aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir.

b. Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y Ciberseguridad.

c. Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.

6.4. Comité de Crisis

a. Asegurar la aplicación de las estrategias para la seguridad de la información y ciberseguridad, durante la ejecución del plan o programa de Continuidad del Negocio que permita la restauración de las operaciones del proceso del negocio ante la

ocurrencia de una contingencia o evento de pérdida según lo descrito en el Plan de Gestión de Crisis.

6.5. Oficialía de Seguridad de información

a. Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.

b. Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.

c. Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.

d. Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y ciberseguridad.

e. Informar sobre los incidentes de seguridad de la información al Comité de Riesgos, según los lineamientos que este establezca, y a las entidades gubernamentales que lo requieran de acuerdo con la normativa vigente.

f. Evaluar las amenazas de seguridad en las estrategias de continuidad del negocio que la empresa defina y proponer medidas de mitigación de riesgos, así como informar al Comité de Riesgos.

g. Asegurar que la gestión de la seguridad de la información de GMoney se realice de manera consistente de acuerdo a las políticas y procedimientos establecidos para la gestión de riesgos.

h. Velar por una gestión de seguridad de información competente, promoviendo el alineamiento de las medidas de tratamiento de los riesgos de GMoney con los niveles de tolerancia al riesgo y el desarrollo de controles adecuados.

i. Guiar la integración entre la gestión de seguridad de información, los planes de negocio y las actividades de gestión empresarial.

j. Informar al Directorio y Gerencia General, los aspectos relevantes de la gestión de seguridad de información para una oportuna toma de decisiones.

6.6. Gerencia de T.I.

a. Administrar la seguridad de la infraestructura de cómputo y los procedimientos de desarrollo y cambios a los programas.

b. Elaborar los procedimientos e implementar los controles de seguridad de la información y ciberseguridad en los procesos de T.I. que realiza GMoney.

c. Coordinar con la empresa subcontratada del servicio de tecnología de la información, la implementación de controles y gestión de seguridad de la información y ciberseguridad.

d. Administración de las operaciones y comunicaciones.

e. Implementar los controles de seguridad aplicables al activo de información de

acuerdo con su criticidad y nivel de clasificación, basándose en la normativa de seguridad de la información y los análisis de riesgos.

f. Facilitar las auditorías del cumplimiento de los controles de seguridad.

g. Asegurar la disponibilidad de los equipos y servicios de TI que soportan las operaciones del Core de negocio y back office coordinando con los respectivos proveedores el cumplimiento de las prestaciones contratadas.

h. Administrar la asignación/retiro de accesos y perfiles del personal, a los sistemas informáticos de GMoney.

i. Ejecutar los contratos y monitorear el cumplimiento de estos, según los acuerdos de niveles de servicio de seguridad de Información pactados.

6.7. Propietario de activo de información

a. Participar en los procesos de identificación, clasificación y valoración de activos de información.

b. Autorizar la asignación de accesos sobre la información.

c. Autorizar los cambios sobre los activos de información de su propiedad.

d. Realizar la revisión de los derechos de acceso de usuarios a intervalos regulares

e. Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.

6.8. Propietario de riesgos

a. Participar y/o delegar al personal que participará en las actividades de identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información.

b. Evaluar y aceptar el riesgo residual de seguridad del activo de información, y revisarlos periódicamente; así como los criterios de evaluación y aceptación de riesgos.

c. Aprobar el plan de tratamiento de riesgos y contribuir a la implementación de los controles de seguridad de la información que estén relacionados a sus responsabilidades.

d. Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, cuando sea requerido.

6.9. Propietario de oportunidades

a. Participar y/o delegar al personal que participará en las actividades de identificación, análisis, evaluación y tratamiento de las oportunidades.

b. Aprobar el plan de tratamiento de oportunidades y contribuir a la implementación de las acciones a fin de que las oportunidades se materialicen.

c. Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, cuando sea requerido.

6.10. Personal de GMoney

a. Velar por la integridad, disponibilidad y confidencialidad de la información, asimismo informar a la Unidad de Riesgos, las incidencias ocurridas en GMoney, relacionadas a la seguridad de información.

b. Velar por la seguridad física de los activos de información, evitando los accesosno autorizados, daño, robo de los activos o cualquier otra circunstancia que pueda afectar la disponibilidad, integridad y confidencialidad de la información.

c. Usar responsablemente los diferentes medios de transmisión de información, ejecutando acciones que aseguren su integridad, disponibilidad y confidencialidad.

6.11. Terceros o proveedores

a. Cumplir las políticas de seguridad de la información que les aplique, las cláusulas incluidas dentro de los contratos o el acuerdo de confidencialidad, que están referidas a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la organización.

b. Brindar todas las facilidades necesarias para que la organización revise el cumplimiento de las condiciones incluidas en los contratos de los servicios brindados; así como también aspectos de seguridad de la información de los servicios.

c. Identificar y notificar debilidades, eventos, incidentes y riesgos de seguridad de la información al área usuaria que lo contrato y/o al OSI.

7. Política General de Seguridad de la Información y la Ciberseguridad

Para la adecuada seguridad de la información, GMoney establece los siguientes lineamientos:

a. Proteger los activos de información frente a amenazas, internas o externas, deliberadas o accidentales, implementando medidas de control con el fin de asegurar la confidencialidad, integridad, disponibilidad de la información.

b. Proporcionar los recursos necesarios para asegurar el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

c. Gestionar de manera efectiva los riesgos de seguridad de la información y ciberseguridad, implementando controles adecuados para garantizar que no se materialicen.

d. Fortalecer el nivel de competencias y conocimientos sobre las mejores prácticas en seguridad de la información y ciberseguridad en los colaboradores, clientes y proveedores de la organización.

e. Promueve y gestiona una cultura de seguridad de la información y ciberseguridad, para lo cual se apoya en el Programa de capacitación y concientización del SGSI-C.

f. Adopta medidas de seguridad necesarias a fin de garantizar el cumplimiento de las normativas legales y regulaciones en materia de seguridad de la información y ciberseguridad, así como el tratamiento de los datos personales consignados ante la autoridad nacional de protección de datos personales.

g. Establecer y mantener actualizado el procedimiento de gestión de base de datos de eventos de pérdida definido en el Manual de Gestión de Riesgo Operacional, para el tratamiento, en caso de que un incidente de seguridad de información materialice algún tipo de pérdida.

h. Para sus procesos internos y/o a través del proveedor de servicios de T.I., durante la aplicación de los planes de contingencia de continuidad del negocio, garantiza la confidencialidad, integridad y disponibilidad de los activos de información involucrados.

i. Continuamente mejorar la eficacia del Sistema de Gestión de Seguridad de la Información y la Ciberseguridad a fin de reducir al mínimo los riesgos e incidentes relacionados con la seguridad de la información y ciberseguridad.

j. Velar por el cumplimiento de los objetivos de Seguridad de la Información de la organización.