POL 013_24 GM

Política específica de seguridad de la información y la ciberseguridad para las relaciones con los proveedores

Versión 1

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 que deben respetar los proveedores con relación a seguridad de información y ciberseguridad.	Gerencia de Riesgos	Directorio	25.09.2024

POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD PARA LAS RELACIONES CON LOS PROVEEDORES

2. Objetivo

Establecer lineamientos específicos para garantizar la protección adecuada de la información que se comparte o gestiona en colaboración con proveedores para cumplimiento del sistema de gestión de seguridad de la información y la ciberseguridad en GMoney, 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 todos los departamentos y unidades de la organización que gestionen o interactúen con proveedores, contratistas, y socios comerciales que tenga acceso a la información y/o los sistemas de 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. **Amenaza**: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

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

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

d. **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.

e. **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la

organización y que requiere de acciones de respuesta y recuperación.

f. **Información:** Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.

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

h. **Política:** Intenciones y dirección de una organización formalmente expresadas por la alta dirección.

i. **Procesamiento de datos:** El conjunto de procesos que consiste en la recolección, registro, organización, estructuración, almacenamiento, adaptación, recuperación, consulta, uso, transferencia, difusión, borrado o destrucción de datos.

j. **Servicio significativo:** Aquel servicio que, en caso de falla o suspensión, puede poner en riesgo importante a GMoney al afectar sus ingresos, solvencia, o continuidad operativa.

6. Política de servicios provistos por terceros

a. El arreglo contractual con el proveedor debe establecer los roles y responsabilidades que asumirá el proveedor a la seguridad de la información y se compromete a cumplirlos.

b. En caso aplique, el proveedor debe asegurar que el servicio brindado cumpla con las obligaciones y/o estándares establecidos en la Resolución SBS N° 504-2021.

c. El proveedor deberá firmar y hacer entrega del documento de constancia de recepción de la presente política antes de iniciar el trabajo, en el caso se haya iniciado operaciones antes de la aprobación del presente documento, este debe regularizarlo.

d. El proveedor se asegurará que solo se realicen las actividades que descritas en el contrato y/o términos de referencia correspondiente al servicio prestado. Además, debe garantizar el cumplimiento del contrato y cuando corresponda los Acuerdos de Nivel de Servicio (SLA) que formen parte del servicio prestado.

e. El proveedor y los terceros relevantes deberán asegurar que su personal que presta los servicios directamente a GMoney cumpla con los lineamientos establecidos en la presente política. En caso de incumplimiento, la organización se reserva el derecho de solicitar al proveedor el cambio de personal involucrado, sin perjuicio del derecho de la organización de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.

f. El proveedor garantizará que todo intercambio de información entre GMoney y el

proveedor durante la ejecución del servicio tendrá carácter confidencial y no podrá ser utilizada ni manipulada fuera del marco establecido en el contrato de prestación de servicios.

g. En el caso de que el proveedor conozca de cualquier pérdida, uso no autorizado, revelación de la información proporcionada o de propiedad de la institución o cualquier otro evento/debilidad/incidente de seguridad de la información, deberá comunicarlo inmediatamente a través de osi@gmoney.pe, y, en caso de que fuera necesario, adoptar todos los pasos necesarios para ayudar a la entidad a remediar tal uso no autorizado o revelación de la información.

h. Todo proveedor es responsable de transmitir y hacer cumplir la presente política a terceros subcontratados, autorizados debidamente por la organización.

i. El proveedor deberá garantizar que el servicio prestado puede ser monitoreado periódicamente para verificar su cumplimiento de las disposiciones relacionadas.

j. Al finalizar el servicio, el proveedor debe eliminar toda la información recibida durante su ejecución, asegurando que no quede almacenada en ningún soporte. Además, las obligaciones de confidencialidad subsistirán independientemente del motivo de la finalización del servicio.

7. Política de servicios significativos de procesamiento de datos

a. El proveedor debe asegurar el acceso adecuado a la información, en tiempos razonables y a solo requerimiento, por parte de la SBS, auditoría interna (cuando GMoney audita al proveedor) y auditoría externa (cuando GMoney es auditado), en condiciones normales de operación y en regímenes especiales.

b. El proveedor debe informar los servicios, a su vez, contrata con terceros (contratación en cadena) y que se encuentren relacionados a los servicios prestados a GMoney.

c. El proveedor debe asegurar que la información de GMoney que custodia sea eliminada definitivamente ante la resolución o finalización del acuerdo contractual.

d. El proveedor de servicios de procesamiento de datos debe garantizar que es posible verificar periódicamente que cuenta con controles de seguridad de la información.

e. En caso de servicios en nube, el proveedor debe evidenciar anualmente que mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes, relevantes al servicio provisto y a la zona o región desde donde se provee el servicio.

f. El proveedor de servicios de procesamiento de tarjetas debe evidenciar anualmente que cuenta con el estándar de seguridad de datos para la Industria de Tarjeta de Pago

o PCI DSS.

g. El proveedor de servicios de procesamiento de datos debe reportar anualmente la realización y resultados de una evaluación de Ethical Hacking.