GMONEY

POL 013_24 GM

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

Versión 02

Uso interno

CONTENIDO

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

1. Historial de revisiones

Versión	Autor (es)	Descripción	Responsable de revisión	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	25/09/2024
2.0	Oficial de Seguridad de la Información	Se agrega la sección “9. Política de privacidad para proveedores que procesan Información Personal Identificable” para cumplir con requerimientos de privacidad.	Oficial de Seguridad de la Información	31/03/2026

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,la ciberseguridad y privacidad 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. ISO/IEC 27701:2019 "Técnicas de Seguridad – Extensión de la ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información – Requerimientos y guías".

e. Ley N° 29733.- Ley de Protección de Datos Personales.

f. 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. **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.

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

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

e. **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.

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

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

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

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

j. **Sistema de información:** Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.

6. Política de servicios provistos por terceros

a. Se evalúa las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios e implementar medidas de tratamiento

b. Se asegurará que toda implementación que se realice cumpla con las obligaciones establecidas en la Resolución 504-2021 Reglamento para la gestión de la seguridad de la información y ciberseguridad.

c. El arreglo contractual con el proveedor debe establecer los roles y responsabilidades que asumirá respecto a la seguridad de la información, ciberseguridad y la privacidad.

d. 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.

e. El proveedor se asegurará que solo se realicen las actividades que están mencionadas

en el contrato y/o términos de referencia correspondiente al servicio prestado. Además, debe garantizar el cumplimiento del contrato y en algunos casos los acuerdos de niveles de servicio que formen parte del servicio prestado.

f. Todo proveedor deberá velar porque su personal que presta los servicios directamente a la organización 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, sin perjuicio del derecho de la organización de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.

g. El proveedor garantizará que todo intercambio de información entre GMoney y el proveedor durante la ejecución del servicio tendrá carácter confidencialidad y no podrá ser utilizada ni manipulada fuera del marco establecido en el contrato de prestación de servicios.

h. 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 los canales de seguridad de la información proporcionados, 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.

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

j. El proveedor deberá garantizar que el servicio prestado puede ser periódicamente monitoreado para verificar su cumplimiento.

7. Política de uso de servicios en nube

a. Si el proveedor hace uso de servicios en nube debe establecer los requerimientos de seguridad de la información que los servicios de nube deben cumplir y los procedimientos para asegurar la implementación antes de su uso.

b. Establecer lineamientos para segregación de redes que permita el aislamiento de la información de la empresa respecto a la de terceros en el entorno compartido del servicio en nube.

c. Realizar la evaluación de la disponibilidad de registro de eventos (log) que el proveedor de servicio en nube ofrece y atención de la necesidad de registros adicionales para el monitoreo de seguridad de la información.

d. Previsión de plan de capacitación para los niveles gerenciales, administradores de estos servicios, personal a cargo de su implementación y quienes hacen uso de ellos, sobre aquello necesario para el manejo de la seguridad de la información en estos.

8. 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 Superintendencia, Auditoría Interna y la Sociedad de Auditoría Externa, en condiciones normales de operación y en regímenes especiales.

b. El proveedor gestiona los incidentes de seguridad y privacidad de la información, conforme al numeral 6 del artículo 12 y de desarrollar las actividades planificadas previstas en el artículo 13 de la Resolución 504-2021, en lo aplicable al servicio significativo de procesamiento de datos del que se trate.

c. El proveedor cuenta con una estrategia de salida de los servicios a cargo del proveedor que permita retomar operaciones por cuenta propia o mediante otro proveedor. Dicha estrategia debe prever, entre otros aspectos, las acciones necesarias para la migración de la información a los recursos de la empresa o de otro proveedor.

d. El proveedor mantiene un inventario de los servicios que contrata con terceros (contratación en cadena) y que se encuentren relacionados a los servicios contratados por la empresa.

e. El proveedor asegura que la información de carácter confidencial o Información Personal Identificable en custodia del proveedor sea eliminada definitivamente ante la resolución del acuerdo contractual.

f. Se verifica anualmente que el proveedor de servicios de procesamiento de datos cuenta con controles de seguridad de la información. Ello puede ser sustentado mediante informes independientes y reportes de auditoría que incluyen en su alcance la verificación de dichos controles.

g. Cuando se trate de servicios en nube, para cumplir con lo requerido en el literal previo, se debe evidenciar anualmente que el proveedor 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.

h. Se verifica anualmente que el proveedor de servicios de procesamiento de datos cuenta con el estándar de seguridad de datos para la Industria de Tarjeta de Pago o

PCI DSS.

i. Se debe asegurar que anualmente el proveedor de servicios de procesamiento de datos realice una evaluación de Ethical Hacking, en los casos que amerite.

9. Política de privacidad para proveedores que procesan Información Personal Identificable

a. Todo proveedor que procese IPI debe contar con un acuerdo contractual que incluya instrucciones documentadas sobre el tratamiento permitido, finalidades autorizadas, medidas de seguridad, plazos de conservación y procedimientos de devolución o eliminación.

b. El proveedor no debe procesar la IPI para fines distintos a los establecidos por GMoney ni transferirla a terceros sin autorización previa y por escrito.

c. El proveedor debe cumplir con la Ley 29733, su reglamento y cualquier normativa sectorial aplicable a la protección de datos personales.

d. El proveedor debe informar a GMoney sobre cualquier transferencia local o transfronteriza de IPI a un entorno propio o de terceros, indicando país de destino, base legal y salvaguardas aplicadas.

e. El proveedor debe implementar medidas técnicas y organizativas adecuadas para proteger la IPI.

f. El proveedor debe implementar medidas técnicas y organizativas adecuadas para cumplir con las solicitudes de modificación, revocación u objeción relacionada con la IPI compartida a pedido explícito de Gmoney.