POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

Objetivo

Dar a conocer a los proveedores, contratistas, subcontratistas, terceras partes y en general a todas aquellas personas que entregan productos o prestan servicios a Américas BPS, las políticas, procedimientos, controles, normas y buenas prácticas de seguridad de información implementadas que impacten la prestación del servicio para garantizar la seguridad de información nuestra y de nuestros clientes.

Alcance

La presente política de Relación con Proveedores aplica para proveedores, contratistas, subcontratistas, terceras partes y en general a todas aquellas personas que entregan productos prestan servicios a Américas BPS.

Responsabilidades

Gestión administrativa

1. Inventariar los proveedores activos en Américas BPS.
2. Facilitar a seguridad de informacion y control de servicios el inventario de los proveedores activos con la relación del productos o servicios que hayan sido contratados por Americas BPS.
3. Facilitar a seguridad de informacion y control de servicios la documentación que soporta las actividades económicas que desarrolla el proveedor.
4. Facilitador de la comunicación entre seguridad de informacion y control de servicios y el proveedor.
5. Solicitud de planes de acción a proveedores de acuerdo con los resultados de auditoria entregados por seguridad de informacion y control de servicios cuando aplique sobre el formato F01 SGI 050003 Acciones Correctivas Preventivas.
6. Tomar las medidas necesarias a nivel de proceso sobre los resultados de auditoría.
7. Asegurar la firma de cláusulas o acuerdos de confidencialidad con proveedores, contratistas, subcontratistas, terceras partes y en general a todas aquellas personas que prestan servicios a Américas BPS que tengan acceso a información clasificada como CONFIDENCIAL y/o PRIVADA.
8. Garantizar la entrega al proveedor del formato F32 SGI 05 Evaluación Proveedores para diligenciamiento al inicio de la relación contractual.

Seguridad de informacion y control de servicios

1. Garantizar la creación y divulgación de la documentación que soporta la relación con los proveedores.
2. Identificación de requisitos de seguridad de informacion con relación a servicios con proveedores citados en la norma ISO 27001 A15 y PCI DSS.
3. Solicitud de inventario de proveedores a gestión administrativa.
4. Clasificación de los proveedores de acuerdo con su criticidad identificada en el formato F01 SGI 050014 Matriz e identificación de proveedores
5. Ejecución de actividades de auditorías a proveedores en ocasión a los requisitos identificados.
6. Generación de informe de auditorias de acuerdo con los resultados.
7. Gestionar los riesgos de acuerdo con la metodología D1 SGI 05 Metodología Valoración Riesgos.
8. Ejecutar seguimiento a los planes de acción entregados por los proveedores a través de gestión administrativa sobre el formato F21 SIG 005 Matriz de oportunidades de mejoramiento – MOM.
9. Asegurar que el documento PO9 SGI 05 Política Relación Proveedores se encuentre publicado en la página web para conocimiento de las partes interesadas.

Comprador operacional

1. Asegurar que se efectúe la gestión de riesgos en los contratos que son responsables.
2. Reportar a seguridad de informacion y control de servicios los riesgos identificados para el proveedor.

Proveedores

1. Adoptar y cumplir con las directrices de la presente política
2. Respuesta oportuna a los requerimientos de Americas BPS en aplicación de la presente política.

Directrices

A continuación, se describen las directrices que deben acatar los proveedores, contratistas, subcontratistas, terceras partes y en general a todas aquellas personas que prestan servicios a Américas BPS, en nuestras instalaciones o cuando se realicen conexiones a nuestros sistemas de información:

1. La evaluación de proveedores se deberá realizar por parte de seguridad de información y control de servicios mínimo una vez al año.
2. Seguridad de la informacion y control de servicios se reserva el derecho de ejecutar auditorias a proveedores para garantizar el cumplimiento de los requisitos técnicos.
3. Al ingresar a las diferentes sedes de Américas BPS, se debe anunciar la llegada del visitante a la persona responsable quien realizara el acompañamiento correspondiente mientras permanezca en las instalaciones de la compañía.
4. Se debe portar en un lugar visible y en todo momento el carné de identificación proporcionado para permanecer dentro de las instalaciones de la compañía.
5. Cuando se vaya a realizar algún trabajo dentro de las instalaciones de Américas BPS debe adjuntar la fotocopia de la planilla del último pago de Seguridad Social (ARL, EPS, AFP) de cada una de las personas que ingresaran a nuestras instalaciones; si se van a realizar trabajos en alturas, se debe adjuntar certificado de aptitud para trabajo en alturas vigente de las personas que realizaran el trabajo.
6. Los equipos equipo de cómputo, computador portátil o equipos de comunicaciones como celulares que ingresen a las instalaciones de Americas BPS, deben ser autorizados previamente por la dirección de seguridad de información y control de servicios.
7. Es responsabilidad de los proveedores, contratistas, subcontratistas, terceras partes y en general a todasaquellas personas que prestan servicios a Américas BPS que ingresen computador portátil, equipo de cómputo o equipos de comunicaciones (celular) a las instalaciones de la compañía velarpor la seguridad e integridad del equipo dentro de las instalaciones.
8. Los usuarios a los cuales se les otorga el permiso de ingreso y manipulación de equipos o computadores portátiles solo deben realizar labores estrictamente necesarias para el cumplimiento de su función.
9. Si el usuario debe conectar el equipo o computador portátil a la red de la compañía para la ejecución de sus actividades debe solicitar permiso de conexión a la dirección de seguridad de información y control de servicios y cumplir con los descrito en el PR SGI 050011 Control Acceso Red ABPS.
10. La Evaluación de riesgos aplica aquellos proveedores que tengan acceso directo a las áreas seguras, activos críticos de información y/o cualquier activo que pueda afectar la Continuidad del negocio, acceso al entorno PCI y acceso a datos personales sobre los cuales Americas BPS actúa como responsable.
11. Para todos los contratistas que tengan acceso a información clasificada como confidencial y/o privada, deben contar bien sea con una cláusula de confidencialidad en su contrato o deben firmar el acuerdo de confidencialidad definido para ello.
12. Para los proveedores que subcontraten partes del servicio de tecnología de la

información y comunicaciones que suministran a AMERICAS BPS, se debe solicitar que divulguen y garanticen el cumplimiento de los requisitos y prácticas de seguridad de Americas BPS a lo largo de la cadena de suministro.

13. Durante la ejecución del contrato, es función del supervisor del contrato (comprador operacional), monitorear y hacer seguimiento a los controles pactados para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
14. Si se detecta un incumplimiento frente a la seguridad de la información, ciberseguridad y privacidad de los datos por parte del proveedor, el comprador operacional deberá reportar a la dirección de seguridad de información y control de servicios para iniciar el proceso de verificación y evaluar las consecuencias posibles.
15. Toda gestión que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe ser evaluado y autorizado por el procedimiento de Gestión de cambios antes de su ejecución por parte de cualquier proveedor.
16. Américas BPS, asegura la verificación del proveedores y contrapartes antes de su contratación y/o vinculación, lo anterior se garantiza a través del cumplimiento del procedimiento de vinculación de grupos de interés en atención a la política de SAGRILAFT (Sistema de Autocontrol y Gestión del Riesgo Integral de Lavado de Activos y Financiación del Terrorismo.) y también, se asegura por medio de la matriz de proveedores entorno de datos de titulares de tarjeta incluida en el procedimiento PR SGI 050014 Gestión Proveedores y con la gestión de la evaluación de proveedores formato 3. F32 SGI 05 Evaluación Proveedores.

Registro de Control de Cambios o Revisiones			
Versión	**Descripción del Cambio o Comentarios de Revisiones**	**Elaboró o Revisó**	**Aprobó**
00 31/07/2020	Elaboración inicial del documento.	Diego Alexander Pérez Rodríguez Director de SGSI	Diego Alexander Pérez Rodríguez Director de SGSI
01 26/07/2022	Se elimina enlace de consulta para proveedores, página web.	Jose Wilfran Giraldo Ospina Analista de Seguridad de la Información	Ruben Alexander Rico Ricaurte Director de SGSI y control de servicios
02 17/11/2022	Se incluye directriz sobre la verificación del proveedores y contrapartes antes de su contratación y/o vinculación en cumplimento a la política de LA/FT; en cumplimiento al PR SGI 050014 Gestión Proveedores (la matriz de proveedores entorno de datos de titulares de tarjeta) y con la gestión de la evaluación de proveedores formato F32 SGI 05 Evaluación Proveedores.	Cristian Vicente Hernández Blanco Practicante Seguridad de la Información	Rubén Alexander Rico Director Seguridad Información y Control Servicios

03 09/03/2023	Se incluyen responsabilidades administrativas, se actualizan responsabilidades de Seguridad de informacion y control de servicios, Comprador operacional, y proveedores,	Adriana Paola Diaz Santos Coordinador SGI	Rubén Alexander Rico Director Seguridad Información y Control Servicios