americas
BPS Outsourcing Transformation

Políticas de Seguridad de la Información, Ciberseguridad y Privacidad para Proveedores y Partes interesadas en la contratación de servicios de Américas BPS

Tabla de contenido

1. Introducción

El presente documento establece los lineamientos, obligaciones y requisitos mínimos en materia de seguridad de la información, ciberseguridad y privacidad que deberán cumplir los proveedores y partes interesadas que mantengan una relación contractual con Américas Business Process Services, con el propósito de extender el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) a terceros y asegurar la adecuada gestión de los riesgos asociados al tratamiento y procesamiento de información.

2. Objetivo

Establecer los lineamientos y requisitos obligatorios en materia de seguridad de la información, ciberseguridad y privacidad que deberán cumplir los proveedores y partes interesadas en el marco de ofertas, acuerdos o contratos con la compañía, con el fin de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, así como la adecuada gestión de los riesgos asociados a su tratamiento, procesamiento y acceso

3. Alcance

Este documento aplica para todos los proveedores, contratistas y terceras partes que interactúen con sistemas de información de la compañía y de nuestros clientes u ofrezcan servicios asociado.

4. Políticas y objetivos de seguridad de la información

AMÉRICAS BPS establece e implementa controles y medidas técnicas, administrativas y organizacionales orientadas a proteger la confidencialidad, integridad, disponibilidad y privacidad de la información, en el marco de su Sistema de Gestión de Seguridad de la Información (SGSI), como mecanismo para fortalecer la ciberseguridad, el relacionamiento y la confianza con sus clientes y partes interesadas.

El enfoque de gestión del riesgo adoptado por la organización se fundamenta en las directrices de las normas ISO/IEC 27005 e ISO 31000, integradas al SGSI y adaptadas a los procesos, activos y contexto estratégico de la compañía, bajo un principio de mejora continua.
En este sentido, los proveedores y partes interesadas deberán conocer, adoptar y cumplir las directrices y requisitos establecidos, conforme a las disposiciones contractuales, legales y regulatorias aplicables.

5. Requisitos de Seguridad de la Información y Ciberseguridad

AMERICAS BPS verificará el cumplimiento de los requisitos planteados en este documento mediante auditorías directas o a través de un tercero para garantizar la aplicación del presente anexo.

1. Proteger la **confidencialidad**, **integridad** y **disponibilidad** de la información propiedad de AMÉRICAS BPS, así como la de sus clientes y usuarios, cuando los servicios contratados así lo requieran. Esto incluye toda información generada, almacenada o procesada en el marco de la relación contractual o jurídica.
2. Garantizar la **disponibilidad del servicio** de acuerdo con los Acuerdos de Nivel de Servicio (ANS) establecidos en el contrato.

3. Utilizar **mecanismos seguros de transmisión de información**, que incluyan cifrado fuerte y autenticación robusta (por ejemplo, cifrado TLS 1.2 o superior y autenticación multifactor).
4. Utilizar únicamente **software legalmente adquirido**, en cumplimiento de la Ley 603 de 2000 o la normativa que la sustituya o complemente. El proveedor mantendrá indemne a AMÉRICAS BPS frente a cualquier reclamación por incumplimiento.
5. Extender los compromisos de **confidencialidad** a todos los colaboradores y terceros involucrados en la ejecución del contrato.
6. Compartir con AMÉRICAS BPS y mantener actualizado durante la relación contractual, el **diagrama de arquitectura tecnológica y/o física** de la infraestructura donde se procesará información de propiedad de AMÉRICAS BPS, sus clientes o usuarios.
7. Informar previamente a AMÉRICAS BPS sobre cualquier **cambio en la infraestructura tecnológica o física** que impacte el tratamiento de dicha información.
8. Colaborar y permitir que AMÉRICAS BPS o un tercero designado que se realicen **auditorías de seguridad y ciberseguridad**, incluyendo revisiones a infraestructura, procesos y procedimientos. Las auditorías se notificarán con al menos cinco (5) días de antelación.
9. Ejecutar procesos de **verificación de antecedentes y validación de hoja de vida** del personal que participará en la relación contractual, conforme con el contrato y las políticas internas del proveedor.
10. **Controlar los accesos físicos y lógicos** del personal a estaciones de trabajo y a la infraestructura tecnológica de AMÉRICAS BPS, en cumplimiento con los procedimientos y manuales del proveedor.
11. Contar con **políticas y procedimientos de borrado seguro** de información que puedan aplicar a datos de AMÉRICAS BPS, sus clientes o usuarios. El borrado debe realizarse mediante destructoras certificadas (para documentos físicos) o herramientas tecnológicas confiables (para datos digitales), y deberá presentarse evidencia documental de su ejecución.
12. **Restringir el uso de medios de almacenamiento removibles** (USB, discos externos, etc.) y controlar la extracción de información alojada en dispositivos del proveedor relacionados con servicios contratados por AMÉRICAS BPS.
13. Contar y aplicar una **metodología de análisis y gestión de riesgos** que permita identificar, al menos anualmente, los riesgos asociados a la seguridad de la información, ciberseguridad y privacidad, considerando procesos, activos y servicios objeto del contrato.
14. Tener procedimientos formales para la **identificación, mitigación y alerta de vulnerabilidades y eventos**, incluyendo:
    - Resultados de análisis de vulnerabilidades
    - Pruebas de penetración (pentesting)
    - Ejercicios de hacking ético y pruebas de ingeniería social

    AMÉRICAS BPS podrá solicitar esta evidencia para evaluar la postura de seguridad del proveedor.
15. Implementar procesos de gestión de vulnerabilidades que permitan identificar, evaluar, mitigar y remediar vulnerabilidades de manera oportuna así como gestionar de manera inmediata el software malicioso. En caso de desarrollar software para AMÉRICAS BPS, el proveedor debe aplicar estándares de desarrollo seguro (ej. OWASP) y, cuando aplique, cumplir con PCI PA-DSS u otros marcos normativos.
16. Tener documentados e implementados **procedimientos de gestión de incidentes de seguridad de la información, ciberseguridad y privacidad**, que incluyan las siguientes fases mínimas:
    - Prevención
    - Protección
    - Detección
    - Contención
    - Respuesta

- Comunicación
- Recuperación
- Aprendizaje

Elementos específicos requeridos:

a. Protocolos de actuación frente a **ransomware**.
b. Protocolos definidos y probados para **análisis forense digital**, ajustados al marco legal colombiano.
c. **Matriz RACI de gestión de incidentes**, con niveles de escalamiento y disponibilidad 24x7 para informar incidentes a AMÉRICAS BPS.
d. Protocolos para la **toma de decisiones** que permitan contener incidentes relacionados con redes, sistemas, personal o datos, incluyendo mecanismos para recolectar evidencia.
e. Estrategias de **validación de seguridad periódicas** orientadas a contrarrestar ataques de día cero.
f. **Planes de simulación de ciberataques** y pruebas de activación de DRP (internos y externos), incluyendo la participación de AMÉRICAS BPS.

17. **AMÉRICAS BPS podrá solicitar los registros o logs necesarios** que respalden la investigación, análisis y solución de incidentes de seguridad de la información, ciberseguridad o privacidad.
18. El proveedor deberá **informar de forma inmediata** cualquier evento de **fuga, pérdida, alteración o acceso no autorizado** a información de AMÉRICAS BPS, de sus clientes y/o usuarios. La notificación debe enviarse a:
    incidentes.seguinfo@americasbps.com
    y al interventor o comprador operacional designado.

20. En caso de incidentes que afecten la confidencialidad, integridad, privacidad o disponibilidad de la información o servicios:

- Reportar inmediatamente a los canales establecidos.
- Informar periódicamente el estado de gestión del incidente, los indicadores de compromiso y las acciones de contención.
- Entregar un informe con la gestión del incidente, medidas de remediación y lecciones aprendidas, a la mayor brevedad.

21. Ejecutar auditorías o revisiones de seguridad sobre terceros críticos o involucrados en la prestación de servicios contratados por AMÉRICAS BPS. AMÉRICAS podrá requerir los resultados en cualquier momento.
22. Contar con un Plan de Contingencia y Continuidad del Negocio (PCN) y un Plan de Recuperación ante Desastres (DRP), documentados, implementados y probados al menos una vez al año. Estos planes deben garantizar la continuidad del servicio prestado y contemplar como mínimo: i). Escenarios adversos como desastres naturales, ciberataques, sabotajes, disturbios, terrorismo, etc. Ii). Evaluación de riesgos asociados a continuidad y recuperación. Iii). Cuando la criticidad del servicio así lo requiera, dos (2) zonas geográficas de disponibilidad separadas con niveles de riesgo diferenciados. Iv). Pruebas de intercambio de zonas de disponibilidad, validadas con el área de continuidad y tecnología de AMÉRICAS BPS. v). Notificación inmediata ante activación de planes o incidentes de indisponibilidad, conforme a ANS

contractuales. vi). Contar con un ambiente de contingencia que garantice el mismo nivel de seguridad de información y ciberseguridad del ambiente de producción

6. Requisitos de Privacidad – Protección de Datos Personales

En caso de que en la ejecución del contrato el proveedor o parte interesada realice tratamiento de datos personales en los cuales AMÉRICAS BPS actúe como responsable o encargado, se entenderá que el proveedor actuará como encargado o subencargado de dicha información por cuenta y orden de AMÉRICAS BPS. En consecuencia, deberá cumplir con la Política de Protección de Datos Personales de la organización, la Ley 1581 de 2012, sus decretos reglamentarios, LEY 2300:2023 y demás normatividad vigente. En caso de tratarse de datos personales de ciudadanos europeos, deberá además cumplir con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

Obligaciones del proveedor o parte interesada:

1. Tratar la información personal exclusivamente para la ejecución del objeto contractual, conforme a las instrucciones de AMÉRICAS BPS.
2. Cumplir la Política de Protección de Datos Personales de AMÉRICAS BPS y toda normatividad vigente en la materia.
3. Implementar medidas técnicas y administrativas apropiadas antes de iniciar el tratamiento, para prevenir la modificación, pérdida, consulta o acceso no autorizado.
4. Establecer mecanismos para la detección de desviaciones y garantizar el nivel de seguridad adecuado según los riesgos asociados al tratamiento.
5. Abstenerse de divulgar, transferir o ceder información personal a terceros sin autorización expresa de AMÉRICAS BPS o del titular, salvo requerimiento legal o de autoridad competente. En este caso, deberá informar de inmediato a AMÉRICAS BPS.
6. Contar con un procedimiento de respuesta a incidentes de datos personales, en línea con lo exigido por la Superintendencia de Industria y Comercio, y reportar de forma inmediata reclamo o solicitud a correo: habeasdata@americasbps.com, si se trata de un incidente o una vulnerabilidad a incidentes.seguinfo@americasbps.com.
7. Trasladar cualquier solicitud o reclamo de titulares a AMÉRICAS BPS en un tiempo máximo de 24 horas.
8. Asegurar que la información de AMÉRICAS BPS sea almacenada exclusivamente en territorios permitidos conforme a la normativa colombiana vigente y las políticas internas de AMÉRICAS BPS.
9. Cuando AMÉRICAS BPS determine que el tratamiento se encuentra sujeto a dicha normativa, garantizar el cumplimiento del GDPR cuando se trate de datos de ciudadanos europeos.
10. En caso de tratamiento de datos sensibles o semisensibles, firmar acuerdos internos con sus colaboradores sobre el manejo adecuado de estos datos.

7. Requisitos de Seguridad de la Información, Ciberseguridad y Privacidad para Servicios en la Nube

Cuando el servicio contratado con AMÉRICAS BPS sea prestado total o parcialmente en ambientes de cómputo en la nube, el proveedor o parte interesada deberá cumplir con los lineamientos definidos en el control 5.23 de la norma ISO/IEC 27001:2022, así como con las siguientes obligaciones:

Control de acceso

- Contar con procedimientos documentados e implementados para la gestión de accesos de usuarios a sistemas en la nube.
- Permitir el acceso exclusivamente a personas y dispositivos autorizados.
- Aplicar el principio de menor privilegio y controles de autenticación fuertes.
- Garantizar que todos los accesos sean registrados, trazables y sujetos a auditoría.

Seguridad en las operaciones:

1. Desarrollar bajo estándares de codificación segura, como los definidos por OWASP.
2. Ejecutar pruebas de código seguro mediante recursos internos o terceros autorizados.
3. Sustentar los cierres de hallazgos con revalidación técnica (retesting) y, cuando aplique, certificados de cumplimiento.
4. Permitir a AMÉRICAS BPS o su delegado ejecutar análisis de vulnerabilidades y pruebas de seguridad informadas.
5. Realizar análisis de vulnerabilidades periódicos sobre los activos de información involucrados. Para hallazgos:
    - Críticos o altos: gestionar y remediar en un plazo máximo de 1 mes.
    - Medios: en un plazo no mayor a 3 meses.
    - Bajos: entregar plan de tratamiento o justificación consensuada con AMÉRICAS BPS.
6. Ejecutar mínimo dos (2) análisis de vulnerabilidades al año y conservar los informes de los últimos dos años.
7. Aplicar prácticas de aseguramiento sobre los dispositivos vinculados al servicio.
8. Implementar cifrado robusto de información en tránsito, reposo y bases de datos.
9. Garantizar la generación, conservación y disponibilidad de registros de auditoría (logs).
10. Restringir el uso de medios removibles para la copia de información.

Copias de respaldo

El proveedor debe informar y certificar ante AMÉRICAS BPS:

1. El alcance y contenido de las copias de respaldo del servicio contratado.
2. El estado de implementación de su política de respaldos.
3. La política de retención de la información, en concordancia con el contrato.
4. Las medidas de protección implementadas (cifrado, traslado seguro, pruebas de restauración).
5. El procedimiento formal para solicitar la restauración de copias de respaldo.

Devolución y destrucción de la información

Al finalizar la relación contractual, el proveedor deberá:

1. Garantizar la devolución de la información propiedad de AMÉRICAS BPS en un formato estándar, en los tiempos establecidos por la compañía.
2. Ejecutar la eliminación o destrucción segura de la información, mediante Métodos certificados o estándares reconocidos internacionalente y entregar evidencia documental del proceso.

Gestión de activos de información

1. Mantener procedimientos y controles vigentes para la gestión de activos vinculados al servicio.
2. Tener identificado y actualizado el inventario de activos utilizados para procesar, almacenar o transmitir información de AMÉRICAS BPS.
3. Reconocer que AMÉRICAS BPS es titular de la información tratada y que no podrá usarse para fines distintos al objeto contractual.

Estaciones de trabajo del personal de gestión

Cuando aplique, el proveedor deberá:

1. Controlar la navegación web para permitir solo sitios necesarios para el cumplimiento del servicio.
2. Restringir el acceso y uso de servicios interactivos o mensajería instantánea no autorizada (ej. WhatsApp Web, Telegram, Facebook Messenger, etc.).
3. Impedir la descarga, intercambio o instalación de contenidos o software no autorizado que comprometa la propiedad intelectual o la seguridad.
4. Prohibir el uso de cuentas de correo o almacenamiento personal para tratar información de AMÉRICAS BPS.
5. Asegurar que los usuarios no tengan privilegios para instalar software o alterar configuraciones del equipo.

8. Requisitos de Seguridad de la Información, Ciberseguridad y Privacidad en Servicios que Involucren el Uso de Inteligencia Artificial

Cuando la prestación de servicios contratados con AMÉRICAS BPS involucre el uso de tecnologías basadas en Inteligencia Artificial (IA), el proveedor o parte interesada deberá cumplir con los principios de responsabilidad, explicabilidad, trazabilidad y seguridad establecidos por la normatividad vigente, incluyendo la Ley 1581 de 2012, ley 2300:2023, el Reglamento General de Protección de Datos (GDPR) cuando aplique, así como los controles de la norma ISO/IEC 27001:2022, ISO 42001:2023, y los requisitos de seguridad técnica definidos en PCI DSS v4.01.

Obligaciones del proveedor:

1. Evaluar y documentar el **nivel de riesgo inherente al uso de la solución de IA**, considerando el contexto del tratamiento de datos y la criticidad del servicio prestado.
2. Ser capaz de **explicar y documentar el modelo de funcionamiento de la IA**, incluyendo los criterios de toma de decisiones automatizadas y la lógica empleada en predicciones, conforme al principio de transparencia.
3. Declarar la fiabilidad y robustez del sistema de IA, incluyendo controles para evitar sesgos, errores o fallas en la interpretación de resultados.
4. Realizar evaluación de impacto en protección de datos cuando el nivel de riesgo del tratamiento lo requiera.
5. No capturar, tratar o utilizar **datos personales sin contar con autorización previa**, expresa e informada de los titulares o sin habilitación contractual de AMÉRICAS BPS.
6. Aplicar el principio de **"seguridad desde el diseño" (Security by Design)** para mitigar riesgos cibernéticos, fuga de información y acceso no autorizado desde el desarrollo y puesta en marcha del sistema de IA.
7. Gestionar vulnerabilidades de forma oportuna:
   - **Críticas:** en un máximo de 30 días.
   - **Altas o medias:** en un máximo de 90 días.
   - Las bajas deben contar con plan de tratamiento o justificación técnica.

8. Garantizar que, en caso de utilizar **datos de personas para entrenamiento, operación o personalización**, se pueda informar con precisión:
   - Qué datos se recopilan.
   - Cómo se utilizan.
   - Qué medidas se adoptan para proteger la privacidad.
   - Qué opciones tiene la persona para gestionar o restringir el tratamiento.
9. Implementar medidas que aseguren que la solución de IA **no cause daño físico, emocional, psicológico o discriminatorio** a los usuarios, titulares o terceros.
10. En caso de utilizar soluciones de IA integradas por terceros (cloud o API externas), el proveedor deberá garantizar su **validación de seguridad, análisis de impacto y cumplimiento contractual con los requisitos aplicables** definidos por AMÉRICAS BPS.

Realizar evaluación de impacto algorítmico cuando el uso de IA implique decisiones automatizadas que puedan afectar derechos de los titulares

9. Control de Cambios

Versión	Descripción del cambio	Elaboró	Aprobó
00 19/04/2024	Creación del documento.		
01 8/01/2025	Se actualiza proceso de acuerdo con los cambios organizacionales, el proceso pasa de ser sistema de gestión integrado 05, a ser Ciberseguridad y privacidad 05. Se incluye subproceso Ciberseguridad 0501. Se actualiza código del documento, anterior código MA46 SGI 05, nuevo código del documento MA02 CYP 0501. Se actualiza imagen corporativa.		
02 15/04/2025	Revisión general e inclusión de requisitos de inteligencia artificial, privacidad ciberseguridad.		
03 002/03/2026	Ajustes asociados a IA, privacidad y seguridad de la información. Se cambia de código pasa de MA02 CYP 0501 a MA02 CYP 01 por cambios estructurales de a la codificación		