americas
BPS Outsourcing Transformation

Manual de Políticas de Seguridad de la Información Américas Business Process Services

Tabla de contenido

Introducción

Américas Business Process Services pone a disposición de sus clientes, colaboradores, contratistas y terceros autorizados el presente documento "MA1 CYP 0501 – Manual de Políticas Américas BPS", el cual contiene una descripción general de las políticas de seguridad de la información implementadas en la organización, con el propósito de fortalecer su Sistema de Gestión de Seguridad de la Información (SGSI).
En caso de requerirse mayor detalle sobre cualquiera de las políticas aquí definidas, esta información podrá ser facilitada únicamente por el Director de Ciberseguridad y Privacidad, en las instalaciones de la compañía, previa solicitud formal y bajo las condiciones establecidas.
Cabe resaltar que el contenido detallado de estas políticas está clasificado como información privada y confidencial de Américas BPS, por lo tanto, su divulgación o reproducción no autorizada se encuentra restringida, en cumplimiento de las normas internas y la legislación aplicable.

1. Definiciones

Directrices: Es una instrucción o norma que se tiene en cuenta para la ejecución de las diferentes actividades labores desarrolladas a diario en la compañía.
Manual: Instrumento de trabajo que contiene el conjunto de normas y directrices que debe seguir cada empleado en el desarrollo de sus actividades laborales diarias.
Política: Es la actividad concerniente a la toma de decisiones que conducirán el accionar de la compañía para alcanzar ciertos objetivos.

2. Objetivo

Dar a conocer las diferentes políticas generadas por la compañía las cuales son de estricto cumplimiento para garantizar la integridad, confidencialidad y disponibilidad de la información.

3. Alcance

El presente Manual de Seguridad de la Información Américas Business Process Services, aplica para todos los clientes , colaboradores, contratistas, proveedores y terceras partes que interactúen con sistemas de información de la compañía y de nuestros clientes.

4. Políticas seguridad de la información Américas Business Process Services

A continuación, se presentan las directrices definidas por el área de Ciberseguridad y Privacidad, aprobadas por la Gerencia General, las cuales deberán ser de estricto cumplimiento por parte de todos los colaboradores, proveedores, contratistas, clientes y terceros que interactúan con los sistemas de información o acceden a activos gestionados por Américas Business Process Services.

Estas políticas establecen el marco normativo interno en materia de seguridad de la información, protección de datos personales y uso adecuado de los recursos tecnológicos, en el contexto de los servicios prestados por la compañía.

4.1. Política y objetivos de seguridad de la información

Américas Business Process Services, en cumplimiento de su misión de proveer servicios de procesos de negocio que agregan valor y fortalecen la estrategia de sus clientes, garantiza la confidencialidad, integridad, disponibilidad, procesamiento y tratamiento seguro de la información, como mecanismo esencial para consolidar la ciberseguridad, el relacionamiento y la confianza con el cliente.

El enfoque institucional de valoración y gestión del riesgo se fundamenta en las Normas Técnicas Colombianas ISO/IEC 27005 e ISO 31000, adaptadas a los procedimientos, objetivos y estrategia organizacional. Este modelo permite establecer actividades coordinadas orientadas a la prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje frente a los riesgos que puedan comprometer la seguridad de la información dentro de los procesos que conforman Américas Business Process Services.

Como parte de su compromiso con la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), la compañía asegura que colaboradores, contratistas, proveedores, clientes y terceros conozcan, acepten y apliquen las directrices establecidas en materia de seguridad, de acuerdo con las disposiciones contractuales, legales y regulatorias aplicables.

4.2. Objetivos del SGSI

- Aumentar el nivel de confianza en los clientes.
- Proporcionar las directrices y herramientas para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de los procesos del negocio y del cliente.
- Proporcionar las directrices y herramientas para asegurar la ciberseguridad y el cumplimiento legal y regulatorio en torno a los datos corporativos.

4.2.1 Alcance

La presente política de seguridad aplica para la comercialización, administración, diseño, implementación y gestión de operaciones en la prestación de servicios BPO con el propósito de garantizar la confidencialidad, integridad, disponibilidad, procesamiento y tratamiento de la información como mecanismo para fortalecer el relacionamiento y la confianza con el cliente.

4.2.2 Responsabilidades

La aprobación de la política de seguridad será realizada por la Gerencia General. Cualquier cambio, corrección o actualización en el presente documento deben ser propuestos por el comité de seguridad de la información y objeto de aprobación de la Gerencia General.

4.3. Política Gestión de contraseñas

Las contraseñas son un medio común de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información.

Américas Business Process Services establece las directrices para proteger el acceso a nuestros sistemas de información, es importante que las contraseñas que usemos sean seguras y fuertes, para evitar que un usuario no autorizado pueda obtenerlas y usarlas para propósitos no deseados.

Los administradores de sistemas de información y redes deben velar por la aplicación permanente de esta

política y de los diferentes controles tecnológicos establecidos para la gestión de contraseñas por parte de todos los empleados de Américas Business Process Services y terceras partes (proveedores, consultores, contratistas, clientes, outsourcing, etc.) así como conocer los mecanismos del dominio de la compañía para establecer políticas a nivel de usuario.

4.3.1 Objetivos de la política

- El propósito de esta política es establecer los lineamientos para el uso, manejo de cambios y elaboración de contraseñas seguras de las aplicaciones Internas y Externas de Américas Business Process Services.
- Dar a conocer a los empleados de Américas Business Process Services, terceras partes (proveedores, consultores, contratistas, clientes, outsourcing, etc.) los lineamentos establecidos por la compañía para la gestión de contraseñas.
- Garantizar la correcta gestión de contraseñas para permitir el ingreso a los diferentes sistemas de información de Américas Business Process Services y de sus clientes.

4.3.2 Alcance

La presente política de gestión de contraseñas aplica para todos los empleados de Américas Business Process Services, proveedores, contratistas, clientes y terceras partes que interactúen con sistemas de información de la compañía y de nuestros clientes.

4.3.3 Responsabilidades

La responsabilidad sobre la elaboración, revisión, actualización y aplicación de la Política de Gestión de Contraseñas recae en el área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier modificación o ajuste al presente documento deberá ser propuesto, validado y formalizado por el Director de Ciberseguridad y Privacidad, asegurando su alineación con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI), los requisitos técnicos aplicables y las mejores prácticas internacionales en gestión de accesos.

4.4. Política Escritorio Despejado Y Pantalla Despejada

Américas Business Process Services establece la política de Escritorio Despejado y Pantalla Despejada para reducir los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo. Archivadores, cajoneras u otras formas de almacenamiento seguro pueden también proteger la información almacenada dentro de ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones.

Los usuarios de los sistemas de información de Américas Business Process Services y de sus clientes son responsables de proteger el acceso a dichos sistemas, siguiendo los diferentes lineamientos y procedimientos establecidos para garantizar la seguridad de la información, el desconocimiento o no uso de estos es sancionado de acuerdo con el procedimiento definido.

4.4.1. Objetivos de la política

- Establecer las directrices que los empleados de Américas Business Process Services, proveedores, contratistas, clientes y terceras partes deben seguir para mantener la integridad, disponibilidad y confidencialidad de la información.
- Sensibilizar a los usuarios de los sistemas de información sobre la importancia que tiene la correcta ejecución de los controles y procedimientos establecidos para salvaguardar la información y ejecutar las mejores prácticas que garanticen la seguridad de la misma.

4.4.2 Alcance

La presente política de Limpieza de Pantalla y Escritorio aplica para todos los empleados de Américas Business Process Services, proveedores, contratistas, clientes y terceras partes que interactúen con sistemas de información de la compañía y de nuestros clientes.

4.4.3 Responsabilidades

La elaboración, mantenimiento, revisión y aprobación de la Política de Escritorio Despejado y Pantalla Despejada será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier cambio, corrección o actualización del presente documento deberá ser propuesto y validado por el Director de Ciberseguridad y Privacidad, asegurando su alineación con los lineamientos del Sistema de Gestión

de Seguridad de la Información (SGSI), los controles físicos y lógicos definidos por la organización y las mejores prácticas de protección de la información.

4.5. Política Uso de la mensajería instantánea

El uso de plataformas de mensajería instantánea y servicios interactivos dentro de Américas Business Process Services estará regulado por las directrices de seguridad de la información definidas por el área de Ciberseguridad y Privacidad, y su aplicación se clasificará conforme al nivel de riesgo que representan.

Américas BPS adopta como plataforma oficial de mensajería colaborativa el ecosistema de Microsoft 365, habilitando exclusivamente el uso de Microsoft Teams para comunicaciones internas, gestión de proyectos y colaboración digital. Su uso está soportado bajo criterios de trazabilidad, monitoreo, control de accesos, cifrado de extremo a extremo y respaldo contractual corporativo.

Se prohíbe expresamente el uso de herramientas de mensajería no autorizadas tales como WhatsApp Web, Telegram, Signal, Discord, Facebook Messenger, Google Chat, Zoom Chat, entre otras, ya sea mediante aplicaciones instaladas o acceso vía navegador web, salvo aprobación previa del área de Ciberseguridad y Privacidad.

Ningún colaborador, contratista o tercero de Américas BPS debe instalar, ejecutar o conectarse a servicios de mensajería instantánea ajenos a los canales oficiales, excepto si cuenta con autorización expresa de la gerencia del área a la que pertenece, previa justificación de uso y validación de riesgos. Dicha autorización deberá quedar documentada, y el colaborador se comprometerá a utilizar exclusivamente el canal aprobado para fines estrictamente laborales y bajo los principios de confidencialidad, integridad y disponibilidad de la información.

El incumplimiento de esta política podrá conllevar sanciones conforme a los procedimientos disciplinarios vigentes, sin perjuicio de las acciones legales aplicables por uso indebido de información o recursos institucionales.

4.5.1 Objetivos de la política

- Establecer lo lineamentos para la correcta utilización del servicio de mensajería instantánea al interior de Américas Business Process Services.
- Garantizar la seguridad de la información mediante la implementación de buenas prácticas al hacer uso de programas de mensajería instantánea minimizando los riesgos que se puedan presentar.

4.5.2 Alcance

La presente política de uso de la mensajería instantánea aplica para todos los empleados de Américas Business Process Services, proveedores, contratistas, clientes y terceras partes.

4.5.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Uso de la Mensajería Instantánea será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier cambio, corrección o actualización en el presente documento deberá ser propuesto y validado por el Director de Ciberseguridad y Privacidad, garantizando su alineación con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) y las tecnologías colaborativas autorizadas por la organización.

4.6. Política Uso de los Recursos Compartidos en la Red (Carpetas)

Américas Business Process Services, crea recursos compartidos en la red para el intercambio seguro de la información de forma temporal entre procesos operativos y administrativos. Estos recursos compartidos tienen las restricciones y permisos de seguridad, que garantizan que solo los usuarios autorizados por el administrador de la información tendrán acceso a la misma.

La administración de los recursos compartidos está a cargo del proceso de Operación y Monitoreo de Servicios de Tecnología quien realiza la gestión teniendo en cuenta las solicitudes recibidas por los administradores de la información a través de la herramienta de gestión definida por la compañía.

Es responsabilidad de cada uno de los administradores de la información aplicar la política de Clasificación, etiquetado y manejo de la información) e identificar regularmente quienes tienen acceso a la información con el propósito de actualizar los permisos y verificar en compañía del proceso de Operación y Monitoreo de Servicios de Tecnología la implementación de los diferentes controles de seguridad que garanticen su integridad, disponibilidad y confidencialidad de la información.

4.6.1 Objetivos de la política

- Establecer los lineamentos para la utilización de los recursos de red asignados por Américas Business Process Services.
- Implementar el procedimiento (PR TEC 040401 Clasificación, etiquetado y manejo de la información) en cada uno de los recursos compartidos asignados por Américas Business Process Services.
- Identificar y aplicar las buenas prácticas para el tratamiento de la información almacenada en los recursos de red de Américas Business Process Services garantizando su correcta utilización.

4.6.2 Alcance

La presente política de Uso de los Recursos Compartidos en la Red (Carpetas), aplica para todos los empleados de Américas Business Process Services, proveedores, contratistas, clientes y terceras partes que interactúen con sistemas de información de la compañía y de nuestros clientes.

4.6.3 Responsabilidades

La aprobación, mantenimiento y actualización de la Política de Uso de los Recursos Compartidos en la Red (Carpetas) será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier cambio, corrección o actualización del presente documento deberá ser propuesto y validado por el Director de Ciberseguridad y Privacidad, asegurando su coherencia con el modelo de control de accesos, los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) y los principios de mínima exposición de la información.

4.7. Política de Uso de Computadores Portátiles por Terceros

4.7.1. Objetivo

Establecer las condiciones de ingreso y uso de computadores portátiles por parte de terceros en las instalaciones de Américas Business Process Services, con el fin de preservar la seguridad física y lógica de la información, así como los activos tecnológicos de la compañía y sus clientes.

4.7.2. Alcance

Aplica a proveedores, contratistas, visitantes y cualquier tercero que solicite ingresar o utilizar equipos portátiles propios dentro de las instalaciones físicas de ABPS.

4.7.3. Lineamientos

El ingreso y uso de computadores portátiles por parte de terceros, proveedores y colaboradores no está permitido, salvo que exista una justificación operativa válida debidamente documentada.

La solicitud de ingreso deberá realizarse con al menos 24 horas de anticipación, dirigida al área de Ciberseguridad y Privacidad, e incluir:

- Motivo y duración de uso.
- Identificación del tercero responsable.
- Tipo de dispositivo y finalidad de la actividad.

Toda autorización debe ser emitida por Ciberseguridad y Privacidad, con copia a Seguridad Física y al área solicitante.

El ingreso no autorizado de dispositivos portátiles será considerado un incumplimiento a las políticas de seguridad, y podrá conllevar a restricciones de acceso o sanciones contractuales.

En ningún caso se permitirá la conexión de equipos portátiles externos a redes internas sin evaluación y aprobación previa.

4.7.4. Responsabilidad

La verificación del cumplimiento de esta política será responsabilidad de Ciberseguridad y Privacidad en conjunto con el área de Seguridad Física. Las áreas operativas o técnicas que requieran la presencia de terceros deberán asegurar que se cumpla el procedimiento descrito.

4.8. Política de Uso del Correo Electrónico Corporativo

4.8.1. Introducción

El correo electrónico es una herramienta clave para la operación de Américas Business Process Services (ABPS), utilizada para la comunicación con colaboradores, clientes, proveedores y terceros. Su uso intensivo lo convierte también en un canal de riesgo frente a amenazas como phishing, malware, fuga de datos y accesos no autorizados.

ABPS utiliza la plataforma Microsoft 365 como sistema corporativo de mensajería, integrando herramientas de seguridad y colaboración. Esta política contempla tanto el uso de cuentas personales de colaboradores como de cuentas de servicio, las cuales requieren controles adicionales para garantizar su uso seguro y conforme a los principios del SGSI.

4.8.1 Objetivos de la Política

- Garantizar un uso seguro, controlado y conforme a la normatividad del correo electrónico corporativo.
- Establecer **controles específicos para cuentas de servicio**, debido a su criticidad y exposición.
- Minimizar los riesgos asociados a la transmisión y gestión de información mediante correo.

4.8.2 Alcance

Esta política aplica a:

- Todos los colaboradores, proveedores, contratistas, clientes y terceros con cuenta de correo @americasbps.com.
- Toda cuenta de servicio técnico o funcional utilizada por sistemas, bots, automatismos o canales de atención.

4.8.3 Lineamientos Generales

- El correo corporativo debe utilizarse exclusivamente para fines laborales y contractuales.
- Se prohíbe el reenvío automático de correos institucionales a cuentas personales.
- Toda información sensible o confidencial debe ser cifrada o gestionada con controles de clasificación de la información.
- Queda prohibido el uso del correo institucional para:
    - Registro en plataformas ajenas no autorizadas.

- Actividades personales, envío de cadenas, publicidad o contenido irrelevante.
- Toda actividad anómala debe ser reportada a Ciberseguridad y Privacidad de forma inmediata.

4.8.4 Controles para Cuentas de Servicio

Con respecto a las cuentas de servicio se debe evaluar, dependiendo del entorno de utilización, el cumplimiento con los siguientes controles:

Control requerido	Aplicación
Registro y justificación formal	Cada cuenta de servicio debe estar registrada, con propósito, dueño y autorización documentada.
Autenticación robusta	Debe habilitarse MFA si es técnicamente viable.
Bloqueo de acceso interactivo	Las cuentas de servicio no deben permitir ingreso por interfaz de usuario (excepto con aprobación).
Rotación periódica de credenciales	Las contraseñas deben renovarse al menos una vez al año y almacenarse de forma segura.
Restricción de envíos externos	Las cuentas de servicio deben tener filtros para evitar envío a dominios no autorizados.
Monitoreo y alertas de uso anómalo	Toda actividad debe estar sujeta a logs, alertamiento y revisión periódica.
Desactivación automática por inactividad	Se recomienda aplicar políticas de expiración automática si no son utilizadas.
Evaluación de privilegios	Solo deben tener los permisos mínimos necesarios para su función.

4.8.5 Responsabilidad

La gestión, aplicación y actualización de esta política será responsabilidad del área de Ciberseguridad y Privacidad. La creación, monitoreo y control de cuentas de servicio corresponde a las áreas técnicas en coordinación con Ciberseguridad.

4.9. Política de Uso de Computadores Portátiles y Dispositivos Móviles por Empleados

4.9.1. Objetivo

Establecer las directrices para el uso seguro de computadores portátiles y dispositivos móviles por parte de empleados de Américas Business Process Services (ABPS), garantizando la protección de la información, la continuidad de las operaciones y la prevención de accesos no autorizados.

4.9.2. Alcance

Esta política aplica a todo colaborador interno o personal autorizado que utilice equipos portátiles o dispositivos móviles (propios o entregados por la compañía) para acceder, almacenar, procesar o transmitir información de Américas BPS o de sus clientes.

4.9.3. Lineamientos Generales

- Solo se permite el uso de dispositivos corporativos o previamente autorizados por el área de Tecnología, bajo criterios de seguridad definidos por el área de Ciberseguridad y Privacidad.
- Los dispositivos portátiles deben contar con:
  - Cifrado de disco completo (BitLocker o equivalente).
  - Contraseña robusta o autenticación biométrica.
  - Instalación y actualización de software de protección contra malware.
  - Bloqueo automático de pantalla tras un período de inactividad.
  - Acceso controlado mediante credenciales corporativas (Azure AD/Intune u otro).
- Se prohíbe el almacenamiento de información sensible en discos locales sin respaldo ni cifrado.
- Está prohibida la instalación de aplicaciones no autorizadas o la conexión a redes Wi-Fi públicas no seguras sin túneles VPN corporativos.
- Todo dispositivo debe cumplir con las políticas de configuración segura y los estándares de gestión definidos por el área de Tecnología.
- En caso de pérdida o robo del equipo, el colaborador debe reportar el incidente inmediatamente al área de Ciberseguridad y Privacidad para activar los protocolos de respuesta y borrado remoto, si aplica.
- El uso de dispositivos móviles personales (BYOD) deberá estar previamente autorizado y sujeto a políticas de gestión de dispositivos (MDM/Intune) y aceptación de condiciones de uso.

4.9.4. Dispositivos no autorizados

- Se prohíbe expresamente el uso de computadores portátiles, tablets o smartphones personales **sin autorización previa** para ejecutar funciones asociadas a sistemas de información de ABPS.
- El incumplimiento de esta política podrá derivar en medidas disciplinarias, suspensión de accesos o sanciones conforme a la normatividad interna vigente.

4.9.5. Responsabilidades

Rol	Responsabilidad
Empleados	Cumplir esta política y custodiar los dispositivos asignados.
Tecnología	Configurar, entregar, mantener y controlar el inventario de equipos autorizados.
Ciberseguridad y Privacidad	Establecer lineamientos, monitorear cumplimiento y coordinar respuesta ante incidentes.

4.10. Política de Control de Acceso (Físico y Lógico)

4.10.1. Objetivo

Establecer las directrices para el control de acceso físico y lógico a la información y a los recursos tecnológicos utilizados en la prestación de servicios a los clientes de AMÉRICAS BPS, asegurando que únicamente personas autorizadas accedan a los activos de información conforme a sus funciones y bajo el principio del mínimo privilegio.

4.10.2. Alcance

Esta política aplica a todos los sistemas de información, plataformas tecnológicas, estaciones de trabajo, instalaciones físicas y recursos informáticos que gestionen información interna, de proveedores, terceros y de clientes.

4.10.3. Lineamientos

- Definir, documentar y aplicar procedimientos de gestión de identidades (alta, modificación, revocación) tanto físicos como lógicos.
- Aplicar el principio de menor privilegio y necesidad de conocer para la asignación de permisos.
- Garantizar el uso de mecanismos de autenticación robustos para el acceso a plataformas y sistemas (MFA, contraseñas seguras, tarjetas de proximidad, biometría).
- Implementar sistemas de control de acceso físico en instalaciones sensibles (áreas restringidas, cuartos de equipos, salas de redes).
- Establecer límites de tiempo para accesos temporales, contratos o roles rotativos.
- Registrar, monitorear y auditar los accesos tanto físicos como lógicos para detectar usos indebidos o no autorizados.
- Realizar revisiones periódicas de privilegios y accesos asignados, en coordinación con el área de Tecnología y responsables funcionales.
- Mantener mecanismos de control para medios de acceso móviles y remotos, especialmente en esquemas de trabajo híbrido.

4.10.4 Responsabilidad

El área de Tecnología es responsable de la gestión de accesos lógicos; Ciberseguridad y Privacidad supervisa su cumplimiento. La administración de accesos físicos será responsabilidad de Seguridad Física, en coordinación con las áreas responsables del servicio.

4.11. Política de Uso de Internet y Prevención de Fuga de Información

4.11.1. Objetivo

Establecer las condiciones y restricciones bajo las cuales los colaboradores y partes involucradas pueden hacer uso de los recursos de Internet durante la prestación de servicios a clientes de AMÉRICAS BPS, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información y prevenir la fuga de datos.

4.11.2. Alcance

Esta política aplica a todos los usuarios que tengan acceso a Internet desde dispositivos corporativos o redes gestionadas por AMÉRICAS BPS, incluidos empleados, contratistas, proveedores y terceros que participen en la operación de servicios de cliente.

4.11.3. Lineamientos

- El uso de Internet debe limitarse estrictamente a fines laborales o aquellos autorizados por el área responsable del servicio.

- Se prohíbe el acceso a sitios web no relacionados con las funciones del cargo o considerados riesgosos (sitios de entretenimiento, juegos, redes sociales, mensajería, descargas no autorizadas, etc.).
- El acceso a servicios de almacenamiento en la nube, mensajería instantánea o plataformas externas deberá estar previamente aprobado y monitoreado.
- Se debe restringir el uso de navegadores no autorizados, extensiones no verificadas o cualquier software que permita la evasión de controles de navegación.
- Los sistemas de filtrado de contenido, proxy o soluciones de DLP (Prevención de Pérdida de Datos) deben aplicarse para controlar el tráfico web y prevenir la exposición, fuga o extracción no autorizada de datos (alineado con el control 8.23 de la ISO/IEC 27002:2022).
- El monitoreo del uso de Internet será realizado conforme a la normatividad vigente, priorizando el cumplimiento legal y el respeto a la privacidad en el marco contractual.
- Se deberán reportar accesos o comportamientos anómalos detectados relacionados con navegación web, descarga de archivos maliciosos o intentos de exfiltración de información.

4.11.4 Responsabilidad

El área de Tecnología aplicará los controles técnicos. Ciberseguridad y Privacidad definirá las reglas de navegación segura y prevención de fuga de información. Los responsables de proceso asegurarán la aplicación de estas directrices en el servicio al cliente.

4.12. Política General de Relación con Proveedores

4.12.1 Objetivo

Establecer principios generales para la gestión segura de las relaciones con proveedores en Américas Business Process Services (ABPS), asegurando la protección de la información y la continuidad operativa mediante el cumplimiento de buenas prácticas y normas internacionales.

4.12.2 Alcance

Aplica a todos los terceros, aliados estratégicos y contratistas que presten servicios a ABPS, especialmente aquellos que tengan acceso físico o lógico a sistemas, información o procesos críticos.

4.12.3 Lineamientos Generales

- Todo proceso de adquisición o contratación debe contemplar desde su origen la participación del área de Ciberseguridad y Privacidad para validar los riesgos asociados y los requisitos de protección de la información.
- Se deben considerar criterios de seguridad de la información en licitaciones, solicitudes de cotización o propuestas, así como en la formalización de contratos.
- Las cláusulas de seguridad deben incluir aspectos mínimos como: confidencialidad, cumplimiento normativo, derechos de auditoría, notificación de incidentes y tratamiento de información sensible.
- Esta política se complementa con la **Política Específica de Gestión de Proveedores**, la cual detalla los controles exigidos en cada fase del ciclo de vida del proveedor, en cumplimiento de los controles 5.19, 5.20 y 5.21 de la norma ISO/IEC 27001:2022.

4.13.4 Responsabilidades

El área de Compras es responsable de incorporar las cláusulas contractuales de seguridad en los acuerdos con terceros. El área de Ciberseguridad y Privacidad definirá los requisitos de seguridad aplicables y participará en las evaluaciones, revisiones y validaciones de proveedores según su criticidad.

4.13. Política Gestión de Piso

Américas Business Process Services define las directrices para garantizar una sana convivencia, así como el orden que se debe mantener en los puestos y áreas de trabajo por parte de los empleados que conforman las diferentes áreas y campañas al interior de la compañía con el objetivo de garantizar una correcta gestión de piso.

4.13.1 Objetivos de la política

Definir las directrices para la organización, ingreso y permanencia al interior de cada una de las áreas y operaciones de la compañía por parte del personal operativo, administrativo, clientes, terceras partes y trabajadores en misión que ingresen y permanezcan en las instalaciones de Américas Business Process Services.

4.13.2 Alcance

La presente política Gestión de Piso, aplica para todos los empleados, proveedores, contratistas, clientes y terceras partes que ingresen a las diferentes sedes de Américas Business Process Services.

4.13.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Gestión de Piso será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services, en coordinación con las áreas operativas y de soporte que administren ambientes físicos o zonas de trabajo.
Cualquier modificación, corrección o actualización de esta política deberá ser propuesta por el Director de Ciberseguridad y Privacidad, asegurando su alineación con las políticas de control de acceso físico, continuidad operativa y requisitos de seguridad definidos en el SGSI.

4.14. Política Gestión del Riesgo

Américas Business Process Services establece los elementos y el marco general de actuación para la gestión integral de los riesgos identificados en cada uno de sus procesos y campañas, con el propósito de asegurar su sostenibilidad y garantizar la continuidad del negocio frente a los diferentes riesgos a los que se encuentre expuesta, tomando como línea base la Metodología de Valoración del Riesgo definida por la compañía para identificar, analizar, evaluar y tratar de manera adecuada los riesgos que se identifiquen.

4.14.1 Objetivos de la política

- Garantizar la sostenibilidad de Américas Business Process Services y la continuidad del negocio.

- Analizar, evaluar y gestionar los riesgos asociados a los procesos y campañas teniendo en cuenta el impacto en la compañía y la probabilidad de ocurrencia.

4.14.2 Alcance

La presente política de Gestión del Riesgo aplica para todos los empleados de Américas Business Process Services y debe ser implementada en cada proceso y campaña de la compañía.

4.14.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Gestión del Riesgo será responsabilidad del área del proceso de Compliance de Américas Business Process Services, en coordinación con las áreas responsables del tratamiento de riesgos en procesos estratégicos, operativos y tecnológicos.

4.15 Política de Controles Criptográficos

4.15.1. Objetivo

Establecer el uso apropiado de controles criptográficos para proteger la confidencialidad, integridad y autenticidad de la información del cliente en tránsito y en reposo, así como otras técnicas de protección de datos en alineación con los requisitos del control 8.11 de la ISO/IEC 27002:2022.

4.15.2 Alcance

Aplica a todos los datos de clientes almacenados, procesados o transmitidos mediante los sistemas gestionados por AMÉRICAS BPS, incluyendo ambientes locales, móviles o en la nube.

4.15.3 Lineamientos

- Aplicar cifrado robusto a la información sensible o crítica en tránsito y en reposo.
- Utilizar algoritmos y protocolos criptográficos aprobados (ej. AES-256, TLS 1.2 o superior, RSA 2048+, SHA-256, etc.).
- Implementar métodos de protección adicionales como:
  - **Enmascaramiento de datos** para ambientes de prueba, desarrollo o para minimizar exposición innecesaria de datos personales.
  - **Tokenización** en operaciones sensibles como pagos u operaciones de sistemas financieros.
  - **Hashing** para autenticación y validación de integridad.
- Aplicar controles que aseguren el almacenamiento seguro de contraseñas, tokens de sesión y credenciales, conforme al principio de no reversibilidad.
- Gestionar de forma segura el ciclo de vida de claves criptográficas (generación, distribución, almacenamiento, rotación y destrucción).
- Establecer procedimientos para la gestión de certificados digitales y el uso de infraestructura de clave pública (PKI) cuando aplique.
- Documentar las decisiones sobre mecanismos criptográficos aplicados a nivel de arquitectura, incluyendo su propósito y justificación.

- Evaluar periódicamente la eficacia de los controles criptográficos implementados y realizar actualizaciones cuando se detecten debilidades o vulnerabilidades.

4.15.4. Responsabilidad El área de Ciberseguridad y Privacidad será responsable de definir, mantener y supervisar la aplicación de los controles criptográficos y mecanismos de protección complementarios, en conjunto con Tecnología y los dueños de proceso.

4.16. Política Control Código Malicioso

Américas Business Process Services establece las directrices para realizar el aseguramiento de nuestros sistemas de información y de los diferentes dispositivos de red de su propiedad (computadores de escritorio, computadores portátiles, servidores, tabletas, celulares, y todos aquellos dispositivos que permitan la instalación de una herramienta antivirus) conectados a la red de la compañía.

4.16.1 Objetivos de la política

- Garantizar el correcto funcionamiento de nuestros sistemas de información realizando un adecuado aseguramiento de los dispositivos de red (computadores de escritorio, computadores portátiles, servidores, tabletas, celulares, y todos aquellos dispositivos que permitan la instalación de una herramienta antivirus) conectados a la red de Américas Business Process Services.

4.16.2 Alcance

La presente política de Control Código Malicioso aplica para todos dispositivos de red propiedad de la compañía (computadores de escritorio, computadores portátiles, servidores, tabletas, celulares, y todos aquellos dispositivos que permitan la instalación de una herramienta antivirus) que se conecten a la red de Américas Business Process Services.

4.16.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Control de Código Malicioso será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services

4.17. Política Realización de Backup

Américas Business Process Services implementa la presente política con el propósito de contrarrestar las interrupciones que se puedan presentar en los sistemas de información de la compañía, protegiendo sus procesos críticos contra los efectos de fallas importantes y desastres, asegurando su recuperación oportuna, manteniendo la confidencialidad, integridad y disponibilidad de la información nuestra y de nuestros clientes contenida en los repositorios de información de la compañía.

4.17.1 Objetivos de la política

Proteger, garantizar y asegurar la disponibilidad de la información digital almacenada en los diferentes dispositivos suministrados por la compañía, con el objetivo de que se mantenga respaldada y sea fácilmente recuperable en el momento que sea requerido.

4.17.2 Alcance

Esta política aplica para todos los empleados, proveedores, contratistas, clientes y terceras partes que interactúen con sistemas de información de la compañía y almacenen información digital nuestra y de nuestros clientes en los diferentes dispositivos suministrados por Américas Business Process Services (computadores de escritorio, computadores portátiles, servidores, discos duros extraíbles, dispositivos de almacenamiento masivo, unidades compartidas, almacenamiento en la nube (herramienta autorizada por la compañía), buzones de correo electrónico (PST) y en general todos aquellos medios donde se almacene información digital).

4.17.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Realización de Backups será responsabilidad de Tecnología de Américas Business Process Services, en coordinación con el área Ciberseguridad y Privacidad

4.18. Política Contingencia y continuidad del negocio

Américas Business Process Services es críticamente dependiente de la continuidad de sus servicios, cualquier pérdida de acceso a los servidores, sistemas, red de comunicaciones o cualquier otro recurso por un período extendido de tiempo, puede tener un impacto serio en la compañía, esta política define las directrices para asegurar la contingencia de los servicios misionales del negocio y de ser necesario prestar la continuidad solicitada a los procesos que así lo requieran.

4.18.1 Objetivos de la política

- Asegurar la adecuada gestión de los activos informáticos y de información ante un evento de desastre dentro de unos márgenes de tiempo apropiados a las necesidades del negocio de Américas Business Process Services.
- Definir las directrices para asegurar la contingencia y continuidad de los sistemas de información críticos de la compañía.
- Definir las directrices para asegurar la contingencia y continuidad de los procesos críticos que conforman Américas Business Process Services.
- Definir las directrices para asegurar la contingencia y continuidad de los procesos que contractualmente lo requieran.

4.18.2 Alcance

La presente política de contingencia y continuidad del negocio aplica para los sistemas de información que soportan los procesos críticos de Américas Business Process Services en Colombia, para los procesos críticos de la compañía y para aquellos procesos que contractualmente así lo requieran.

4.18.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Continuidad del Negocio será responsabilidad del área de Ciberseguridad y Privacidad, en coordinación con las áreas de Continuidad Operativa y Tecnología, según corresponda.
Cualquier modificación, corrección o actualización del presente documento deberá ser propuesta por el Director de Ciberseguridad y Privacidad, asegurando su alineación con los lineamientos del SGSI, los marcos de gestión de continuidad y los compromisos contractuales y regulatorios aplicables.

4.19. Política Tecnologías Críticas

Las tecnologías críticas son aquellas tecnologías no habituales o que no han sido autorizadas formalmente por Américas Business Process Services y que debido al riesgo que pueden representar, deberán ser autorizadas por el Director de Seguridad de la Información Y Control del Servicio quien aprobará el uso de estas mediante un acta firmada que incluye la justificación para el uso de la tecnología especifica.

4.19.1 Objetivos de la política

Garantizar la correcta utilización de las tecnologías críticas definidas por Américas Business Process Services para el adecuado aseguramiento y funcionamiento de los procesos del negocio que así lo requieran.

4.19.2 Alcance

Esta política aplica para todos los empleados, proveedores, contratistas, clientes y terceras partes que interactúen con sistemas de información de la compañía prestando, recibiendo o gestionando servicios dentro y fuera de las instalaciones de la empresa y mediante la utilización de dispositivos de tecnología critica suministrados por Américas Business Process Services.

4.19.3 Responsabilidades

La aprobación, mantenimiento y actualización de la Política de Tecnologías Críticas será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier modificación, corrección o actualización del presente documento deberá ser propuesta por el Director de Ciberseguridad y Privacidad, asegurando su alineación con los principios del SGSI, las prioridades de continuidad operativa y los lineamientos tecnológicos de la organización.

4.20. Política de Gestión de LOG y Registros de Auditoría

4.20.1. Objetivo

Establecer los lineamientos para la generación, recolección, almacenamiento, protección y revisión de los registros de auditoría (LOGs) generados por los sistemas de información, aplicaciones, plataformas tecnológicas y

dispositivos críticos utilizados en Américas Business Process Services, con el fin de facilitar la detección de actividades no autorizadas, el análisis forense, el cumplimiento normativo y la mejora continua del SGSI.

4.20.2. Alcance

Esta política aplica a todos los sistemas de información, servicios, dispositivos de red, plataformas en la nube, servicios tercerizados (como el SOC), aplicaciones internas, y servicios de infraestructura utilizados para el tratamiento de información institucional o de clientes, que generen eventos relevantes desde el punto de vista de la seguridad.

4.20.3. Lineamientos alineados al control 5.33 de la ISO/IEC 27002:2022

- Todos los sistemas críticos deben estar configurados para generar registros de auditoría que incluyan: accesos exitosos/fallidos, cambios de configuración, uso de privilegios, ejecución de comandos, fallos de autenticación, y eventos críticos de seguridad.
- Los LOGs deben incluir información detallada como: identidad del usuario, fecha y hora con sincronización NTP, dirección IP de origen, acción ejecutada y resultado obtenido.
- Se debe garantizar que los registros no puedan ser modificados, sobrescritos ni eliminados sin trazabilidad. Para ello se aplicarán medidas de protección de integridad, cifrado y control de acceso.
- Se establecerán períodos mínimos de retención, en función de requerimientos legales, contractuales y operacionales. Por defecto, la retención mínima será de 12 meses para sistemas críticos.
- El acceso a los registros estará restringido al personal autorizado, en función de sus responsabilidades dentro del área de Ciberseguridad y Privacidad o del proveedor de servicios gestionados SOC.
- Se utilizarán herramientas SIEM, agentes de auditoría o servicios integrados como por j. Microsoft Sentinel, Syslog, Elastic, etc., para consolidar, analizar y generar alertas sobre eventos sospechosos.
- Deberán ejecutarse revisiones periódicas, manuales o automatizadas, de los registros, con foco en eventos críticos, actividades anómalas o indicadores de compromiso.
- Todo LOG relacionado con eventos de seguridad debe ser utilizable como evidencia digital en investigaciones internas, auditorías o procesos disciplinarios.
- Se deberá garantizar que los sistemas tercerizados también cumplan con estos principios, como parte de los contratos y acuerdos de nivel de servicio.

4.20.4. Responsabilidades

El área de Ciberseguridad y Privacidad es responsable de definir los eventos auditables, supervisar la integridad, acceso y revisión de los registros, y garantizar su disponibilidad como evidencia en investigaciones y auditorías.

El área de Tecnología debe configurar y mantener los sistemas para la generación, retención y protección de LOGs, asegurando su disponibilidad y sincronización horaria.

Cuando los registros sean gestionados por un proveedor externo (SOC), este deberá recolectar, conservar y correlacionar los eventos conforme a los acuerdos vigentes, notificando oportunamente hallazgos y entregando reportes a Ciberseguridad y Privacidad.

4.21. Política Gestión de Vulnerabilidades

Américas Business Process Services define las directrices para llevar a cabo la gestión de vulnerabilidades técnicas como proceso continuo para asegurar el adecuado funcionamiento de cada uno de los dispositivos que forman parte de la plataforma tecnológica con el propósito de asegurar el adecuado funcionamiento y gestión de las operaciones del negocio.

4.21.1 Objetivos de la política

Definir las directrices para llevar a cabo la identificación, seguimiento, control y atención de las vulnerabilidades técnicas identificadas mediante la realización de pruebas de ethical hacking y análisis de vulnerabilidades internas y externas ejecutados en los diferentes sistemas de información, dispositivos conectados a la red y plataformas tecnológicas de Américas Business Process Services, con el propósito de mantener un aseguramiento adecuado de la plataforma tecnológica, mitigando siempre que sea posible los diferentes riesgos asociados a las vulnerabilidades identificadas.

4.21.2 Alcance

Esta política aplica para todos los dispositivos de la plataforma tecnológica de Américas Business Process Services.

4.21.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Gestión de Vulnerabilidades será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

Cualquier modificación, corrección o actualización del presente documento deberá ser propuesta por el Director de Ciberseguridad y Privacidad, garantizando su coherencia con el modelo de gestión de riesgos, las obligaciones normativas y los controles definidos en el Sistema de Gestión de Seguridad de la Información (SGSI).

4.22. Política Despliegue de Actualizaciones

Américas Business Process Services define las directrices para llevar a cabo la adecuada actualización e instalación de actualizaciones y parches de seguridad para cada uno de los dispositivos que forman parte de la infraestructura tecnológica que soporta las operaciones del negocio, con el objetivo de asegurar una adecuada prestación de los servicios.

4.22.1 Objetivos de la política

Llevar a cabo la adecuada instalación, actualización y despliegue de las diferentes actualizaciones y parches de seguridad requeridos para el adecuado funcionamiento y aseguramiento de cada uno de los dispositivos que conforman la plataforma tecnológica de Américas Business Process Services.

4.22.2 Alcance

Esta política aplica para llevar a cabo el despliegue de actualizaciones y parches de seguridad de cada uno de los dispositivos y sistemas de información que forman parte de la plataforma tecnológica que soporta las operaciones del negocio de Américas Business Process Services.

4.22.3 Responsabilidades

La aprobación, revisión y actualización de la Política de Despliegue de Actualizaciones será responsabilidad del área de Ciberseguridad y Privacidad, en coordinación con el área de Tecnología para la ejecución técnica y seguimiento de los lineamientos definidos.

Cualquier cambio, corrección o actualización del presente documento deberá ser propuesto por el Director de Ciberseguridad y Privacidad, garantizando su alineación con los controles del SGSI, las mejores prácticas de gestión de parches y actualizaciones, y los requisitos regulatorios aplicables.

4.23. Política Gestión de Usuarios y Contraseñas

4.23.1. Objetivo

Establecer los lineamientos para la **gestión segura de identidades, accesos y credenciales** dentro del entorno de datos del titular de tarjeta (CDE) de Américas Business Process Services, garantizando la protección de los activos de información asociados al procesamiento, almacenamiento y transmisión de datos de tarjetas, conforme a los controles de la **ISO/IEC 27001:2022** y los requisitos de **PCI DSS v4.0**.

4.23.2. Alcance

Esta política aplica a todos los **usuarios, cuentas, servicios y componentes tecnológicos** que interactúan con sistemas dentro del CDE, incluyendo personal técnico, usuarios administrativos, proveedores, cuentas de servicio y terceros autorizados.

4.23.3. Lineamientos Generales

- Todo acceso al CDE debe estar basado en el principio de mínimo privilegio y necesidad de conocer (*need to know*), conforme al control 8.2 de la ISO/IEC 27002:2022 y PCI DSS 4.0 requisito 7.2.1.
- Se deben implementar mecanismos de autenticación multifactor (MFA) para todo acceso remoto y para todos los accesos administrativos e individuales al CDE (PCI DSS 4.0 requisito 8.4.2).
- Las cuentas de usuario deben ser únicas, personales y no compartidas. El uso de cuentas genéricas o por grupos está prohibido.
- Toda creación, modificación o eliminación de cuentas debe estar documentada, justificada y aprobada por el responsable del sistema o del servicio (ISO 27002:2022 control 8.2.4).

- El registro de usuarios debe mantenerse actualizado, y se deben realizar revisiones periódicas (mínimo trimestral) para identificar cuentas inactivas o no autorizadas (PCI DSS 4.0 requisito 7.2.4).

4.23.3. Responsabilidades

La gestión de identidades y credenciales dentro del CDE será responsabilidad conjunta del área de Ciberseguridad y Privacidad y del área de Tecnología, quienes deberán implementar, monitorear y mejorar continuamente los controles establecidos.

4.24. Política de Continuidad de la Seguridad de la Información

4.24.1. Objetivo

Establecer los lineamientos para garantizar la continuidad de la seguridad de la información durante eventos de interrupción no planificada, afectación a servicios críticos, incidentes de seguridad o desastres que puedan comprometer la confidencialidad, integridad o disponibilidad de la información gestionada por AMÉRICAS BPS para sus clientes.

4.24.2. Alcance

Esta política aplica a todos los servicios prestados por AMÉRICAS BPS que gestionen información del cliente, así como a los sistemas, personas, procesos y proveedores que intervienen en la continuidad del servicio y la protección de los activos de información durante situaciones de contingencia.

4.24.3. Lineamientos

- Integrar la seguridad de la información en los planes de continuidad del negocio y recuperación ante desastres (BCP/DRP).
- Identificar procesos críticos y sus activos de información asociados, estableciendo medidas para mantener su operación segura durante eventos disruptivos.
- Evaluar riesgos de seguridad asociados a escenarios de interrupción y establecer controles preventivos y correctivos.
- Mantener respaldos seguros y actualizados de la información crítica, con procedimientos documentados de restauración.
- Realizar pruebas periódicas (al menos una vez al año) de los planes de continuidad que incluyan validaciones de seguridad de la información.
- Asegurar que los proveedores o terceros críticos cuenten con planes de continuidad compatibles y procedimientos de seguridad alineados con los niveles acordados contractualmente.
- Mantener comunicación efectiva con el cliente ante incidentes que afecten la seguridad o continuidad del servicio, conforme a los Acuerdos de Nivel de Servicio (ANS).
- Documentar lecciones aprendidas y ejecutar planes de mejora como resultado de pruebas o activaciones reales del plan.

4.25. Política Desarrollo Seguro de Aplicaciones

Las fallas de seguridad en el software pueden introducirse en cualquiera de las etapas del ciclo de desarrollo del software, derivados de:

- Implantación del software de forma inapropiada.
- Introducción de fallas durante el mantenimiento o actualización del producto.
- Utilizar prácticas débiles de codificación que introduzcan vulnerabilidades desde el punto de vista técnico.

En esta política se enumerarán los principios de seguridad, prácticas o directrices que deben ser tenidas en cuenta a la hora de desarrollar una aplicación de forma segura, con el fin de garantizar la seguridad de la información para el entorno de datos de titulares de tarjeta (CDE) y en general de Américas Business Process Services.

4.25.1 Objetivos de la política

Definir las directrices para llevar a cabo la elaboración de aplicaciones seguras al interior de Américas Business Process Services mediante la aplicación de diferentes estándares, normas, controles y directrices definidas de acuerdo a las buenas prácticas adoptadas en esta política.

4.25.2 Alcance

Definir los principios y directrices que Americas Business Process Services, tendrá en cuenta a la hora de desarrollar una aplicación para que esta cumpla con las normativas de seguridad establecidas por el entorno y por la compañía.

4.25.3 Responsabilidades

La responsabilidad directa sobre la aprobación, revisión y actualización de la Política de Desarrollo Seguro de Aplicaciones recae sobre el área de Desarrollo de Américas Business Process Services, como responsable de asegurar que los procesos de codificación, diseño, prueba y liberación de aplicaciones cumplan con los requisitos de seguridad definidos por la organización.

Cualquier modificación, corrección o actualización del presente documento deberá ser coordinada por el área de Desarrollo, con la validación y acompañamiento del área de Ciberseguridad y Privacidad, a fin de garantizar su alineación con el SGSI, las buenas prácticas de codificación segura (OWASP, NIST, ISO 27002) y los estándares regulatorios aplicables.

4.26. Política de Seguridad en servicios en la nube

Con el fin de garantizar la seguridad de la información en los servicios contratados o soportados mediante plataformas o infraestructuras de computación en la nube, AMÉRICAS BPS establece los siguientes lineamientos:

4.26.1. Objetivo

Establecer directrices que aseguren la protección de la información en entornos de servicios en la nube contratados por o en nombre del cliente, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y privacidad.

4.26.2 Alcance

Aplica a todos los servicios que involucren procesamiento, almacenamiento o transmisión de información del cliente a través de plataformas en la nube, gestionadas directamente por AMÉRICAS BPS o por proveedores contratados.

4.26.3 Lineamientos

- Identificar y documentar claramente las responsabilidades de seguridad entre AMÉRICAS BPS, el cliente y el proveedor del servicio en la nube (modelo de responsabilidad compartida).
- Asegurar la aplicación de controles de acceso lógico bajo el principio de mínimo privilegio.
- Garantizar el cifrado de datos en tránsito y en reposo mediante algoritmos y estándares robustos.
- Implementar mecanismos de monitoreo, generación de registros (logs) y detección de eventos de seguridad sobre los entornos cloud.
- Establecer procedimientos documentados para la devolución, transferencia o eliminación segura de la información al término del servicio.
- Exigir a los proveedores de servicios en la nube que mantengan planes de continuidad del negocio y recuperación ante desastres con niveles de servicio compatibles con los acuerdos establecidos con el cliente.
- Incluir escenarios de afectación en la nube dentro del proceso de gestión de incidentes y reportes de eventos de seguridad.
- Validar que los servicios contratados cumplan con los requisitos legales y regulatorios aplicables, especialmente en materia de protección de datos personales Ley 1581, RGPD, Ley 23001 y otras aplicables.

4.26.4 Responsabilidad

La implementación, seguimiento y verificación de estos lineamientos será responsabilidad del área de Ciberseguridad y Privacidad de AMÉRICAS BPS, en conjunto con las áreas técnicas involucradas en la provisión del servicio al cliente.

4.27.1. Política de Evaluación de Riesgos en Proyectos y Servicios

4.27.2. Objetivo

Establecer directrices para la identificación, análisis y tratamiento de riesgos de seguridad de la información asociados a nuevos proyectos, servicios, tecnologías o cambios significativos en los servicios prestados a los clientes de AMÉRICAS BPS.

4.27.3 Alcance

Aplica a todos los proyectos, iniciativas o cambios operacionales, tecnológicos, regulatorios o contractuales que puedan impactar la seguridad de la información de los clientes gestionada por AMÉRICAS BPS.

4.27.4 Lineamientos

Toda nueva iniciativa deberá incluir una evaluación de riesgos de seguridad de la información antes de su implementación o puesta en producción.

Los riesgos identificados deben ser valorados con base en metodologías aprobadas por AMÉRICAS BPS -ISO 27005, ISO 31000-, considerando el contexto del cliente y el entorno operativo.

El resultado de la evaluación de riesgos debe ser aprobado por el área de Ciberseguridad y Privacidad antes de la activación del proyecto o servicio.

En caso de identificarse riesgos no mitigados, deberán establecerse planes de tratamiento con responsables, plazos y controles asociados.

Se deberán ejecutar evaluaciones adicionales cuando existan cambios significativos que modifiquen el alcance, tecnología o contexto del servicio.

Las evidencias de la evaluación de riesgos deberán estar disponibles para auditoría interna o externa.

La gestión de riesgos debe ser trazable y estar integrada con el Sistema de Gestión de Seguridad de la Información (SGSI).

4.27.5. Responsabilidad

El líder del proyecto o proceso será responsable de iniciar la evaluación de riesgos. El área de Ciberseguridad y Privacidad será responsable de su validación, control y documentación conforme al SGSI de AMÉRICAS BPS.

4.28. Política de Seguridad en el Ciclo de Vida de los Sistemas

4.28.1. Objetivo

Asegurar que los principios de seguridad de la información sean aplicados en todas las fases del ciclo de vida de los sistemas que gestionan información del cliente, desde el diseño hasta el retiro.

4.28.2. Alcance

Aplica a todos los sistemas desarrollados o adquiridos por AMÉRICAS BPS que gestionen datos de clientes o que formen parte de los servicios contratados.

4.28.3. Lineamientos

Aplicar principios de seguridad desde el diseño (security by design) y durante todo el desarrollo o adquisición de sistemas.

- Incluir requisitos de seguridad de la información en especificaciones funcionales y técnicas.
- Evaluar los riesgos de seguridad antes del paso a producción de sistemas nuevos o modificados.
- Realizar pruebas de seguridad, revisiones de código y análisis de vulnerabilidades antes de la implementación.
- Gestionar el retiro seguro de sistemas asegurando el borrado o traspaso de datos de manera controlada.

4.28.4. Responsabilidad

Las áreas de Tecnología, Desarrollo y Ciberseguridad serán responsables de garantizar la aplicación de estos lineamientos en los sistemas gestionados para los clientes.

4.29. Política de Gestión de Configuraciones

4.29.1. Objetivo Garantizar que las configuraciones de los sistemas que gestionan información de los clientes se mantengan controladas, seguras y auditables durante su operación.

4.29.2. Alcance Aplica a toda la infraestructura tecnológica, plataformas, aplicaciones y servicios gestionados por AMÉRICAS BPS que intervienen en el procesamiento de información de clientes.

4.29.3. Lineamientos

- Mantener inventarios actualizados de configuraciones autorizadas (baseline) para todos los componentes críticos.
- Aplicar configuraciones seguras siguiendo estándares reconocidos (CIS Benchmarks, NIST, etc.).
- Controlar los cambios en configuraciones a través de procedimientos formales de gestión del cambio.
- Realizar auditorías periódicas para verificar la conformidad con las configuraciones establecidas.
- Registrar, documentar y revisar cualquier desviación de las configuraciones aprobadas.

4.29.4. Responsabilidad El área de Tecnología será responsable de aplicar la configuración técnica, y el área de Ciberseguridad supervisará el cumplimiento de las políticas de configuración.

4.30. Política de Clasificación y Tratamiento de Activos de Información

4.30.1. Objetivo Establecer criterios para identificar, clasificar, proteger y gestionar los activos de información utilizados en la prestación de servicios a clientes de AMÉRICAS BPS, de acuerdo con su nivel de criticidad, sensibilidad y valor para el negocio.

4.30.2. Alcance Aplica a todos los activos de información tangibles e intangibles, incluyendo datos, documentos, sistemas, bases de datos, dispositivos, software, medios electrónicos y soportes físicos gestionados por AMÉRICAS BPS en el marco de los servicios contratados.

4.30.3 Lineamientos

- Identificar y documentar todos los activos de información que soportan procesos relacionados con clientes.
- Asignar un propietario responsable por cada activo, quien deberá asegurar su adecuado uso, protección y actualización.
- Clasificar los activos según su nivel de confidencialidad, criticidad, sensibilidad y requerimientos legales o contractuales (ej. Pública, Interna, Restringida, Confidencial).
- Aplicar criterios de clasificación basados en la Ley 1581 de 2012 y el Reglamento General de Protección de Datos de la Unión Europea (GDPR), diferenciando:
    - **Datos personales públicos:** libre acceso (según Ley 1581).
    - **Datos personales privados:** requieren autorización para su tratamiento.
    - **Datos personales sensibles:** salud, orientación política o religiosa, datos biométricos, etc., requieren medidas reforzadas de seguridad.
    - **Datos personales especiales (GDPR):** categorías especiales que requieren base legal explícita para su tratamiento.
- Etiquetar los activos según su clasificación y aplicar controles de protección acordes a dicha categoría.
- Definir procedimientos específicos para el manejo, almacenamiento, transmisión, respaldo y eliminación segura de cada tipo de activo, con base en su clasificación.
- Realizar revisiones periódicas de la clasificación y tratamiento de activos como parte del ciclo de mejora continua del SGSI.
- Asegurar que los activos de los clientes sean tratados conforme a los principios contractuales, regulatorios y de confidencialidad establecidos.

4.30.4 Responsabilidad El área de Tecnología será responsable de mantener el inventario de activos actualizado; Ciberseguridad y Privacidad definirá los lineamientos de clasificación, y los responsables de proceso asegurarán la protección de los activos bajo su gestión.

4.31. Política de Gestión de Servicios SOC Tercerizados e Inteligencia de Amenazas (Control 5.7)

4.31.1 Objetivo Establecer los lineamientos para la gestión de los servicios tercerizados de Centro de Operaciones de Seguridad (SOC) y la integración de capacidades de inteligencia de amenazas, con el fin de garantizar una

postura proactiva frente a riesgos cibernéticos, y asegurar la detección, respuesta y aprendizaje frente a amenazas emergentes, en cumplimiento del control 5.7 de la ISO/IEC 27002:2022.

4.31.2 Alcance Esta política aplica a todos los servicios prestados por proveedores SOC para ABPS, así como al tratamiento de inteligencia técnica, contextual y operativa derivada de fuentes internas y externas, aplicable a los activos críticos y medios definidos por la organización.

4.31.3 Lineamientos

- El proveedor SOC deberá operar bajo un modelo híbrido, con monitoreo continuo, escalamiento oportuno, soporte a la respuesta y alineación con el procedimiento PR32 CYP 0501.
- Se exigirá al SOC la administración de herramientas SIEM/SOAR integradas con plataformas de Threat Intelligence (ej. OpenCTI, Kaspersky TIP) para la detección avanzada de amenazas.
- El proveedor debe recolectar, enriquecer, correlacionar y escalar indicadores de compromiso (IoC) y técnicas, tácticas y procedimientos (TTP) conforme al marco MITRE ATT&CK.
- Se deberán aplicar reglas de correlación, análisis de campañas activas, y priorización de amenazas conforme al contexto de ABPS.
- Los incidentes deben ser gestionados bajo SLAs definidos, con trazabilidad, clasificación y participación del CSIRT según criticidad.
- Las fases de gestión (evaluación, contención, reanudación, recuperación y retorno) deberán estar integradas con el modelo de continuidad del negocio y las capacidades del proveedor.
- El SOC deberá participar en ejercicios de simulación y entregar informes mensuales de amenazas emergentes, tendencias y efectividad de controles.
- Los hallazgos relevantes deben retroalimentar el SIEM/SOAR y ser incluidos en los procesos de mejora continua del SGSI.

4.31.4 Inteligencia de Amenazas (cumplimiento control 5.7)

- La inteligencia de amenazas deberá ser procesada desde fuentes OSINT, CERT, feeds comerciales y alianzas del sector.
- Se documentarán campañas dirigidas al sector BPO, técnicas utilizadas, vectores observados y actores asociados.
- Se generarán alertas preventivas con recomendaciones técnicas, priorización de activos y ajustes de controles.
- La inteligencia se integrará en decisiones tácticas y estratégicas del SGSI, con métricas de desempeño como MTTI, % de amenazas anticipadas, y cobertura de fuentes.

4.31.5 Responsabilidad

El área de Ciberseguridad y Privacidad será responsable de la supervisión del proveedor SOC, la validación de capacidades de inteligencia y la integración de la información en los procesos de gestión de incidentes, mejora continua y cumplimiento regulatorio.

4.32 Política de Protección de Información en Dispositivos de Usuario Final

4.32.1 Objetivo

Establecer los lineamientos para proteger la información que es accedida, procesada o almacenada en dispositivos de usuario final utilizados por colaboradores, contratistas o terceros autorizados de Américas Business Process Services

4.32.2 Alcance

Esta política aplica a todos los dispositivos portátiles, estaciones de trabajo, dispositivos móviles, terminales conectadas, y otros equipos utilizados para interactuar con activos de información de ABPS, tanto corporativos como personales previamente autorizados.

4.32.3 Lineamientos Generales

- Todo dispositivo que acceda a información clasificada como confidencial, restringida o sensible deberá contar con controles técnicos para evitar su exposición, pérdida o uso no autorizado.
- Se deben aplicar las siguientes medidas mínimas:
    - Cifrado de disco completo o de particiones sensibles.
    - Autenticación robusta (contraseña segura, biometría o doble factor).
    - Bloqueo automático de sesión por inactividad.
    - Actualización periódica del sistema operativo y software.
    - Instalación de software antimalware y protección de endpoint.
    - Desactivación de puertos o funciones innecesarias (ej. USB, Bluetooth).
- Los dispositivos deben estar configurados de acuerdo con los lineamientos de seguridad definidos por el área de Tecnología y validados por Ciberseguridad y Privacidad.
- No está permitido el almacenamiento local de información confidencial, a menos que se cuente con autorización expresa y controles de cifrado activos.
- Los accesos remotos deben realizarse exclusivamente a través de canales seguros (VPN, conexiones cifradas).
- El uso de dispositivos personales está restringido y debe cumplir con las políticas de gestión de dispositivos móviles y uso aceptable de activos.

4.32.4 Responsabilidades

- Los usuarios son responsables de proteger adecuadamente los dispositivos que se les asignen o autoricen, así como de reportar cualquier pérdida, robo o anomalía.
- Ciberseguridad y Privacidad establecerá los controles técnicos y requisitos mínimos de protección, realizará auditorías y monitoreo de cumplimiento.
- El área de Tecnología será responsable de aplicar la configuración segura, el soporte y la gestión del ciclo de vida de los dispositivos.

5. Cumplimiento

El incumplimiento de este Manual, podrá derivar en la restricción de accesos, medidas disciplinarias o acciones contractuales conforme a lo definido en los procedimientos internos de ABPS.

6. Revisión

Esta política debe ser revisada por lo menos una vez al año

Control de Cambios			
Versión	Descripción del cambio	Elaboró	Aprobó
00 25/04/2019	Creación del documento.	Richard Mauricio Sanabria Bello Director Seguridad de la información yControl del Servicio	Luzmila Cruz Gaitán Gerente General
01 31/07/2020	Modificación de código del documento	Diego Alexander Pérez Rodríguez Director de Seguridad de la Información	Luzmila Cruz Gaitán Gerente General
02 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 MA3 SGI 05, nuevo código del documento MA01 CYP 0501. Se actualiza imagen corporativa.	Adriana Paola Diaz Santos Coordinacion del SGI	Adriana Paola Diaz Santos Coordinacion del SGI
03 15/04/2025	Se incluyen requisitos de seguridad en la nube, modificación política de mensajería instantánea. Inclusión de la política de continuidad de seguridad de la información.	Rubén Alexander Rico Director de ciberseguridad y privacidad	Rubén Alexander Rico Director de ciberseguridad y privacidad