americas
BPS Outsourcing Transformation

Manual de Política de Seguridad de la Información Americas Business Process Services

Tabla de contenido

1. 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.

2. Alcance

El presente Manual de Seguridad de la Información de Américas Business Process Services aplica a todos los colaboradores, contratistas, proveedores, terceros y demás partes interesadas que interactúen con los activos de información, sistemas de información, infraestructura tecnológica y datos de la compañía o de sus clientes, en el desarrollo de sus funciones o en la prestación de servicios para la organización.

3. 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.

4. Desarrollo del Documento

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.

4.1.1. Objetivos del SGSI

- ✓ Fortalecer la confianza de las partes interesadas mediante la adecuada protección de la información gestionada por la organización.
- ✓ Establecer directrices y controles que garanticen la confidencialidad, integridad y disponibilidad de los activos de información de Américas Business Process Services y de sus clientes.
- ✓ Asegurar la ciberseguridad y el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables a la protección de la información.

4.1.2. Alcance

La presente política de seguridad de la información aplica a los procesos relacionados con la comercialización, administración, diseño, implementación y gestión de operaciones en la prestación de servicios BPO de Américas Business Process Services, así como a los colaboradores, contratistas, proveedores y terceros que participen en dichos procesos, con el propósito de garantizar la confidencialidad, integridad, disponibilidad, procesamiento y tratamiento seguro de la información.

4.1.3. 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

4.2. 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.

4.2.1. 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.

4.2.2. 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.

4.2.3. 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 y validado por el área de Ciberseguridad y Privacidad, y aprobado por la instancia correspondiente, asegurando su alineación con los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI).

Los administradores de sistemas y redes deberán implementar los controles tecnológicos necesarios para el cumplimiento de la política de gestión de contraseñas.
Todos los colaboradores, proveedores, contratistas y terceros con acceso a los sistemas de información de Américas Business Process Services deberán cumplir con los lineamientos definidos para el uso y protección de credenciales de acceso.

4.3. Política Escritorio Despejado Y Pantalla Despejada

Américas Business Process Services establece la política de Escritorio Despejado y Pantalla Despejada con el fin de reducir los riesgos de acceso no autorizado, pérdida, alteración o exposición de la información durante y fuera de las horas normales de trabajo, promoviendo el adecuado manejo y protección de la información en los espacios de trabajo físicos y digitales.

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 lineamientos y procedimientos establecidos para garantizar la seguridad de la información. El incumplimiento de estas disposiciones podrá ser gestionado de acuerdo con los procedimientos disciplinarios definidos por la organización...

4.3.1. 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.

4.3.2. 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.

4.3.3. Responsabilidades

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

La aprobación del presente documento será realizada por la instancia de gobierno correspondiente, de acuerdo con el marco de gestión del Sistema de Gestión de Seguridad de la Información (SGSI).

Los líderes de proceso y responsables de área deberán promover el cumplimiento de la presente política dentro de sus equipos de trabajo y apoyar las actividades de sensibilización relacionadas con la protección de la información.

Todos los colaboradores, proveedores, contratistas y terceros que tengan acceso a la información o a los recursos tecnológicos de Américas Business Process Services deberán cumplir con los lineamientos establecidos en esta política, asegurando la adecuada protección de la información en los espacios de trabajo físicos y digitales.

4.4. Política Uso de la mensajería instantánea

El uso de plataformas de mensajería instantánea y servicios interactivos dentro de Américas Business Process Services se encuentra regulado por las directrices de seguridad de la información definidas por el área de Ciberseguridad y Privacidad, con el fin de garantizar el uso seguro de los canales de comunicación y la protección de la información corporativa y de los clientes.

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.

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.

4.4.1. 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.

4.4.2. Alcance

La presente política de uso de la mensajería instantánea aplica para todos los colaboradores de Américas Business Process Services, así como para proveedores, contratistas, clientes y terceros que utilicen los recursos tecnológicos, plataformas de comunicación o sistemas de información de la organización o de sus clientes.

4.4.3. 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.

La aprobación del presente documento será realizada por la instancia de gobierno correspondiente dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Los líderes de proceso deberán promover el uso adecuado de las plataformas de comunicación autorizadas y asegurar que sus equipos de trabajo conozcan y cumplan los lineamientos establecidos en la presente política.

Todos los colaboradores, proveedores, contratistas y terceros que utilicen plataformas de mensajería corporativa deberán hacer uso de estas de acuerdo con las directrices establecidas por la organización, evitando el uso de herramientas no autorizadas para el intercambio de información corporativa o de clientes.

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

Américas Business Process Services dispone de recursos compartidos en la red con el fin de facilitar el intercambio y almacenamiento controlado de información entre procesos operativos y administrativos, garantizando que el acceso a dichos recursos se otorgue únicamente a usuarios autorizados mediante la aplicación de controles de seguridad y gestión de permisos.

La administración de los recursos compartidos está a cargo del proceso de Operaciones IT, quien realizará la gestión de creación, modificación o eliminación de accesos con base en las solicitudes realizadas por los administradores de la información, de acuerdo con los procedimientos y herramientas de gestión definidos por la organización.

Es responsabilidad de los administradores de la información aplicar los lineamientos definidos en la política de clasificación, etiquetado y manejo de la información, así como revisar periódicamente los accesos otorgados a los recursos compartidos con el fin de validar su vigencia y actualizar los permisos cuando sea necesario.

4.5.1. Objetivos de la política

- ✓ Establecer los lineamentos para la utilización de los recursos de red asignados por Américas Business Process Services.
- ✓ Promover la correcta aplicación de los lineamientos de clasificación, etiquetado y manejo de la información en los recursos compartidos de la organización.
- ✓ 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

4.5.2. Alcance

La presente política de uso de los recursos compartidos en la red aplica para todos los colaboradores de Américas Business Process Services, así como para proveedores, contratistas, clientes y terceros que utilicen o tengan acceso a los recursos tecnológicos y sistemas de información de la organización o de sus clientes

4.5.3. Responsabilidades

- ✓ La elaboración, mantenimiento y revisión de la Política de Uso de los Recursos Compartidos en la Red será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.
- ✓ La aprobación del presente documento será realizada por la instancia de gobierno correspondiente dentro del Sistema de Gestión de Seguridad de la Información (SGSI).
- ✓ El proceso de Operaciones It será responsable de administrar los recursos compartidos y gestionar la asignación, modificación o revocación de accesos de acuerdo con las solicitudes debidamente autorizadas.
- ✓ Los administradores o responsables de la información deberán definir y revisar periódicamente los permisos de acceso a los recursos compartidos bajo su responsabilidad, garantizando que estos se otorguen conforme al principio de mínimo privilegio y a los lineamientos de clasificación de la información.

4.6. Política de Uso de Computadores Portátiles por Terceros

4.6.1. 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.

4.6.2. Alcance

La presente política aplica a proveedores, contratistas, visitantes, colaboradores y cualquier tercero que solicite ingresar o utilizar computadores portátiles propios dentro de las instalaciones físicas de Américas Business Process Services.

4.6.3. Lineamientos

El ingreso y uso de computadores portátiles propios por parte de terceros, proveedores o colaboradores dentro de las instalaciones de Américas Business Process Services no estará permitido, salvo que exista una justificación operativa debidamente documentada y autorizada por el área de Ciberseguridad y Privacidad

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 Gestión Administrativa 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.

4.6.4. Responsabilidad

La verificación del cumplimiento de esta política será responsabilidad del proceso de Ciberseguridad y Privacidad en conjunto con el proceso Gestión Administrativa.

Las áreas operativas o técnicas que requieran la presencia de terceros deberán gestionar la solicitud correspondiente y asegurar que se cumplan los lineamientos establecidos para el ingreso y uso de equipos portátiles dentro de las instalaciones de la organización.

Los terceros autorizados deberán cumplir las condiciones establecidas para el uso de dispositivos dentro de las instalaciones de Américas Business Process Services.

4.7. Política de Uso del Correo Electrónico Corporativo

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.

4.7.1. 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.

4.7.2. Alcance

Esta política aplica a todos los colaboradores, proveedores, contratistas y terceros que tengan asignada una cuenta de correo corporativo de Américas Business Process Services.
Toda cuenta de servicio técnico o funcional utilizada por sistemas, bots, automatismos o canales de atención que utilicen la plataforma de correo institucional.

4.7.3. 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.

4.7.4. 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 credenciales deberán renovarse periódicamente de acuerdo con los lineamientos de gestión de identidades definidos por la organización.
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.

4.7.5. Responsabilidad

La elaboración, mantenimiento y revisión de la Política de Uso del Correo Electrónico Corporativo será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.

El proceso de tecnología será responsable de la administración técnica de la plataforma de correo, incluyendo la creación, configuración, monitoreo y control de las cuentas corporativas y de servicio, en coordinación con el proceso de Ciberseguridad.

Todos los colaboradores, proveedores, contratistas y terceros que tengan acceso al correo electrónico corporativo deberán utilizarlo conforme a los lineamientos establecidos en la presente política y reportar cualquier actividad sospechosa o incidente de seguridad.

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

4.8.1. Objetivo

Establecer las directrices para el uso seguro de computadores portátiles y dispositivos móviles por parte de los colaboradores de Américas Business Process Services (ABPS), garantizando la protección de la información, la continuidad de las operaciones y la prevención de accesos no autorizados a los recursos tecnológicos de la organización y de sus clientes.

4.8.2. Alcance

Esta política aplica a todos los colaboradores y personal autorizado que utilicen computadores portátiles o dispositivos móviles (propios o suministrados por la compañía) para acceder, almacenar, procesar o transmitir información de Américas Business Process Services o de sus clientes.

4.8.3. Lineamientos Generales

- Solo se permite el uso de dispositivos corporativos o previamente autorizados por el área de Ciberseguridad y Privacidad.
- Los dispositivos portátiles deben contar con:

- Cifrado de disco completo (BitLocker o equivalente).
- Ccontraseña robusta y/o mecanismos de autenticación fuerte, tales como autenticación biométrica cuando el dispositivo lo permita.
- Instalación y actualización de software de protección contra malware.
- Bloqueo automático de pantalla tras un período de inactividad.
- Acceso controlado mediante credenciales corporativas.

- 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 proceso de Tecnología y Ciberseguridad y Privacidad.
- 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.

4.8.4. 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.

4.8.5. Responsabilidades

- Los colaboradores deben cumplir con los lineamientos establecidos en la presente política, hacer uso adecuado de los dispositivos asignados y garantizar la custodia de los mismos. Asimismo, deben reportar de manera inmediata al área de Ciberseguridad y Privacidad cualquier incidente relacionado con pérdida, robo, acceso no autorizado o uso indebido del dispositivo.
- Tecnología: Gestionar la configuración, entrega, mantenimiento y control de inventario de los computadores portátiles y dispositivos móviles corporativos, garantizando que estos cumplan con los estándares de seguridad definidos por la organización.
- Ciberseguridad y Privacidad: Definir los lineamientos de seguridad aplicables a los dispositivos, monitorear el cumplimiento de esta política, apoyar en la gestión de incidentes de seguridad asociados a los equipos y coordinar las acciones de mitigación cuando sea necesario.

4.9. Política de Control de Acceso

4.9.1. 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.

4.9.2. 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.

4.9.3. 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, PAM, 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.

4.9.4. Responsabilidad

- Tecnología/Operaciones IT: Administrar y gestionar los accesos lógicos a los sistemas de información, incluyendo la creación, modificación y revocación de usuarios y privilegios. Asimismo, gestionar los accesos físicos a los cuartos de comunicaciones, salas técnicas y data center, garantizando que solo el personal autorizado tenga acceso a estos espacios.
- Ciberseguridad y Privacidad: Definir los lineamientos de control de acceso, supervisar el cumplimiento de esta política, promover revisiones periódicas de privilegios y apoyar la investigación de incidentes relacionados con accesos indebidos.
- Gestión Administrativa: Administrar y controlar los accesos físicos a las instalaciones de la compañía, incluyendo la asignación y control de credenciales físicas, registro de visitantes y control de ingreso a áreas restringidas.
- Líderes de área / responsables del proceso: Solicitar, validar y aprobar los accesos requeridos por los colaboradores bajo su supervisión, asegurando que los permisos otorgados correspondan a las funciones del cargo.

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

4.10.1. 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.

4.10.2. 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.

4.10.3. 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 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.

4.10.4. 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.

4.11. Política General de Relación con Proveedores

4.11.1. 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.

4.11.2. 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.

4.11.3. 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.
- Cuando los proveedores utilicen tecnologías emergentes, incluyendo inteligencia artificial (IA), para el procesamiento de información de ABPS o de sus clientes, dichas soluciones deberán ser evaluadas previamente por el área de Ciberseguridad y Privacidad para identificar riesgos asociados a seguridad de la información, privacidad y cumplimiento normativo.
- 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.

4.11.4. 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.

4.12. Política Gestión de Piso

4.12.1. Objetivos de la política

Definir las directrices para la organización, ingreso y permanencia al interior de las áreas operativas y administrativas de la compañía, garantizando el orden en los puestos de trabajo, la adecuada convivencia y la protección de la información gestionada en las instalaciones de Américas Business Process Services

4.12.2. 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.

4.12.3. Lineamientos

- Los puestos de trabajo deben mantenerse organizados y libres de información sensible cuando el colaborador se ausente del lugar de trabajo, conforme a la política de Escritorio y Pantalla Despejada.

- No está permitido dejar documentos, credenciales, notas con contraseñas o información de clientes visibles en los puestos de trabajo.
- El ingreso de personas ajenas a la operación (visitantes, proveedores o terceros) debe realizarse únicamente con autorización y acompañamiento del área responsable.
- No se permite el consumo de alimentos o bebidas en áreas donde se manipule información sensible o equipos tecnológicos.
- Los colaboradores deben mantener un comportamiento adecuado dentro de las áreas operativas, evitando acciones que puedan poner en riesgo la información, los equipos o la continuidad de la operación.
- Cualquier situación que afecte el orden, la seguridad física o la protección de la información dentro del piso operativo debe ser reportada al líder de la operación o a las áreas de soporte correspondientes.

4.12.4. Responsabilidades

- **Ciberseguridad y Privacidad:** Definir los lineamientos de seguridad de la información aplicables a las áreas operativas y administrativas, garantizar la alineación de esta política con el Sistema de Gestión de Seguridad de la Información (SGSI) y realizar seguimiento al cumplimiento de los controles asociados.
- **Gestión Administrativa:** Controlar el ingreso, permanencia y circulación de personas dentro de las instalaciones, garantizando el cumplimiento de los controles de acceso físico y las normas establecidas para las áreas operativas.
- **Áreas Operativas y Líderes de Campaña:** Velar por el cumplimiento de las normas de gestión de piso dentro de sus equipos de trabajo, asegurando el orden en los puestos de trabajo, el uso adecuado de los recursos asignados y el respeto de las directrices definidas por la compañía.
- **Colaboradores, proveedores y terceros:** Cumplir las directrices establecidas en esta política durante su permanencia en las instalaciones de Américas Business Process Services.

4.13. 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.
La gestión del riesgo desde seguridad de la información se orienta a la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, tomando como línea base la Metodología de Valoración del Riesgo definida por la compañía.

4.13.1. 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.
- Proteger la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de la metodología de gestión de riesgos definida por la organización.

4.13.2. 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.

4.13.3. Responsabilidades

- El proceso de Compliance será responsable de la aprobación, revisión y actualización de la Política de Gestión del Riesgo.
- Los líderes de procesos y campañas serán responsables de identificar, evaluar y gestionar los riesgos asociados a sus actividades, aplicando la metodología de gestión de riesgos definida por la organización.
- Las áreas de soporte, incluyendo Tecnología y Ciberseguridad y Privacidad, deberán apoyar la identificación y tratamiento de riesgos relacionados con sus ámbitos de gestión.

4.14. Política de Controles Criptográficos

4.14.1. 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.

4.14.2. 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.

4.14.3. 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

4.14.4. 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.

4.15. Política Control Código Malicioso

Américas Business Process Services establece las directrices para la protección de sus sistemas de información y activos tecnológicos frente a amenazas de código malicioso, mediante la implementación de herramientas de seguridad como antivirus, EDR u otras soluciones de protección para endpoints.

Estas medidas aplican a los equipos y dispositivos tecnológicos propiedad de la compañía que se conecten a la red corporativa, con el fin de prevenir, detectar y responder ante amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

4.15.1. Objetivos de la política

- Prevenir, detectar y mitigar amenazas de código malicioso que puedan afectar los sistemas de información de Américas Business Process Services.
- Garantizar la protección de los activos tecnológicos mediante la implementación de herramientas de seguridad como antivirus, EDR u otras soluciones de protección para endpoints.
- Reducir el riesgo de propagación de software malicioso dentro de la infraestructura tecnológica de la compañía.

4.15.2. Alcance

La presente política de Control de Código Malicioso aplica a todos los activos tecnológicos propiedad de la compañía, tales como computadores de escritorio, computadores portátiles, servidores, tabletas, dispositivos móviles y cualquier otro equipo que permita la instalación de herramientas de protección contra malware y que se conecte a la red de Américas Business Process Services.

4.15.3. Responsabilidades

- Ciberseguridad y Privacidad: Definir los lineamientos de protección contra código malicioso, revisar y actualizar la política, así como supervisar su cumplimiento.
- Tecnología en conjunto con Ciberseguridad: Implementar, administrar y mantener las herramientas de protección contra malware (antivirus, EDR u otras soluciones de seguridad) en los dispositivos de la organización.
- Usuarios: Utilizar los equipos conforme a las políticas de seguridad establecidas y abstenerse de deshabilitar o manipular las herramientas de protección instaladas.

4.16. Política Realización de Backup

Américas Business Process Services establece la presente política con el propósito de asegurar la protección y recuperación de la información ante incidentes, fallas tecnológicas o eventos que puedan afectar la continuidad de las operaciones.

Para ello, la compañía implementa mecanismos de respaldo de información que permiten proteger los sistemas y repositorios críticos, asegurando la confidencialidad, integridad y disponibilidad de la información propia y de nuestros clientes.

4.16.1. Objetivos de la política

- Garantizar la disponibilidad y recuperación de la información digital almacenada en los sistemas y repositorios de Américas Business Process Services.
- Proteger la información frente a incidentes tecnológicos, fallas operativas o desastres que puedan comprometer su disponibilidad.
- Asegurar que los respaldos de información permitan la restauración oportuna de los datos cuando sea requerido para la continuidad de las operaciones.

4.16.2. Alcance

Esta política aplica a los sistemas de información, plataformas tecnológicas, servidores, dispositivos de almacenamiento, repositorios de información, unidades compartidas, almacenamiento en la nube autorizado por la compañía y demás medios donde se almacene información digital de Américas Business Process Services o de sus clientes.

4.16.3. Responsabilidades

- Tecnología: Implementar, administrar y ejecutar los procesos de respaldo y recuperación de la información, así como realizar pruebas periódicas de restauración.
- Ciberseguridad y Privacidad: Definir lineamientos de seguridad para la protección de los respaldos y supervisar el cumplimiento de la política.
- Usuarios: Almacenar la información corporativa en los repositorios autorizados por la compañía para garantizar su correcta protección y respaldo.

4.17. Política Contingencia y continuidad del negocio

Américas Business Process Services reconoce la importancia de garantizar la continuidad de sus operaciones frente a eventos que puedan afectar la disponibilidad de sus servicios, infraestructura tecnológica o procesos críticos.

Por lo anterior, la compañía establece lineamientos para la gestión de la continuidad del negocio y la recuperación ante desastres, con el fin de asegurar la disponibilidad de los servicios, la protección de la información y la recuperación oportuna de las operaciones ante incidentes que puedan interrumpir su funcionamiento normal.

4.17.1. Objetivos de la política

- Establecer lineamientos para garantizar la continuidad de los procesos críticos de Américas Business Process Services ante eventos de interrupción o desastre.
- Asegurar la disponibilidad y recuperación de los sistemas de información que soportan la operación del negocio.
- Definir el marco general para la implementación, mantenimiento y mejora de los planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP).
- Garantizar el cumplimiento de los compromisos contractuales y regulatorios asociados a la continuidad de los servicios prestados a los clientes.

4.17.2. Alcance

La presente política aplica a los procesos críticos, servicios, infraestructura tecnológica y sistemas de información que soportan la operación de Américas Business Process Services en Colombia, así como a aquellos procesos que contractualmente requieran mecanismos formales de continuidad del negocio.

4.17.3. 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 apoyo, Continuidad Operativa y Tecnología.

Las áreas responsables de los procesos deberán participar en la definición, implementación y actualización de los planes de continuidad del negocio, asegurando que se mantengan alineados con los lineamientos del SGSI, los análisis de impacto al negocio (BIA) y los requisitos contractuales o regulatorios aplicables.

4.18. Política Tecnologías Críticas

Américas Business Process Services establece lineamientos para la evaluación, autorización y uso de tecnologías críticas o no estandarizadas que puedan representar riesgos para la seguridad de la información, la continuidad operativa o el cumplimiento de los requisitos contractuales y regulatorios.

Toda tecnología, herramienta, plataforma o componente tecnológico que no se encuentre previamente autorizado dentro del portafolio tecnológico de la compañía deberá ser evaluado antes de su implementación, con el fin de identificar los riesgos asociados y definir los controles necesarios para su uso seguro.

La aprobación para el uso de tecnologías críticas o no autorizadas deberá ser otorgada por el Director de Ciberseguridad y Privacidad, mediante la correspondiente documentación que incluya la justificación del uso, evaluación de riesgos y condiciones de implementación.

4.18.1. Objetivos de la política

- Establecer lineamientos para la evaluación y autorización del uso de tecnologías críticas o no estandarizadas dentro de Américas Business Process Services.
- Garantizar que la adopción de nuevas tecnologías no genere riesgos inaceptables para la seguridad de la información, la continuidad del negocio o la prestación de servicios a los clientes.
- Asegurar que toda tecnología utilizada en la organización se encuentre debidamente evaluada, aprobada y controlada conforme a los lineamientos del SGSI.

4.18.2. Alcance

Esta política aplica para todos los empleados, proveedores, contratistas, clientes y terceras partes que soliciten o requieran implementar, utilizar o integrar tecnologías que no se encuentren previamente autorizadas dentro del entorno tecnológico de Américas Business Process Services, ya sea dentro o fuera de las instalaciones de la compañía.

4.18.3. 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.

Las áreas que requieran la implementación o uso de tecnologías no autorizadas deberán presentar la solicitud correspondiente, incluyendo la justificación de negocio y el análisis de impacto, para su evaluación y aprobación por parte del área de Ciberseguridad y Privacidad.

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.

4.19. Política de Gestión de LOG y Registros de Auditoría

4.19.1. 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.

4.19.2. 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.

4.19.3. 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.

4.19.4. 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.

4.20. Política Gestión de Vulnerabilidades

Américas Business Process Services establece las directrices para la gestión de vulnerabilidades técnicas como un proceso continuo orientado a identificar, evaluar, priorizar y gestionar las debilidades de seguridad presentes en los sistemas de información, dispositivos tecnológicos y plataformas que hacen parte de la infraestructura tecnológica de la compañía, con el fin de reducir los riesgos de seguridad de la información y garantizar la adecuada protección de los activos tecnológicos del negocio.

4.20.1. Objetivos de la política

- Establecer las directrices para la identificación, análisis, seguimiento y remediación de vulnerabilidades técnicas en los activos tecnológicos de Américas Business Process Services.

- Reducir la exposición a riesgos de seguridad mediante la detección temprana y tratamiento oportuno de vulnerabilidades en sistemas, aplicaciones, redes y dispositivos tecnológicos.
- Garantizar que las pruebas de seguridad como análisis de vulnerabilidades y pruebas de ethical hacking contribuyan al fortalecimiento continuo de la postura de seguridad de la organización...

4.20.2. Alcance

Esta política aplica a todos los activos tecnológicos que conforman la infraestructura tecnológica de Américas Business Process Services, incluyendo servidores, estaciones de trabajo, dispositivos de red, sistemas de información, aplicaciones, servicios en la nube y cualquier otro componente tecnológico que procese, almacene o transmita información de la organización o de sus clientes.

4.20.3. 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.
El área de Tecnología será responsable de ejecutar las acciones de remediación y actualización de los activos tecnológicos cuando se identifiquen vulnerabilidades que requieran intervención técnica.
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).

4.21. 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.

4.21.1. 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.

4.21.2. 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.

4.21.3. 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.

4.22. Política de Continuidad de la Seguridad de la Información

4.22.1. Objetivos

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.

4.22.2. 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.

4.22.3. 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.

4.23. 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, derivadas de:

- Implementación inapropiada del software.
- Introducción de fallas durante el mantenimiento o actualización del producto.
- Uso de prácticas débiles de codificación que pueden introducir vulnerabilidades desde el punto de vista técnico.

La presente política establece los principios, prácticas y directrices que deben ser tenidas en cuenta durante el ciclo de vida de desarrollo de software, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en las aplicaciones desarrolladas o gestionadas por Américas Business Process Services, incluyendo aquellas que procesen información sensible o regulada como datos personales, información de clientes o, cuando aplique, datos del entorno de titulares de tarjeta (CDE).

4.23.1. Objetivos de la política

Establecer los lineamientos de seguridad que deben ser aplicados durante el ciclo de vida de desarrollo de aplicaciones en Américas Business Process Services, mediante la adopción de estándares, controles y buenas prácticas de desarrollo seguro que permitan prevenir vulnerabilidades, proteger la información y asegurar el cumplimiento de los requisitos del SGSI y de las regulaciones aplicables.

4.23.2. Alcance

La presente política aplica a todas las aplicaciones desarrolladas, adquiridas, mantenidas o modificadas por Américas Business Process Services, incluyendo sistemas internos, aplicaciones web, móviles, integraciones y cualquier componente de software que procese, almacene o transmita información de la organización o de sus clientes.

También aplica a terceros o proveedores que desarrollen software para la organización.

4.23.3. Responsabilidades

- Los procesos responsables del desarrollo, automatización o implementación de soluciones tecnológicas dentro de Américas Business Process Services deberán asegurar que las aplicaciones, scripts, automatizaciones, integraciones o componentes desarrollados cumplan con los principios y lineamientos de desarrollo seguro definidos por la organización.
- El proceso de Ciberseguridad y Privacidad podrá realizar acompañamiento o revisiones cuando se considere necesario, con el fin de verificar el cumplimiento de los lineamientos de seguridad establecidos.
- Las áreas responsables del desarrollo o implementación de soluciones tecnológicas deberán incorporar controles de seguridad, pruebas y revisiones que permitan identificar y mitigar vulnerabilidades antes de su puesta en producción.

Cualquier modificación, corrección o actualización del presente documento deberá ser coordinada por el área de Ciberseguridad y Privacidad, garantizando su alineación con el SGSI, así como con buenas prácticas y marcos de referencia reconocidos para el desarrollo seguro de software tales como OWASP, NIST e ISO/IEC 27002, entre otros que la organización adopte.

4.24. 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:

4.24.1. Objetivo

Establecer directrices que aseguren la protección de la información gestionada en entornos de servicios en la nube contratados por Américas Business Process Services o en nombre de sus clientes, garantizando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y privacidad de la información.

4.24.2. Alcance

Aplica a todos los servicios que involucren el procesamiento, almacenamiento o transmisión de información de Américas Business Process Services o de sus clientes a través de plataformas o infraestructuras de computación en la nube, gestionadas directamente por la compañía o mediante proveedores de servicios cloud contratados.

4.24.3. 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 2300 y demás normativas aplicables.
- Evaluar los riesgos de seguridad asociados al uso de servicios en la nube antes de su contratación o implementación, en el marco del proceso de gestión de riesgos de la compañía.

4.24.4. Responsabilidad

La implementación, seguimiento y verificación de estos lineamientos será responsabilidad del área de Ciberseguridad y Privacidad, en coordinación con el área de Tecnología y las áreas responsables de la gestión de servicios tecnológicos, según corresponda.

4.25. Política de Evaluación de Riesgos en Proyectos y Servicios

4.25.1. Objetivo

Establecer directrices para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información asociados a nuevos proyectos, servicios, tecnologías o cambios significativos en los servicios prestados por Américas Business Process Services, con el fin de proteger la información de la compañía y de sus clientes.

4.25.2. Alcance

Aplica a todos los proyectos, iniciativas, implementaciones tecnológicas, nuevos servicios o cambios operacionales, tecnológicos, regulatorios o contractuales que puedan impactar la seguridad de la información gestionada por Américas Business Process Services.

4.25.3. Lineamientos

- Toda nueva iniciativa, proyecto o cambio significativo deberá incluir una evaluación de riesgos de seguridad de la información antes de su implementación o puesta en producción.
- Los riesgos identificados deberán ser analizados, evaluados y tratados con base en metodologías aprobadas por Américas Business Process Services, tales como ISO/IEC 27005 e ISO 31000, considerando el contexto operativo de la compañía y de los clientes.
- En caso de identificarse riesgos que superen el nivel de aceptación definido por la organización, deberán establecerse planes de tratamiento que incluyan responsables, controles y plazos definidos.
- Se deberán ejecutar evaluaciones adicionales cuando existan cambios significativos que modifiquen el alcance, tecnología, arquitectura o contexto operativo del servicio.
- Las evidencias asociadas a las evaluaciones de riesgos deberán ser documentadas y conservadas, garantizando su disponibilidad para procesos de auditoría interna o externa.
- La gestión de riesgos deberá ser trazable y estar integrada con el Sistema de Gestión de Seguridad de la Información (SGSI) de Américas Business Process Services

4.25.4. Responsabilidad

- El líder del proyecto, servicio o proceso será responsable de iniciar y gestionar la evaluación de riesgos correspondiente
- El área de Ciberseguridad y Privacidad será responsable de validar la evaluación realizada, verificar la aplicación de controles de seguridad y asegurar su registro dentro del SGSI.
- Las áreas técnicas o responsables del servicio deberán implementar los controles definidos en los planes de tratamiento de riesgos.

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

4.26.1. 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 de la compañía y de los clientes, desde su diseño, desarrollo o adquisición hasta su retiro o desmantelamiento.

4.26.2. Alcance

Aplica a todos los sistemas de información desarrollados, adquiridos, implementados o administrados por AMÉRICAS BPS, que gestionen información de la compañía, de los clientes o que formen parte de los servicios prestados.

4.26.3. Lineamientos

- Aplicar principios de seguridad desde el diseño (Security by Design) y durante todo el ciclo de vida de los sistemas.
- Incluir requisitos de seguridad de la información dentro de las especificaciones funcionales, técnicas y contractuales durante el desarrollo o adquisición de sistemas.
- Realizar evaluaciones de riesgos de seguridad de la información antes de la puesta en producción de sistemas nuevos o de cambios significativos en sistemas existentes.
- Ejecutar pruebas de seguridad, revisiones de código seguro y análisis de vulnerabilidades antes de la implementación en ambientes productivos.
- Gestionar adecuadamente los cambios, actualizaciones y mantenimiento de los sistemas garantizando que se mantengan los controles de seguridad definidos.
- Asegurar el retiro o desmantelamiento seguro de sistemas, garantizando la eliminación, transferencia o protección adecuada de la información almacenada.

4.26.4. Responsabilidades

- El área de Tecnología será responsable de la administración de los sistemas, la infraestructura asociada y la correcta implementación técnica de los controles definidos durante el ciclo de vida.
- Las áreas de Desarrollo, Automatización u otras áreas responsables de la construcción o configuración de soluciones tecnológicas deberán asegurar la aplicación de prácticas de desarrollo seguro y pruebas de seguridad antes de la liberación de sistemas.
- El área de Ciberseguridad y Privacidad será responsable de definir los lineamientos de seguridad, validar la gestión de riesgos y verificar el cumplimiento de los controles dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

4.27. Política de Gestión de Configuraciones

4.27.1. Objetivo

Garantizar que las configuraciones de los sistemas, plataformas e infraestructuras tecnológicas que gestionan información de AMÉRICAS BPS y de sus clientes se mantengan controladas, seguras y auditables durante su operación.

4.27.2. Alcance

Aplica a toda la infraestructura tecnológica, plataformas, aplicaciones, sistemas operativos, dispositivos de red y servicios gestionados por AMÉRICAS BPS que intervienen en el procesamiento, almacenamiento o transmisión de información de la compañía o de sus clientes.

4.27.3. Lineamientos

- Mantener inventarios actualizados de configuraciones autorizadas (baseline) para los componentes tecnológicos críticos.
- Aplicar configuraciones seguras siguiendo estándares y buenas prácticas reconocidas (CIS Benchmarks, NIST u otros aplicables).
- Gestionar los cambios en configuraciones mediante procedimientos formales de gestión del cambio, asegurando su evaluación, aprobación y documentación previa a su implementación.
- Realizar verificaciones y auditorías periódicas para validar la conformidad de los sistemas con las configuraciones aprobadas.
- Registrar, documentar y gestionar cualquier desviación de las configuraciones autorizadas, implementando acciones correctivas cuando sea necesario.
- Mantener evidencia documental de las configuraciones aplicadas para fines de auditoría y cumplimiento del SGSI.

4.27.4. Responsabilidad

- El área de Tecnología será responsable de implementar y mantener las configuraciones técnicas de los sistemas e infraestructuras de acuerdo con los estándares definidos.
- El área de Ciberseguridad y Privacidad será responsable de definir los lineamientos de configuración segura, supervisar su cumplimiento y realizar revisiones periódicas dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI).

4.28. Política de Clasificación y Tratamiento de Activos de Información

4.28.1. Objetivo

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

4.28.2. Alcance

Aplica a todos los activos de información tangibles e intangibles, incluyendo datos, documentos, sistemas, bases de datos, dispositivos tecnológicos, software, medios electrónicos y soportes físicos gestionados por AMÉRICAS BPS en el desarrollo de sus procesos internos y en la prestación de servicios a clientes.

4.28.3. Lineamientos

- Identificar, documentar y mantener un inventario actualizado de los activos de información que soportan los procesos de la organización y los servicios prestados a 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, Privada, 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 o identificar los activos según su clasificación de seguridad y aplicar controles de protección acordes a dicha categoría.
- Definir y aplicar procedimientos específicos para el manejo, almacenamiento, transmisión, respaldo y eliminación segura de la información según su clasificación.
- Realizar revisiones periódicas del inventario y de la clasificación de activos como parte del proceso de mejora continua del SGSI.
- Asegurar que los activos de información de los clientes sean tratados conforme a los acuerdos contractuales, regulatorios y de confidencialidad establecidos.

4.28.4. Responsabilidad

- El área de Tecnología será responsable de mantener actualizado el inventario de activos tecnológicos y de información asociados a la infraestructura y sistemas de la organización.
- El proceso de Ciberseguridad y Privacidad será responsable de definir los lineamientos de clasificación, protección y tratamiento de los activos de información, así como supervisar su cumplimiento dentro del Sistema de Gestión de Seguridad de la Información (SGSI).
- Los propietarios de los activos (responsables de proceso o líderes de área) serán responsables de asegurar el uso adecuado, la correcta clasificación y la protección de los activos bajo su gestión.

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

4.29.1. 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.

4.29.2. Alcance

Aplica a los servicios de monitoreo de seguridad, gestión de eventos y análisis de amenazas prestados por proveedores SOC a AMÉRICAS BPS, así como al tratamiento de información de inteligencia de amenazas proveniente de fuentes internas y externas que puedan impactar los activos de información y la infraestructura tecnológica de la organización.

4.29.3. Lineamientos

- Los servicios de monitoreo de seguridad podrán ser prestados por proveedores especializados (SOC) bajo esquemas de operación continua y con niveles de servicio definidos contractualmente.

- El proveedor SOC deberá realizar el monitoreo, análisis y correlación de eventos de seguridad provenientes de los activos tecnológicos críticos de la organización.
- Los eventos relevantes deberán ser analizados, clasificados y escalados oportunamente conforme a los procedimientos de gestión de incidentes de seguridad y de acuerdo al procedimiento PR32 CYP 0501
- Se exigirá al SOC la administración de herramientas SIEM/SOAR integradas con plataformas de Threat Intelligence 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.
- 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 proveedor SOC deberá generar informes periódicos sobre eventos de seguridad, tendencias de amenazas y efectividad de los controles implementados
- Los resultados del monitoreo y la inteligencia de amenazas deberán ser considerados como insumo para la gestión de riesgos, la gestión de vulnerabilidades y la mejora continua del SGSI.

4.29.4. 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.

4.29.5. 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.
El proveedor SOC será responsable de realizar el monitoreo de seguridad de acuerdo con los lineamientos definidos. Escalar oportunamente eventos e incidentes de seguridad. Y entregar reportes periódicos de análisis y tendencias de amenazas

4.30. Política de Protección de Información en Dispositivos de Usuario Final

4.30.1. Objetivo

Establecer las directrices de seguridad para la protección de la información gestionada a través de dispositivos de usuario final utilizados para acceder a los sistemas, aplicaciones y recursos tecnológicos de Américas Business Process Services.

4.30.2. Alcance

Esta política aplica a todos los dispositivos utilizados para interactuar con activos de información de Américas Business Process Services, incluyendo estaciones de trabajo, computadores portátiles, dispositivos móviles, terminales conectadas y cualquier otro equipo utilizado por empleados, contratistas o terceros autorizados, ya sean dispositivos corporativos o personales previamente autorizados.

4.30.3. 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 cifrados 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.

4.30.4. 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.

4.31. Política de Uso de Inteligencia Artificial

Américas Business Process Services establece los lineamientos para el uso responsable y seguro de herramientas basadas en Inteligencia Artificial (IA) con el fin de prevenir riesgos asociados a la exposición de información confidencial, el tratamiento inadecuado de datos personales y el uso no autorizado de información de la compañía o de sus clientes.

4.31.1. Objetivo

Definir las directrices para el uso adecuado de herramientas de Inteligencia Artificial por parte de los empleados, proveedores, contratistas y terceros autorizados de Américas Business Process Services, garantizando la protección de la información, el cumplimiento de los requisitos legales y la gestión adecuada de los riesgos asociados a estas tecnologías.

4.31.2. Alcance

Esta política aplica para todos los empleados, proveedores, contratistas y terceros que utilicen herramientas de Inteligencia Artificial en el desarrollo de sus funciones o en el marco de los servicios prestados por Américas Business Process Services, ya sea mediante plataformas públicas, privadas o integradas a los sistemas corporativos.

4.31.3. Lineamientos

- El uso de herramientas de Inteligencia Artificial deberá realizarse únicamente mediante cuentas corporativas y en herramientas autorizadas por la organización.
- El uso de herramientas de Inteligencia Artificial deberá realizarse únicamente para fines laborales autorizados y relacionados con las funciones asignadas.
- No está permitido ingresar en herramientas de Inteligencia Artificial información clasificada como confidencial, restringida o sensible, ni datos personales de clientes, empleados o terceros, salvo que la herramienta haya sido previamente autorizada por la compañía y cuente con los controles de seguridad requeridos.
- El uso de herramientas de IA deberá cumplir con los lineamientos de protección de datos personales, confidencialidad de la información y las políticas de seguridad de la información definidas por Américas Business Process Services.
- Las soluciones de Inteligencia Artificial implementadas o utilizadas deberán cumplir con estándares y buenas prácticas de seguridad reconocidas, tales como lineamientos de NIST, OWASP u otros marcos de referencia aplicables
- La información generada mediante herramientas de Inteligencia Artificial deberá ser revisada y validada por el usuario antes de su utilización en documentos, procesos o comunicaciones oficiales.
- En caso de que proveedores o terceros utilicen herramientas de Inteligencia Artificial dentro de los servicios prestados a AMÉRICAS BPS (por ejemplo, automatizaciones, asistentes virtuales o análisis automatizado), estos deberán garantizar la implementación de controles de seguridad adecuados para la protección de la información, incluyendo controles de acceso, protección de datos y cumplimiento de la normativa aplicable.
- El uso de herramientas de IA deberá respetar los principios de confidencialidad, integridad y disponibilidad de la información, así como las obligaciones contractuales y regulatorias aplicables

4.31.4. Responsabilidades

La aprobación, revisión y actualización de la Política de Uso de Inteligencia Artificial será responsabilidad del área de Ciberseguridad y Privacidad de Américas Business Process Services.
El área de Tecnología será responsable de evaluar y habilitar técnicamente las herramientas de Inteligencia Artificial autorizadas para su uso dentro de la organización.

Los usuarios serán responsables de utilizar estas herramientas de manera responsable, garantizando que no se divulgue información sensible o confidencial de la compañía o de sus clientes.

4.32. 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.

4.33. Revisión

Este Manual debe ser revisada por lo menos una vez al año

5. Control de Cambios

Versión	Descripción del cambio	Elaboró	Aprobó
00 25/04/2019	Creación del documento.		
01 31/07/2020	Modificación de código del documento		
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.		
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.		
04 05/03/2026	Se actualizaron redacciones de políticas existentes para mayor claridad y coherencia. Se incluyeron		

Versión	Descripción del cambio	Elaboró	Aprobó
	lineamientos adicionales en políticas de Desarrollo Seguro de Aplicaciones, Política Gestión de Piso. Se ajustaron las responsabilidades en las políticas incluyendo roles de Tecnología, Desarrollo y Ciberseguridad, gestión administrativa y usuarios/colaboradores. Se elimino 4.23. Política Gestión de Usuarios y Contraseñas, ya que se repetía. Se agregó la Política de Uso de Inteligencia Artificial con lineamientos de uso corporativo, protección de información confidencial y controles para proveedores que utilicen IA. Se actualizo código paso de MA01 CYP 0501 a MA01 CYP 01.		