


Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

Elaborado por: Adriana Yibeth Alarcon Infante Profesional de seguridad de la información Kely Johana Gonzalez Hernandez Profesional I	Revisado por: Paola Marcela Hernandez Sierra Directora de Seguridad de la Información y ciberseguridad Jhon Jairo Rosas Alba Oficial de Protección de Dato Personales Alexander Cardozo Niño Control Fraude	Aprobado por: Paola Marcela Hernandez Sierra Directora de Seguridad de la Información y ciberseguridad
--	---	--

Nombre de proceso: 09.7 Gestión de la seguridad de la información, ciberseguridad y protección de la privacidad

Nombre de Procedimiento: 09.7.1 Planeación de la gestión de la seguridad de la información, ciberseguridad y protección de la privacidad


Objetivo: Establecer los lineamientos de seguridad de la información que deberán ser cumplidos por los proveedores, contratistas o terceros que accedan, transporten, intercambien, custodien o almacenen por cualquier medio información (datos) de ETB, garantizando su confidencialidad, integridad y disponibilidad.

Alcance: Aplica para todos los proveedores, contratistas, terceros y aliados denominados a partir de ahora terceros quienes directa e indirectamente puedan acceder, procesar, almacenar y/o comunicar información confidencial de ETB, en el desarrollo del objeto del contrato o servicio prestado, incluyendo, sin limitarse, servicios de servicios de data center, negocios especiales, datos, televisión, voz e internet, fijo y móvil y cualquier otro asociado al servicio de telecomunicaciones en general.

Segmento: Todos los segmentos.

Definiciones:

- **Acuerdo de Confidencialidad (NDA):** Documento legal que compromete a las partes a proteger la información compartida.
- **Autenticación fuerte (MFA):** Método de autenticación que requiere dos o más factores de verificación para el acceso.
- **Ciclo de vida del desarrollo seguro:** Integración de prácticas de seguridad en todas las etapas del desarrollo de software.

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

- **Cifrado:** Proceso de convertir información en un código para evitar el acceso no autorizado.
- **Confidencialidad:** Asegurar que la información solo sea accesible para aquellos autorizados.
- **Continuidad del negocio:** Capacidad de una organización para mantener sus operaciones esenciales durante y después de una interrupción.
- **Declaración de Aplicabilidad (SOA):** Documento que especifica los controles de seguridad de la información que son relevantes para una organización o servicio.
- **Destrucción segura de información:** Eliminación de datos de manera que sea irrecuperable.
- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando sea necesario.
- **Gestión de cambios:** Proceso para controlar las modificaciones en los sistemas y servicios.
- **Incidente de seguridad:** Evento que compromete la seguridad de la información.
- **Integridad:** Mantener la exactitud y completitud de la información y los métodos de procesamiento.
- **Medios removibles:** Dispositivos de almacenamiento de datos que pueden ser fácilmente retirados de un sistema (ej., USB, discos externos).
- **Principio de mínimo privilegio:** Otorgar solo los accesos y privilegios estrictamente necesarios para realizar una tarea.
- **Pruebas de penetración:** Simulaciones de ataques cibernéticos para identificar vulnerabilidades.
- **Subcontratación:** Contratación de un tercero por parte del proveedor para la ejecución de parte del servicio.
- **Vulnerabilidad:** Debilidad en un sistema que puede ser explotada por una amenaza.



Código			POLÍTICA			
09-09.7-Pol-023-v.2			Seguridad de la información y ciberseguridad para las relaciones con terceros			
Fecha de emisión						
19	12	2025				

Tabla de contenido

1. Principios generales y cumplimiento normativo	4
2. Seguridad de la información y ciberseguridad	4
3. Gestión de riesgos	5
4. Controles de acceso y gestión de identidades	5
5. Desarrollo seguro	7
6. Infraestructura y conectividad	7
7. Gestión de vulnerabilidades y pruebas de seguridad	8
8. Equipos, software y medios removibles	8
9. Gestión de cambios	9
10. Gestión de incidentes y respuesta	9
11. Servicios en la nube	9
12. Continuidad del negocio	10
13. Devolución y destrucción de información	10
14. Formación, conciencia y antecedentes del personal	10
15. Auditorías	10
16. Aceptación y vigencia	11

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		


Los terceros deberán cumplir, de acuerdo con el objeto del contrato o servicio prestado, los lineamientos descritos en la presente política

1. Principios generales y cumplimiento normativo

- Los terceros deben conocer y evidenciar el cumplimiento de la normativa colombiana aplicable (p. ej. Leyes 1266/2008, 1581/2012 y sus decretos) y las normas internacionales que ETB determine (entre ellas, ISO/IEC 27001 y buenas prácticas de la industria) según la naturaleza del servicio.
- Los terceros deben cumplir con las políticas y procedimientos establecidos en ETB y estándares de seguridad de la información, ciberseguridad y protección de la privacidad que sean aplicables al objeto del contrato.
- Los terceros deben contar con políticas, estándares y procedimientos documentados y auditables relacionados con seguridad de la información, protección de datos personales, control de acceso físico y lógico, manejo de credenciales, escritorio limpio, gestión de cambios, gestión de vulnerabilidades, entre otros, los cuales deben ser comunicados y aplicados al personal asignado al contrato.
- Se prohíbe expresamente a terceros la captación de clientes y uso de datos de ETB para fines comerciales.
- Validar y revisar que los cambios en los acuerdos contractuales en el servicio de los terceros realizados de manera unilateral o bilateral garanticen la continuidad de la adherencia de los requisitos de seguridad.

2. Seguridad de la información y ciberseguridad

- Todo Tercero que acceda a información de ETB deberá suscribir un acuerdo de confidencialidad (NDA) firmado y cláusulas contractuales que establezcan obligaciones de protección, limitación de uso, continuidad, transferencia, y salvaguardas técnicas y organizativas.
- Los Terceros estarán obligados a cumplir con los controles de seguridad de la información considerados en la Declaración de Aplicabilidad (SOA) vigente, cuando estos sean aplicables al servicio o activo provisto.
- Los Terceros son responsables de demostrar la eficacia de sus controles de seguridad a través de informes periódicos que incluyan evidencias de cumplimiento. Ante cualquier hallazgo o brecha de seguridad, el Tercero deberá definir y presentar a ETB el plan para su corrección.
- Cualquier subcontratación que realice el tercero y que implique acceso a información (datos) de ETB, requiere autorización previa y por escrito.

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

ETB se reserva el derecho de aprobar o rechazar subcontratistas que representen riesgos para la seguridad de la información; asimismo, el Tercero será responsable por el cumplimiento del subcontratista y deberá contractualmente imponer las mismas obligaciones de seguridad establecidas por ETB.

- El Tercero se obligan a no revelar, divulgar, exhibir, mostrar, comunicar, utilizar o emplear la información de ETB con personas naturales o jurídicas, que no tengan autorización contractual, y, en consecuencia, se obliga a mantenerla de manera confidencial y privada, y a proteger dicha información para evitar su divulgación no autorizada.
- Los Terceros deben implementar los controles de seguridad equivalentes a los exigidos por ETB en toda la prestación del bien o servicio contratado.


3. Gestión de riesgos

- Los terceros deberán colaborar con ETB en la identificación, análisis y tratamiento de riesgos asociados a los servicios contratados y a los activos de información involucrados.
- Los terceros deberán informar y gestionar los riesgos relacionados con obsolescencia tecnológica o indisponibilidad de productos o servicios.

4. Controles de acceso y gestión de identidades


- Todo Tercero que requiera que su personal acceda a plataformas, aplicaciones o elementos de infraestructura TI de ETB, deberá remitir previamente al supervisor o líder técnico designado la siguiente documentación:
 - Formato autorización para el tratamiento de datos personales (07-09.8-F-030), debidamente firmada por el personal.
 - Formato de Información para Gestión de Seguridad (09-09.8-F-006), debidamente diligenciado y firmado.
 - Formato de Solicitud de Cuentas y Claves de Acceso (05.2-05.2.5-F-042), firmado y autorizado.
 - Documento de identidad.
 - Fotografía reciente.

El envío completo y validación de estos documentos será requisito indispensable para que el supervisor o líder técnico gestione ante la Mesa de Servicios la creación de cuentas de usuario o asignación o

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

modificación de roles. Ninguna cuenta será habilitada sin la recepción y aprobación previa de la documentación exigida.

- Para el caso de los contratistas o terceros que finalizan su contrato y serán vinculados mediante uno nuevo, deberán a través del supervisor del contrato solicitar la creación de los nuevos usuarios con una anticipación mínima de quince (15) días calendario antes de la fecha de inicio del nuevo contrato. Esta solicitud debe realizarse a través de Mesa de Servicio, ya que no se aceptarán solicitudes con un tiempo menor, dado que esto compromete la validación de seguridad y la continuidad operativa.
- Los Terceros no están autorizados a realizar solicitudes directamente a la Mesa de Servicio TI, es por esto que todas las solicitudes deben realizarse exclusivamente a través del supervisor o líder técnico designado.
- Acceso bajo el principio de mínimo privilegio y necesidad de conocer. Los roles y privilegios deben estar documentados y aprobados por ETB.
- Cada usuario debe contar con credenciales únicas, personales e intransferibles.
- Está prohibido compartir usuarios o contraseñas. El uso indebido será considerado incumplimiento grave.
- Cuando se reciba por primera vez la cuenta de usuario y contraseña, esta última debe ser cambiada inmediatamente en el primer ingreso a los sistemas, posteriormente el cambio de contraseñas se deberá realizar mensualmente. Las contraseñas deben contener más de 12 caracteres, combinar mayúsculas y minúsculas, incluir números y caracteres especiales.
- Los Terceros que son administradores y usuarios de los sistemas de información y las plataformas de servicios de ETB son responsables del buen uso de la información que tienen a su cargo, atendiendo las políticas de seguridad definidas en ETB y teniendo en cuenta el nivel de criticidad de los activos o los datos que allí se gestionan.
- Implementación de autenticación fuerte (MFA) para accesos privilegiados y acceso remoto a entornos de ETB.
- Los Terceros deben participar en procesos de certificación y depuración de cuentas (altas, bajas, cambios) y reportar oportunamente cambios en los roles y permisos de su personal a través del supervisor del contrato o líder técnico.
- Notificar inmediatamente a ETB cualquier compromiso, pérdida o sospecha de compromiso de credenciales o accesos.
- Los Terceros entiende y acepta que ETB se reserva el derecho de negar la entrega o suspender las credenciales de acceso a las instalaciones físicas o a los sistemas de información de ETB a cualquier empleado

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

directo o indirecto del Tercero, en caso de considerar que ha ejecutado actividades que incumplan las políticas de seguridad de la información o que hayan sido de carácter doloso o fraudulento, sin que sea necesario presentar al Tercero evidencias de tales hallazgos.


- Los Terceros comunicarán al personal asignado las responsabilidades asociadas a la cuenta de usuario entregada para la prestación de servicios a ETB. Además, Los Terceros deberán remitir a ETB constancia de la aceptación de dichas responsabilidades con las cuentas de usuario.

5. Desarrollo seguro

- Los Terceros deben asegurar que el ciclo de vida del desarrollo incluya prácticas de seguridad: definición de requisitos de seguridad, diseño seguro, revisiones de código, pruebas de seguridad (SAST/DAST), gestión de dependencias y liberación segura.
- Los Terceros deben mantener control de cambios y repositorios con control de acceso a fin de proteger el código fuente frente a accesos no autorizados.
- Los Terceros deben asegurar que se usen versiones estables y fuentes confiables; mantener inventario de dependencias y realizar análisis de vulnerabilidades de terceros.

6. Infraestructura y conectividad

- Los Terceros deben garantizar el cifrado de la información en tránsito y en reposo cuando la naturaleza de la información lo requiera. Así mismo, gestionar de forma segura las claves y materiales criptográficos.
- Los Terceros deben utilizar canales seguros y autenticados para intercambios de información con ETB. Todo acceso a la infraestructura debe ser autorizado y registrado.
- Los Terceros deben contar con estándares de direccionamiento para redes privadas.
- Los Terceros deben asegurar la segmentación de red y aislamiento lógico de servicios. El tráfico debe estar separado para mitigar la exposición entre dominios.
- Los Terceros mantendrán la documentación de arquitectura de seguridad detallando los controles y los flujos seguros de información.
- Los Terceros deben asegurar el monitoreo continuo de redes y sistemas para detección de actividades anómalas; mantener registros de logs y proveer trazabilidad punta a punta de eventos de operación y seguridad.

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		


- Para contratos relacionados con adquisición, mantenimiento o soporte de tecnología, los Terceros deberán gestionar los riesgos asociados a la obsolescencia de componentes y a la indisponibilidad de los Terceros (end-of-life, fin de soporte o salida del mercado). Los Terceros deberán informar a ETB sobre riesgos de obsolescencia y proponer planes de mitigación y reemplazo que garanticen continuidad y seguridad.
- Cuando se requiera integración con plataformas de Terceros, los Terceros deberán garantizar que toda la conexión se realice mediante VPN seguras y protocolos de comunicación cifrados, de forma que se preserve la confidencialidad, integridad y disponibilidad de la información transmitida entre las partes.
- Los Terceros deberán implementar medidas para minimizar la exposición de recursos tecnológicos, asegurando que todos los accesos de red sean autenticados, controlados y verificados, y que exista trazabilidad completa mediante registros de auditoría que permitan identificar al usuario, la acción realizada y el momento en que ocurrió.
- Para el establecimiento de túneles de conexión o servicios de VPN sitio a sitio, Los Terceros deberán diligenciar el formato de Solicitud de Servicios VPN (05.1-05.1.2-F-071) definido por ETB.

7. Gestión de vulnerabilidades y pruebas de seguridad

- Los Terceros deben realizar análisis periódicos de vulnerabilidades y/o pruebas de penetración. Los resultados deben ser compartidos con ETB y los hallazgos críticos deben mitigarse con prioridad.
- Los Terceros deberán permitir revisiones técnicas, pruebas de Ethical hacking, pentesting y auditorías de seguridad por parte de ETB o un tercero designado.

8. Equipos, software y medios removibles

- Los Terceros deben asegurar que los equipos utilizados en la prestación del servicio deben tener antivirus/antimalware con licenciamiento vigente y actualizaciones automáticas.
- Solo se permitirá a los Terceros la instalación de software soportado y debidamente licenciado.
- Se prohíbe que los Terceros hagan uso de cuentas de correo público para comunicaciones oficiales.
- Se prohíbe al Tercero el uso de medios removibles no autorizados por ETB. Cualquier excepción debe ser aprobada y controlada.

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		


- Se prohíbe al Tercero enviar información confidencial por aplicaciones de mensajería no autorizadas (WhatsApp, Telegram, etc.) por ETB.
- El Terceros que brindan servicios como operaciones, agentes, centros de llamadas debe establecer controles que impidan el ingreso a las áreas de actividades de dispositivos electrónicos (cámaras, celulares, USB, discos de almacenamiento externo, etc.) Y elementos de escritura (cuadernos, lápices, hojas, etc.) o cualquier medio físico o electrónico que permita extraer información propiedad de ETB. Los Terceros deberán establecer espacios para el almacenamiento seguro de estos elementos.
- Todo Tercero que ingrese a las instalaciones de ETB o que maneje información de la organización deberá entender y aceptar que, una vez conectado a la red corporativa, ETB podrá monitorear la actividad de red y las estaciones de trabajo utilizadas estarán sujetas a revisión o inspección técnica cuando ETB lo requiera, con el fin de verificar el cumplimiento de las políticas de seguridad.
- Al ingresar a las instalaciones de ETB y hacer uso de los recursos tecnológicos, los Terceros deberá permitir la instalación, configuración y uso de software o soluciones de seguridad que ETB considere necesarias (por ejemplo, sistemas de control de acceso, validación de identidad u otros equivalentes), como requisito para garantizar la protección de la red y los activos de información.

9. Gestión de cambios

- Todo cambio realizado por el Tercero que impacte servicios prestados a ETB debe ser notificado y aprobado por escrito antes de su implementación.
- Los cambios realizados por el Tercero deben probarse en entornos controlados y disponer de planes de rollback documentados.
- Los Terceros deben mantener una bitácora de cambios con fecha, responsable, motivo, aprobación y evidencia de pruebas.

10. Gestión de incidentes y respuesta

- Los Terceros deben definir y mantener procedimientos claros para la identificación, reporte, contención, erradicación, recuperación y lecciones aprendidas.
- Los incidentes que afecten la información de ETB deben ser reportados de forma inmediata y, como máximo, dentro de las 24 horas hábiles al punto de contacto designado por ETB (Help Desk, supervisor de contrato o líder técnico) .

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

- Los Terceros deben preservar evidencia y colaborar con ETB en la investigación, contención, remediación y preservación de evidencia de incidentes.
- ETB se reserva el derecho de ejecutar acciones de contención, bloqueo o suspensión de accesos para proteger sus activos.

11. Servicios en la nube


- Los Terceros deberán documentar la configuración, el hardening y la segregación de los entornos virtuales, asegurando la separación lógica entre clientes y servicios.
- En los casos en que los servicios de ETB se encuentren alojados en infraestructuras de nube de algún Tercero, este deberá garantizar la seguridad por diseño, implementar una arquitectura de nube segura, aplicar el principio de mínimo privilegio, y establecer controles de seguridad en capas que protejan la información y los activos tecnológicos de ETB durante todo el ciclo de vida del servicio.

12. Continuidad del negocio

- Los Terceros deben contar con planes de continuidad que garanticen la prestación del servicio (infraestructura, sistemas, personal y comunicaciones) y pruebas de verificación periódicas.
- Los Terceros deben implementar redundancia acorde a los SLA definidos.

13. Devolución y destrucción de información

- Al terminar el contrato, los Terceros deben devolver la información a ETB por medios seguros y acreditar la destrucción segura de información mediante certificación escrita.
- En caso de que los Terceros o sus trabajadores o sus propios contratistas hayan adquirido un conocimiento importante a partir del desarrollo del contrato, el Contratista se obliga a documentar y transferir a ETB ese conocimiento, de acuerdo con lo estipulado en el contrato.
- Quedan prohibidas las copias no autorizadas o backups que contengan información de ETB sin autorización previa y por escrito.
- Los Terceros deben tener procedimientos documentados para el retorno y eliminación segura de datos al terminar la relación contractual.

Código	POLÍTICA	
09-09.7-Pol-023-v.2	Seguridad de la información y ciberseguridad para las relaciones con terceros	
Fecha de emisión		
19 12 2025		

14. Formación, conciencia y antecedentes del personal

- Los Terceros deben realizar campañas periódicas de concienciación en seguridad de la información, ciberseguridad y protección de la privacidad y realizar formación en temas específicos para el personal asignado.
- Los Terceros deben verificar los antecedentes del personal asignado a fin de asegurar que no cuentan con sanciones por incumplimiento de confidencialidad.

15. Auditorías

- ETB o un tercero designado por ETB podrá realizar auditorías y revisiones de seguridad; los Terceros deberán facilitar acceso y evidencias.
- En caso de hallazgos, los Terceros deberán definir e implementar planes de acción en los plazos acordados y reportar a ETB las remediaciones.
- El incumplimiento por parte del Tercero podrá acarrear sanciones contractuales, suspensión de servicios o acciones legales según lo establecido en el contrato.

16. Aceptación y vigencia

- La aceptación de este documento por parte del Tercero implica cumplimiento estricto de los requisitos aplicables según el objeto contractual. El incumplimiento de lo establecido en esta política podrá dar lugar a sanciones contractuales, suspensiones temporales del contrato o terminación de la relación contractual de manera unilateral por parte de ETB.
- Esta política entra en vigencia a partir de su firma/aceptación contractual.
- Esta política será revisada periódicamente por la Dirección de Seguridad de la Información y Ciberseguridad de ETB.

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
v1	Creación del documento	10/04/2018
v2	Actualización de la política	19/12/2025