RESOLUCION N. 0184

(29 JUL 2026)

"POR LA CUAL SE MODIFICA LA RESOLUCIÓN N. 0668 DEL 29 DE JUNIO DE 2019, QUE ADOPTA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL S.A E.S.P OFICIAL"

EL GERENTE GENERAL DE LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL S.A. E.S.P. OFICIAL, en uso de sus facultades legales y estatutarias que le han sido otorgadas, así mismo en uso de las establecidas en los artículos 209 y 211 de la Constitución Nacional y,

CONSIDERANDO:

1.- Que mediante Resolución No. 0668 del 29 de junio de 2019 se adoptó la Política de Seguridad y Privacidad de la Información de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL S.A. E.S.P. OFICIAL, con el propósito de proteger la información y los activos de información frente a amenazas y vulnerabilidades, garantizando su confidencialidad, integridad y disponibilidad.

2.- Que el proceso de Gestión Tecnológica realizó la actualización de la Política de Seguridad y Privacidad de la Información, generando el documento GT-O-001 Versión 01, con fecha de vigencia 4 de junio de 2026, mediante solicitud realizada al SIG en el Formato SG-R-038 Solicitud de elaboración, actualización o eliminación de documentos de fecha 04-06-2026, incorporando la modernización de su contenido, la actualización de terminología y definiciones, así como nuevos lineamientos relacionados con Inteligencia Artificial, Teletrabajo y Conexiones Remotas, Phishing e Ingeniería Social, Ransomware y BYOD (Bring Your Own Device), en concordancia con la normativa vigente.

3.- Que igualmente se incorporó nueva normatividad regulatoria que fortalece el Modelo de Seguridad y Privacidad de la Información, estableciendo lineamientos adicionales que se encuentran identificados en la matriz de requisitos legales del proceso de Gestión Tecnológica.

4.- Que mediante Resolución No. 166 de 2020 se modificó la Resolución No. 0655 del 29 de junio de 2019, mediante la cual se integra y establece el reglamento de funcionamiento

---0184

29 JUL 2026

del Comité Institucional de Gestión y Desempeño de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL S.A. E.S.P. OFICIAL.

5.- Que el Decreto 338 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones estableció los lineamientos generales para fortalecer la gobernanza de la seguridad digital.

6.- Que mediante Resolución No. 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

7.- Que mediante Resolución No. 2239 de 2024 del Ministerio de Tecnologías de la Información y las Comunicaciones, "Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio-Fondo Único de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la Resolución 448 de 2022". La cual se toma como referencia.

8.- Que la Guía N. 2 de MINTIC, fue tomada como documento referencia para la elaboración de la Política general y privacidad de la información.

9.-Que MINTIC establecido la guía para la implementación de seguridad de la información MIPYME y el Modelo de seguridad de la información para la estrategia de Gobierno en Línea del Fondo de Tecnologías de la Información y la Comunicación.

10.- Que la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL S.A. E.S.P. OFICIAL, en cumplimiento de la normatividad vigente, como el Decreto 767 de 2022 de MINTIC, la Política de Gobierno Digital y de las actividades definidas en el Modelo Integrado de Planeación y Gestión – MIPG, debe mantener actualizada su Política de Seguridad y Privacidad de la Información.

11.- Que en virtud de lo anteriormente expuesto, el Gerente General de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL S.A E.S.P OFICIAL,

RESUELVE:

ARTÍCULO PRIMERO: Modificar la Resolución No. 0668 del 29 de junio de 2019 mediante la actualización de la Política de Seguridad y Privacidad de la Información contenida en el documento GT-O-001, Versión 01, con fecha de vigencia 4 de junio de 2026, aprobado por el comité del Sistema Integrado de Gestión, el cual hace parte integral del presente acto administrativo y consta de treinta (30) folios.

ARTÍCULO SEGUNDO: Incorporar a la Política de Seguridad y Privacidad de la Información los numerales 7.9 Inteligencia Artificial, 7.10 Teletrabajo y Conexiones

Remotas, 7.11 Phishing e Ingeniería Social, 7.12 Ransomware y 7.13 BYOD (Bring Your Own Device), así como las actualizaciones de terminología, definiciones y demás ajustes requeridos para su alineación con la normativa vigente.

ARTÍCULO TERCERO: Las demás disposiciones contenidas en la Resolución N. 0668 del 29 de junio de 2019 que no fueron modificadas mediante el presente acto administrativo, continúan vigentes.

ARTÍCULO CUARTO: El proceso de Gestión Tecnológica realizará la socialización de la presente actualización a todos los servidores públicos, trabajadores oficiales, contratistas y terceros que tengan acceso a los activos de información de la entidad.

ARTÍCULO QUINTO: La presente resolución rige a partir de la fecha de su expedición.

Dada en Ibagué, a los 29 JUL 2026

PUBLÍQUESE, COMUNIQUESE Y CÚMPLASE

ROBERTO SANTOFIMIO VARÓN
Gerente General

Elaboró: Ing. Carlos Andrés Camacho Acuña — Prof. Especializado III — Gestión Tecnológica

Revisión Jurídica: Dr. John Jairo Medina Diez- Asesor Externo

VoBo: Dra. Sandra Velez Bocanegra — Directora Administrativa y Financiera

VoBo.: Dr. German Dario Fonseca Salcedo - Secretario General

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IBAL SA ESP OFICIAL

ELABORÓ:	REVISÓ Y APROBO:
Equipo de trabajo del proceso	Comité del Sistema Integrado de Gestión

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las políticas de seguridad definidas en el presente documento están dirigidas a los funcionarios, contratistas, practicantes y terceros de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL. Su cumplimiento es obligatorio y tiene como fin proteger la información y otros activos informáticos de amenazas y vulnerabilidades, garantizando la integridad, confidencialidad y disponibilidad de la información institucional.

El Grupo Tecnológico y de Sistemas de IBAL SA ESP OFICIAL reconoce que la información constituye un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes. Por tanto, la adecuada gestión y protección de la información es una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Para ello se implementa un modelo de gestión de seguridad de la información como herramienta que permite identificar y minimizar los riesgos, garantizar el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes, y alinear las actuaciones con la misión y visión de la entidad.

Toda persona que, en algún momento, tenga responsabilidad sobre el sistema de información o alguno de sus componentes, deberá adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información acorde con las necesidades de los diferentes grupos de interés.

En el contexto tecnológico actual, marcado por el auge de la Inteligencia Artificial, el teletrabajo, los ataques de phishing y ransomware, y el uso generalizado de dispositivos móviles, esta política se actualiza para incluir lineamientos específicos que respondan a estos nuevos escenarios de riesgo.

2. OBJETIVOS

De acuerdo con lo anterior, se establecen los siguientes objetivos de seguridad y privacidad de la información:

- Coordinar de manera armónica las soluciones de TI de mediano y largo plazo en cuanto a tecnología, sistemas de información y gestión dentro de la entidad.
- Documentar la configuración de las redes de comunicación implantadas en la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.
- Establecer las políticas e instructivos para la seguridad de la información.
- Administrar y monitorear la integridad de las bases de datos y establecer los procedimientos de recuperación de desastres.
- Minimizar el riesgo en las funciones de las diferentes áreas ejercidas por la empresa.
- Desempeñar los principios de seguridad de la información.
- Reforzar la cultura de seguridad de la información entre funcionarios, terceros, practicantes y usuarios de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.
- Garantizar la continuidad de las actividades frente a posibles incidentes.
- Definir lineamientos para el uso responsable de herramientas de Inteligencia Artificial, conexiones remotas, dispositivos móviles y medios digitales emergentes.
- Implementar, ejecutar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos alineados con las necesidades de la empresa y los requerimientos regulatorios.

3.DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas técnicas, operativas, organizadas y legales que permiten a las organizaciones resguardar y proteger la información, manteniendo la confidencialidad, la disponibilidad e integridad de la misma. Se encarga de garantizar la integridad, confidencialidad y disponibilidad de nuestra información.

La información es considerada un activo esencial en las actividades de la organización. Por ello, se deben establecer estrategias que permitan el control y administración de los datos, así como el uso adecuado de los recursos informáticos tanto de hardware como de software.

4. ALCANCE

Esta política aplica a todos sus funcionarios, terceros, aprendices, practicantes, proveedores y partes interesadas en utilizar y manejar la información y los servicios de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL. Incluye también a quienes accedan a los sistemas institucionales desde dispositivos personales o en modalidad de teletrabajo.

El incumplimiento al presente documento podrá presumirse como causa de responsabilidad administrativa y/o disciplinaria, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

5. TERMINOLOGÍA Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Amenaza: Causa potencial de un incidente no deseado que puede provocar daño a un sistema o a la organización. Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS). (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Antispam: Producto, herramienta, servicio o mejor práctica que detiene el correo no deseado antes de que se convierta en una molestia para los usuarios.

Antivirus: Categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Backups: Copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Base de Datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

BYOD (Bring Your Own Device): Práctica mediante la cual un funcionario utiliza su propio dispositivo móvil (celular, tableta, portátil personal) para acceder a sistemas, aplicaciones o información institucional. Implica riesgos adicionales de seguridad que deben ser gestionados mediante controles específicos.

Confidencialidad: Acceso a la información únicamente por parte de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]: característica o propiedad por la que la información no está disponible o revelada a individuos, entidades o procesos no autorizados.

Control de Acceso: Mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Firewall: Aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.

Hardware: Características técnicas y físicas de las computadoras.

Inteligencia Artificial (IA): Conjunto de tecnologías que permiten a los sistemas informáticos realizar tareas que normalmente requieren inteligencia humana, como procesamiento de lenguaje natural, generación de texto, imágenes o código. En el contexto institucional, su uso implica riesgos de fuga de información si se emplean herramientas no autorizadas con datos confidenciales.

Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.

IP: Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo habitualmente una computadora dentro de una red que utilice el protocolo IP.

Phishing: Técnica de ingeniería social mediante la cual un atacante suplanta la identidad de una entidad de confianza (banco, entidad gubernamental, proveedor de servicios) para engañar a la víctima y lograr que revele información confidencial como contraseñas, datos personales o credenciales de acceso. Se presenta principalmente a través de correo electrónico, mensajes de texto o llamadas telefónicas.

Plan de Contingencia: Instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Ransomware: Tipo de software malicioso que, al infectar un equipo o red, cifra los archivos y sistemas, impidiendo el acceso a la información, y exige un pago (rescate) para restaurar el acceso. Representa una de las amenazas más críticas para la continuidad operacional de las organizaciones.

Redes: Término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables). La transmisión y la recepción se realizan a través de puertos.

Riesgo: El efecto de la incertidumbre sobre los objetivos.

Servidores: Computador que responde peticiones o comandos de un computador cliente. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sistemas de Información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Software: Programas y documentación de respaldo que permite y facilita el uso del computador. El software controla la operación del hardware.

Spam: También conocido como correo basura. Correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo.

Teletrabajo: Modalidad laboral en la que el funcionario desempeña sus funciones desde un lugar distinto a las instalaciones de la entidad, haciendo uso de tecnologías de la información y las comunicaciones. Implica el acceso remoto a sistemas y datos institucionales desde redes externas, lo que requiere controles adicionales de seguridad.

UTM (Unified Threat Management): Término de seguridad de la información que se refiere a una sola solución de seguridad que ofrece varias funciones de protección en un solo punto en la red.

VPN (Virtual Private Network): Red privada virtual que permite establecer una conexión segura y cifrada entre un dispositivo y una red corporativa a través de Internet, protegiendo la información transmitida de accesos no autorizados.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alta Dirección de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, reconociendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Esta política aplica a la entidad según lo definido en el alcance: funcionarios, terceros, aprendices, practicantes, proveedores y ciudadanía en general. Las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

1. Minimizar el riesgo en las funciones más importantes de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de sus usuarios y empleados.
5. Apoyar la innovación tecnológica.
6. Proteger los activos tecnológicos.
7. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
8. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.
9. Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la empresa y a los requerimientos regulatorios.
10. Establecer lineamientos para el uso seguro y responsable de herramientas de Inteligencia Artificial, conexiones remotas y dispositivos personales en el entorno laboral.

PRINCIPIOS

A continuación, se establecen los principios de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de sus funcionarios, terceros, aprendices, practicantes, proveedores y partes interesadas.
- Protegerá la información generada, procesada o resguardada por los procesos de la empresa, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio interno en outsourcing.
- Protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debidos a un uso incorrecto de esta.
- Protegerá su información de las amenazas originadas por parte del personal.
- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlará la operación de sus procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Adoptará buenas prácticas en el uso de herramientas de Inteligencia Artificial, previniendo la exposición de información confidencial a plataformas no autorizadas.

7. POLÍTICAS Y CONTROLES

7.1 POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

La Alta Dirección de la empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL se compromete a apoyar activamente la seguridad de la información, lo cual se verá reflejado en la inclusión de la temática en el Comité Institucional de Gestión de Desempeño MIPG, como instancia orientadora de la implementación de la estrategia de gobierno en línea. Las funciones de seguridad de la información del Comité incluyen:

1. Coordinar la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información en nombre de la entidad.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la entidad.
5. Recomendar roles y responsabilidades específicos relacionados con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad los documentos generados al interior del Comité de Seguridad de la Información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

7.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.2.1 Política de Autorización para los Servicios de Procesamiento de Información

Objetivo: Minimizar los riesgos de falla en los sistemas, velar por la utilización adecuada de los recursos y garantizar que estos contribuyan con el cumplimiento de los objetivos institucionales.

Política: El Grupo Tecnológico y de Sistemas será el responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de desarrollo, pruebas y producción, y de toda la infraestructura tecnológica relacionada, de conformidad con las mejores prácticas y reglas internacionales de seguridad informática.

Para la puesta en producción de aplicativos nuevos o actualizaciones, estas deberán estar evaluadas de manera minuciosa para evitar la redundancia en las salidas de información y/o errores de cálculo. Esta revisión deberá estar sustentada con un acta emitida por el responsable de la ejecución del proceso.

7.2.2 Política de Confidencialidad de la Información

Todos los funcionarios que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por el IBAL, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso, so pena de las investigaciones disciplinarias a las que haya lugar.

7.3 GESTIÓN DE ACTIVOS

7.3.1 Política de Generación y Restauración de Copias de Seguridad

Objetivo: Evitar la pérdida de información por daños en los discos duros, eliminación errónea de archivos o manipulación inadecuada de información, mediante la generación de copias actualizadas de la información.

Política: La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL tiene la siguiente infraestructura de la información:

Información en arquitectura cliente/servidor:

Esta información se encuentra almacenada de manera ordenada, centralizada en bases de datos, en servidores con alta disponibilidad, con un propósito específico: estar disponible para ser accedida o procesada por los funcionarios del IBAL mediante el uso de software o aplicaciones informáticas.

Información de herramientas ofimáticas:

Esta información está almacenada de manera descentralizada en cada uno de los computadores de los funcionarios del IBAL, organizada en archivos, su uso es individual y tienen como fin apoyar las actividades propias de cada funcionario.

Información de Equipos de Comunicación:

Esta información se encuentra almacenada en los equipos de comunicación y corresponde a la configuración que se realiza de cada dispositivo. Es de vital importancia, ya que por medio de esta se integran todos los elementos activos de una red de comunicaciones.

El Grupo Tecnológico y de Sistemas del IBAL deberá garantizar la disponibilidad y el respaldo de la información en la arquitectura cliente/servidor y la información de los equipos de comunicación que se encuentren bajo su responsabilidad. Igualmente deberá garantizar la disponibilidad del software y aplicaciones que utilizan los funcionarios de la empresa con el fin de acceder a la información almacenada.

La información de las herramientas ofimáticas deberá ser protegida y respaldada por cada funcionario de la empresa, así como la de los otros dispositivos de comunicación que estén bajo su responsabilidad. Esta actividad será realizada de acuerdo con los lineamientos que determine el Grupo Tecnológico y de Sistemas del IBAL.

Controles: Estos controles están documentados en el Instructivo para la Realización de Copias de Respaldo GT-I-003, donde se describe el responsable, periodicidad y registro como evidencia.

SERVIDOR DE BASE DE DATOS:

En este servidor se almacenan las copias de respaldo de las bases de datos y del registro de transacciones del SOFTWARE ERP; esta información se encuentra en el motor de base de datos SQL SERVER.

Servidor de Respaldo:

1. En este servidor se respalda la información que los funcionarios del IBAL almacenan en sus computadores y que son elaboradas con herramientas ofimáticas como Microsoft Office.
2. Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.
3. El Grupo Tecnológico y de Sistemas, como evidencia de las copias de seguridad, cuenta con el registro GT-R-003 Seguimiento de Copias de Respaldo.
4. Las copias de respaldo son enviadas automáticamente desde el almacenamiento en los servidores del IBAL, a una unidad de almacenamiento en la Nube (Google Drive), que la empresa tiene contratado con una capacidad de 1 Terabyte, administrada única y exclusivamente por el Grupo Tecnológico y de Sistemas.
5. El respaldo de la información almacenada en los equipos de los funcionarios se realizará mediante el Software SYNOLOGY, herramienta autorizada por el Grupo Tecnológico y de Sistemas para tal fin. Cada funcionario deberá verificar periódicamente que sus copias de respaldo se ejecuten correctamente y que los archivos puedan ser recuperados cuando sea necesario.
6. Los contratistas (OPS y apoyo a la gestión) deben entregar al supervisor del contrato una copia de respaldo de toda la información institucional almacenada en su equipo al momento de finalizar el contrato. Esta obligación aplica especialmente a quienes desarrollen sus labores desde equipos personales. El supervisor del contrato deberá verificar el cumplimiento de esta entrega como condición para la liquidación del contrato.

7.3.2 Políticas para el Manejo de los Datos

Uso Compartido

Política: El usuario que autoriza el uso compartido de carpetas es responsable de las acciones y el acceso a la carpeta de la información compartida. Debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta. Además, debe asegurarse de que el usuario autorizado cuente con el antivirus autorizado.

Antivirus:

Política: Todos los equipos de la Empresa deben tener instalado, en funcionamiento, actualizado y debidamente licenciado un antivirus, el cual será suministrado por el Grupo Tecnológico y de Sistemas.

El Grupo Tecnológico y de Sistemas proporcionará herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica y los servicios que se ejecutan en la misma.

Todos los archivos anexos a los mensajes recibidos en el correo institucional estarán sujetos al análisis del antivirus, y el destinatario final recibirá solo los que hayan sido exitosos.

Los usuarios que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a Sistemas para que le brinden el soporte técnico de erradicación del virus.

Administración de Bases de Datos y Seguridad de la Información:

Objeto: Administrar y Monitorear la Integridad de las Bases de Datos y establecer los Procedimientos de Recuperación de Desastres.

Política: El Grupo Tecnológico y de Sistemas generará copias de respaldo de la información de manera automática, mediante la producción de información espejo en dos servidores y/o almacenamiento redundante. Para lo cual se estableció como procedimiento la ejecución de las tareas programadas de Windows , de SQL y NAS , que de manera autónoma produzca copia de la información almacenada en las bases de datos sobre un servidor de Backup y/o NAS , Y copia de ella en un espacio de almacenamiento en la nube (Google Drive). Este proceso se realiza con una periodicidad diaria.

Controles: Estos controles están documentados en el Instructivo Para la Gestión y Protección de la seguridad de la información GT-I-006, donde se describe el responsable y registro como evidencia.

SEGURIDAD DE LA INFORMACIÓN

La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por lo tanto, es un compromiso su protección como estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Por lo que se implementará un modelo de gestión de seguridad de la información como herramienta que permita identificar y minimizar los riesgos a los cuales se expone la información y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Toda persona que tenga responsabilidad, en algún momento, con el sistema de información o de alguno de sus componentes, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Medios de Almacenamiento Removibles:

Política: Los funcionarios que contengan información confidencial de propiedad de la entidad en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso. La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible debe ser protegida mediante cifrado o contraseñas. No está autorizado el uso de dispositivos de almacenamiento externos removibles con información del IBAL en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

Protección de Documentos para su Distribución

Política: Los documentos que son distribuidos o compartidos con terceros tendrán como marca de agua la clasificación de la información contenida, y su copia magnética se realizará en formato PDF de solo lectura, para impedir la modificación o eliminación accidental o intencional de los datos y la pérdida de la confidencialidad inadvertida.

7.4 USO DEL CORREO ELECTRÓNICO

Objetivo: Garantizar el uso adecuado y seguro del correo electrónico institucional como herramienta de comunicación oficial de la entidad.

Política: El Grupo Tecnológico y de Sistemas es el encargado de definir los nombres, estructura y plataforma que se debe utilizar para la cuenta de correo institucional de cada dependencia. Las cuentas se crean desde Google Workspace, con dominio @ibal.gov.co.

Controles: Los controles están documentados en el instructivo MANTENIMIENTO PAGINA WEB Y CORREOS INSTITUCIONALES GT-R-001

Para la creación y configuración de un nuevo correo institucional se debe realizar solicitud escrita o mediante correo electrónico desde una de las cuentas registradas en el dominio WEB de la empresa IBAL SA ESP OFICIAL, al correo sistemas@ibal.gov.co.

Todos los usuarios internos de la empresa que pertenezcan al área administrativa tienen asignado correo institucional para las actuaciones inherentes a la empresa.

Los mensajes y la información contenida en los correos electrónicos deben estar relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del IBAL. El correo institucional no debe ser utilizado para actividades personales.

Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios del IBAL y el personal provisto por terceras partes.

Todo correo institucional debe ser descargado periódicamente de la bandeja de entrada para así liberar y dar capacidad al servidor. Todos los correos de publicidad, cadenas y demás correos que no hagan parte de las actividades de la empresa, deberán ser borrados en el mismo instante que se lee, La información institucional contenida en el buzón es propiedad del IBAL SA ESP OFICIAL.

El usuario responsable del correo institucional debe evitar abrir los adjuntos de correos de origen desconocido o que contengan palabras en inglés, a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.

7.5 ACCESO A INTERNET, INTRANET Y PORTAL WEB

Objetivo: Proveer la información necesaria a los usuarios sobre las políticas y controles a aplicar para hacer uso de los recursos de Internet, Intranet y portal Web del IBAL SA ESP OFICIAL.

Política: En el IBAL SA ESP OFICIAL el acceso a Internet e Intranet es permitido a todos los trabajadores y contratistas para facilitar el desarrollo de los procesos propios de la Entidad, pero deben cumplir con los controles de acceso y uso implementados.

Los usuarios del servicio de Internet deben evitar la descarga de software, así como la instalación en su computador o dispositivos móviles asignados para el desempeño de sus labores. Los usuarios de Internet no están autorizados para descargar software, música, juegos, películas, protectores de pantalla, ni para efectuar pagos, compras de bienes o servicios a través de los canales de acceso a internet del IBAL SA ESP OFICIAL, salvo cuando medie autorización.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento; se bloquearán mediante el firewall.

Los canales de acceso a internet de la Entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

La IBAL SA ESP OFICIAL se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad, restringir accesos y recursos.

Para facilitar las comunicaciones internas, el Grupo Tecnológico y de Sistemas instalará en cada computador un software de mensajería instantánea (Spark) para lo cual asignará un usuario y una contraseña a cada funcionario. Esta mensajería deberá ser utilizada para fines empresariales y netamente laborales. Los usuarios tienen prohibido el envío de cadenas de mensajes de cualquier tipo.

Publicación Portal Web:

Esta actividad está documentada en el Instructivo Mantenimiento Pagina web y correos Institucionales GT-I-001.

La página web de la empresa www.ibal.gov.co fue diseñada incluyendo todas las exigencias impuestas por el Ministerio de las TIC en la estrategia de Gobierno en Línea, así como cada uno de los componentes descritos en el Manual Estrategia Gobierno en Línea en su última versión, y lo estipulado en la Ley 1712 de 2014 y Resolución 3564 del 31 de diciembre de 2015 Anexo 1 Estándares para publicación y divulgación de información, Anexo 2 Lineamientos sobre el formulario electrónico para la recepción de solicitudes de información pública.

La información de los procesos que requiere ser publicada, debe ser enviada al Grupo Tecnológico y de sistemas por el jefe del área encargada de generar la información, quien será el responsable del contenido de la publicación, de acuerdo a lo descrito en el instructivo de publicación en la página Web GT-I-001.

En cumplimiento a la normatividad vigente, mediante la Resolución N. 0439 del 9 de julio de 2021 , se adopta el esquema de publicación de información de la empresa ibaguereña de acueducto y alcantarillado IBAL SA ESP OFICIAL", como instrumento para informar, de forma ordenada, a la ciudadanía, interesados y usuarios, sobre la información publicada y que publicará, conforme al principio de divulgación proactiva de la información previsto en el artículo 3° de la Ley 1712 de 2014.

Este esquema presenta toda la información alojada en la página para conocimiento y acceso público, describiendo entre otras características el formato del documento, Descripción, frecuencia de actualización y el área o dependencia responsable de su producción y actualización.

Este documento esta publicado en la página web de la empresa www.ibal.gov.co , Menú Transparencia, Link Datos Abiertos - Instrumentos de gestión de la información- https://ibal.gov.co/wp-content/uploads/2026/02/Esquema-de-Publicacion-de-Informacion-2026.pdf

La página web www.ibal.gov.co , es auditada anualmente por la Procuraduría General de la Nación, a través del aplicativo Índice de Transparencia y Acceso a la información Pública (ITA), mediante el cual vigila el cumplimiento de la Ley 1712 de 2014 y las demás normas que la regulan.

7.6 CONFIGURACIÓN Y ADMINISTRACIÓN DE LAS REDES

Objetivo: Documentar la configuración de las redes de comunicación implantadas en la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.

Política: Los cambios de configuración de red solo los realizará el Grupo Tecnológico y de Sistemas. Se prohíbe el cambio de configuración de la Red LAN, Conexión de área local, direccionamiento y configuración en los equipos de cómputo.

Para evitar sanciones establecidas por la Ley, se prohíbe la instalación de software no autorizado. El Grupo Tecnológico y de Sistemas realizará revisión dentro de los mantenimientos de todos los computadores que pertenecen al IBAL, para proceder a desinstalar el software no autorizado o sin licencias. De igual manera revisará inconsistencias y cambios realizados en la configuración de la red.

Si se llegara a comprobar que algún funcionario del IBAL está llevando a cabo estos procedimientos sin autorización, dicha situación será notificada a la Oficina de Control Disciplinario.

Las redes de comunicaciones LAN y WAN del IBAL SA ESP OFICIAL son gestionadas a través de un UTM, ubicado en el cuarto de telecomunicaciones y servidores del Grupo Tecnológico y de Sistemas.

Controles: Los controles están documentados en el Instructivo Administración de redes y comunicaciones GT-I-002.

7.7 ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE Y HARDWARE

Política: Toda adquisición de recurso tecnológico en la Empresa IBAL SA ESP OFICIAL deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte del Grupo Tecnológico y de Sistemas.

Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.

Adquisición de Equipos de Cómputo:

El Grupo de Sistemas verificará las características y el estado de todos los equipos digitales y análogos que ingresan a la Empresa IBAL SA ESP OFICIAL, previo al ingreso a almacén. Todos los dispositivos adquiridos deben contar con la garantía de fábrica, licencias de sistema operativo y software ofimático.

Actividad documentada en el Procedimiento Manejo de Licencias Adquiridas por el IBAL SA ESP OFICIAL GT-P-002

Mantenimiento de Equipos, Impresoras y Scanner:

Actividad documentada en el Procedimiento Gestión Tecnológica GT-P-001. Cuando se presenten fallas en el hardware, el usuario deberá reportarlo al Grupo Tecnológico y de Sistemas, donde se diligencia el formato GT-R-001. No se autoriza a ningún usuario final reparar, modificar los computadores, impresoras, periféricos o software instalados en ellos.

Todo software instalado en equipos del IBAL será autorizado o instalado por el Grupo Tecnológico y de Sistemas, el cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

7.8 USO DE SERVIDORES Y CONTROL DE ACCESOS

Política: El Grupo Tecnológico y de Sistemas es el responsable de verificar la instalación y configuración de todo servidor que sea conectado a la red, y de implementar mecanismos de seguridad física y lógica.

7.8.1 Control de Accesos Lógico

Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas de información.

Política: Las tareas realizadas por los usuarios en cada uno de los sistemas de información del IBAL SA ESP OFICIAL serán controladas por medio de la creación de cuentas de usuario, a las cuales se les controlarán los privilegios de acceso, de conformidad con los roles y perfiles establecidos.

Para la creación, actualización o bloqueo de cuentas de usuario, el jefe del área correspondiente realizará la solicitud escrita o al correo de sistemas@ibal.gov.co especificando el perfil requerido para dicho usuario, detallando las diferentes opciones a las que deberá tener acceso. Será responsabilidad del jefe de cada área reportar al Grupo Tecnológico el retiro de funcionarios para poder inhabilitarlos en el sistema de información.

Se establecerán privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información del IBAL. Los funcionarios y el personal provisto por terceras partes tendrán acceso únicamente a la información necesaria para el desarrollo de sus labores.

El usuario deberá conservar su contraseña y usuario teniendo en cuenta el riesgo que presenta el manejo inadecuado o préstamo de su perfil de usuario en el sistema de información. Las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Los funcionarios serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia las darán a conocer a otras personas, ni harán uso de contraseñas ajenas.

Se precisa que todos los usuarios cambien periódicamente la contraseña en el sistema. Todos los usuarios deben cerrar sesión cuando no van a hacer más uso del aplicativo o cuando van a abandonar su estación de trabajo.

7.8.2 Control de Acceso Físico

Política: El ingreso al área de servidores y de procesamiento de información será restringido y controlado, y solo se autorizará, por el jefe del área, con fines o propósitos esenciales.

7.8.3 Seguridad Física y del Entorno

Política: Los equipos que hacen parte de la infraestructura tecnológica del IBAL SA ESP OFICIAL, tales como servidores, estaciones de trabajo, centro de cableado, aires acondicionados, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

Está prohibido fumar, beber o consumir alimentos en las áreas de servidores. No está autorizado almacenar material peligroso, combustible e inflamable en sitios cercanos a las áreas de procesamiento o almacenamiento de información.

7.9 INTELIGENCIA ARTIFICIAL — USO RESPONSABLE

IMPORTANTE: Las herramientas de Inteligencia Artificial (IA) pueden ser útiles para la gestión institucional, pero su uso inadecuado representa un riesgo crítico de fuga de información confidencial. Esta sección establece los lineamientos obligatorios para el uso de IA en el IBAL SA ESP OFICIAL.

Objetivo: Establecer lineamientos para el uso seguro y responsable de herramientas de Inteligencia Artificial por parte de los funcionarios y terceros del IBAL SA ESP OFICIAL, previniendo la exposición no autorizada de información institucional confidencial.

Política: El uso de herramientas de IA en el ejercicio de funciones institucionales estará sujeto a las siguientes condiciones:

1. Está prohibido ingresar información confidencial, datos personales de ciudadanos, contraseñas, información financiera o documentos internos reservados en herramientas de IA públicas o no autorizadas por el Grupo Tecnológico y de Sistemas (ej.: ChatGPT, Copilot no institucional, Gemini en cuentas personales).
2. Las herramientas de IA autorizadas para uso institucional son exclusivamente las habilitadas por el Grupo Tecnológico y de Sistemas. Actualmente: Google Gemini dentro del entorno de Google Workspace institucional. Esta lista puede actualizarse mediante comunicado oficial del área de Tecnología.
3. La información generada por herramientas de IA deberá ser verificada por el funcionario antes de ser utilizada en documentos, informes, comunicaciones oficiales o decisiones administrativas. La IA puede cometer errores, omisiones o generar datos incorrectos.
4. El uso de IA no exime al funcionario de su responsabilidad sobre la información que produce, divulga o firma en ejercicio de sus funciones. La responsabilidad final es siempre del funcionario.
5. Los desarrolladores o contratistas de software que presten servicios al IBAL no podrán incorporar herramientas de IA externas en los sistemas institucionales sin previa autorización del Grupo Tecnológico y de Sistemas.
6. Ante cualquier duda sobre si una herramienta de IA es segura para usarla con información institucional, el funcionario deberá consultar al Grupo Tecnológico y de Sistemas antes de utilizarla.
7. Cualquier incidente relacionado con el uso indebido de IA o exposición de información institucional en plataformas de IA deberá ser reportado de inmediato al Grupo Tecnológico y de Sistemas.

Controles: El Grupo Tecnológico y de Sistemas velará por la sensibilización periódica de los funcionarios respecto al uso seguro de IA, y realizará monitoreo de las herramientas utilizadas en el entorno institucional.

7.10 TELETRABAJO Y CONEXIONES REMOTAS

Objetivo: Garantizar que el acceso remoto a los sistemas y la información del IBAL SA ESP OFICIAL se realice de forma segura, minimizando los riesgos derivados de conexiones desde redes externas o entornos no controlados.

Política: Los funcionarios que realicen teletrabajo o trabajo remoto deberán acogerse a los siguientes lineamientos:

1. El acceso a los sistemas institucionales desde ubicaciones remotas se realizará únicamente a través de los canales y herramientas autorizadas por el Grupo Tecnológico y de Sistemas. Cuando se disponga de VPN institucional, su uso será obligatorio para acceder a recursos internos de la entidad.
2. Está prohibido acceder a información institucional confidencial desde redes Wi-Fi públicas (centros comerciales, cafés, aeropuertos) sin el uso de VPN institucional. Las redes abiertas pueden ser interceptadas por terceros.
3. El funcionario que realice teletrabajo deberá asegurar que su red doméstica cuente con contraseña robusta y que el router esté configurado con las actualizaciones de seguridad vigentes. Se recomienda no compartir la red de trabajo con dispositivos de entretenimiento o de terceros.
4. Los equipos utilizados para el teletrabajo deben cumplir con las mismas políticas de seguridad aplicadas a los equipos corporativos: antivirus activo, contraseña de acceso, sesión bloqueada cuando no se use.
5. Al finalizar la jornada de teletrabajo, el funcionario deberá cerrar sesión en todos los sistemas institucionales y desconectarse de la VPN.
6. El Grupo Tecnológico y de Sistemas establecerá, a través del Instructivo de Trabajo Remoto, los procedimientos específicos, herramientas autorizadas y mecanismos de acceso remoto disponibles para los funcionarios.

7.11 PHISHING E INGENIERÍA SOCIAL

ALERTA: El phishing y la ingeniería social son actualmente las principales causas de incidentes de seguridad en entidades públicas. Todo funcionario debe conocer y aplicar estos lineamientos.

Objetivo: Prevenir que los funcionarios del IBAL SA ESP OFICIAL sean víctimas de ataques de phishing o ingeniería social que comprometan la seguridad de la información institucional.

Definición: El phishing es un intento de engaño mediante correo electrónico, mensaje de texto, llamada telefónica o redes sociales, en el que el atacante suplanta la identidad de una entidad confiable para obtener información confidencial (contraseñas, datos personales, accesos a sistemas). La ingeniería social es la manipulación psicológica de personas para obtener información o inducirlas a realizar acciones que comprometan la seguridad.

Política:

1. El Grupo Tecnológico y de Sistemas NUNCA solicitará contraseñas, credenciales de acceso o información personal a través de correo electrónico, mensaje de texto o llamada telefónica. Ante cualquier solicitud de este tipo, el funcionario deberá abstenerse de responder y reportarla inmediatamente.
2. Ante la recepción de un correo, mensaje o llamada con las siguientes características, el funcionario deberá tratarlo con máxima desconfianza: urgencia extrema para actuar de inmediato, solicitud de contraseñas o datos personales, remitente desconocido o dirección de correo que no corresponde al dominio oficial, enlaces que al pasar el cursor muestran una URL diferente a la esperada.
3. Antes de hacer clic en un enlace recibido por correo o mensaje, el funcionario deberá verificar que la URL de destino corresponde al sitio oficial esperado. En caso de duda, acceder directamente al sitio web desde el navegador sin usar el enlace.
4. Los correos sospechosos de phishing deberán ser reportados al Grupo Tecnológico y de Sistemas (sistemas@ibal.gov.co) antes de abrirlos, responderlos o hacer clic en sus enlaces o adjuntos.
5. El Grupo Tecnológico y de Sistemas podrá realizar ejercicios de simulación de phishing para evaluar el nivel de preparación de los funcionarios y brindar formación específica.
6. Ningún funcionario deberá proporcionar información confidencial o credenciales institucionales a terceros que se identifiquen como personal de soporte técnico, sin verificar previamente su identidad a través de un canal oficial conocido.

7.12 RANSOMWARE — PREVENCIÓN Y RESPUESTA

CRÍTICO: El ransomware puede dejar inoperante la totalidad de los sistemas institucionales. Conocer los pasos de respuesta inmediata puede limitar significativamente el impacto de un ataque.

Objetivo: Establecer lineamientos de prevención y un protocolo de respuesta ante incidentes de ransomware que minimicen el impacto sobre la operación del IBAL SA ESP OFICIAL.

Política:

1. Todos los equipos deben mantener el antivirus actualizado y activo en todo momento. El Grupo Tecnológico y de Sistemas gestionará las actualizaciones de forma centralizada.
2. No se deben abrir adjuntos de correos de remitentes desconocidos, ni ejecutar archivos descargados de sitios no autorizados.
3. Se deben realizar copias de seguridad periódicas conforme a la política establecida en la sección 7.3.1. Estas copias son la principal defensa ante un ataque de ransomware.
4. El sistema operativo y las aplicaciones institucionales deben mantenerse actualizados con los parches de seguridad vigentes, gestionados por el Grupo Tecnológico y de Sistemas.

Protocolo de respuesta ante sospecha de ransomware:

1. Si el funcionario observa mensajes inusuales en pantalla, no puede abrir archivos que antes funcionaban correctamente, o detecta un comportamiento anormal del equipo, debe DETENER inmediatamente la actividad que está realizando.
2. Desconectar el equipo de la red de inmediato: desconectar el cable de red o desactivar el Wi-Fi. NO apagar el equipo.
3. Reportar el incidente de manera inmediata al Grupo Tecnológico y de Sistemas, informando la ubicación del equipo, la hora aproximada del inicio del comportamiento inusual y los archivos o sistemas afectados.
4. No intentar recuperar archivos por cuenta propia ni pagar ningún rescate. El pago no garantiza la recuperación de la información y puede financiar actividades delictivas.
5. No conectar dispositivos USB u otros medios de almacenamiento al equipo potencialmente comprometido.
6. El Grupo Tecnológico y de Sistemas activará el Plan de Contingencia correspondiente y coordinará las acciones de recuperación.

7.13 DISPOSITIVOS MÓVILES PERSONALES (BYOD)

Objetivo: Regular el uso de dispositivos móviles personales para acceder a sistemas e información institucional del IBAL SA ESP OFICIAL, minimizando los riesgos de seguridad asociados.

Política:

1. El uso de dispositivos personales (celulares, tabletas, portátiles personales) para acceder a sistemas institucionales está permitido únicamente con autorización del Grupo Tecnológico y de Sistemas y bajo las condiciones establecidas en este artículo.
2. Todo dispositivo personal utilizado para acceder a información institucional debe contar con: bloqueo de pantalla activo (PIN, patrón o huella digital), antivirus instalado y actualizado, sistema operativo actualizado con los últimos parches de seguridad.
3. No se instalarán aplicaciones de origen desconocido o no verificado en dispositivos desde los cuales se acceda a sistemas del IBAL.
4. Está prohibido acceder a información institucional desde dispositivos personales en redes Wi-Fi públicas sin el uso de VPN institucional.
5. En caso de pérdida o robo de un dispositivo personal con acceso a sistemas o información del IBAL, el funcionario deberá reportarlo de manera inmediata al Grupo Tecnológico y de Sistemas para bloquear los accesos asociados al dispositivo.
6. El funcionario acepta que el IBAL SA ESP OFICIAL podrá revocar remotamente el acceso a los sistemas institucionales desde el dispositivo personal en caso de incidente de seguridad, pérdida o desvinculación del funcionario.
7. La información institucional no deberá ser almacenada de forma permanente en dispositivos personales. Los documentos institucionales trabajados desde dispositivos personales deberán eliminarse de estos una vez finalizado su uso.

7.14 REGISTRO Y AUDITORÍA

Política: Los sistemas de información que soporten los procesos críticos de la Empresa IBAL SA ESP OFICIAL contarán con registros de auditoría de las actividades de usuario, de operación y administración del sistema.

Los logs de auditoría deben proporcionar información relevante para soportar procesos de auditoría y para contribuir al cumplimiento de las políticas de seguridad de la información.

Los líderes de los procesos propietarios de la información definirán los criterios a auditar de acuerdo con los requerimientos internos o externos o con los datos que considere sensibles a hechos fraudulentos.

El acceso a los logs de auditoría será restringido solo a los administradores del Sistema y a los propietarios de información o a quien estos autoricen por medios escritos.

8.REGISTROS DE REFERENCIA

Las políticas de seguridad han sido formuladas teniendo como referencia los siguientes instrumentos normativos y técnicos:

- Norma NTC-ISO/IEC 27001
- Guía de elaboración de la política general y privacidad de la información de MINTIC
- Guía para la implementación de Seguridad de la Información MIPYME de MINTIC
- Modelo de seguridad de la información para la estrategia de Gobierno en Línea del Fondo de Tecnologías de la Información y la Comunicación
- Ley 1266 de 2008 — Hábeas Data
- Decreto 1083 de 2015 — Decreto Único Reglamentario del Sector de Función Pública
- Decreto 415 de 2016 — Fortalecimiento institucional en materia de TIC
- Decreto 1008 de 2018 — Lineamientos digitales de la política de gobierno digital
- Decreto 338 de 2022 — Lineamientos generales para fortalecer la gobernanza de la seguridad digital
- Resolución 746 de 2022 — Lineamientos adicionales para fortalecer el Modelo de Seguridad y Privacidad de la Información en Colombia
- Resolución N. 2239 de 2024 —Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación

9.CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO REALIZADO	IMPACTO QUE GENERA
2019-07-16	0	Versión inicial del documento.	
2026-06-04	01	Actualización integral: modernización del lenguaje, incorporación de los artículos 7.9 (Inteligencia Artificial), 7.10 (Teletrabajo y Conexiones Remotas), 7.11 (Phishing e Ingeniería Social), 7.12 (Ransomware), y 7.13 (BYOD — Dispositivos Móviles Personales). Actualización de terminología con nuevas definiciones. Revisión y alineación con normativa vigente.	Información actualizada y veraz del proceso