RESOLUCIÓN N° - 0668

(29 JUL 2019

"POR MEDIO DE LA CUAL SE ADOPTA LA POLITICA 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 la Ley 1266 de 2008 del Congreso de la república, "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."

2. Que el Decreto 1083 de 2015 del Departamento Administrativo de la Función Pública "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", en su Título 35 establece Lineamientos para el fortalecimiento en materia de Tecnologías de la información y las comunicaciones, Articulo 2.2.22.2.1 Políticas de gestión y desempeño institucional, Articulo 2.2.22.3.14 Integración de los planes institucionales y estratégicos al Plan de acción.

3. Que el Decreto 415 de 2016 del Departamento Administrativo de la Función Pública ""Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

4. Que el Decreto N° 1008 de 2018 del Ministro de Tecnologías de la Información y las Comunicaciones, "establece los lineamientos digitales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015".

5. Que mediante Resolución 0655 de 2018 "se integra y se establece el funcionamiento del comité institucional de gestión y desempeño de la empresa IBAL SA ESP OFICIAL.

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

7. Que MINTIC estableció 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.

8. Que conforme a lo anterior la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL S.A. E.S.P OFICIAL, por estar incluida dentro de los sujetos obligados le corresponde adoptar en cumplimiento al Plan de acción establecido dentro del MIPG y a la normatividad vigente la Política de seguridad y privacidad de la información de la empresa IBAL SA ESP OFICIAL.

9. 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: Adoptar al interior de la empresa IBAL SA ESP OFICIAL la Política de seguridad y privacidad de la información, documento aprobado por el comité del Sistema Integrado de Gestión GT-O-001 – Versión 0, la cual hace parte integral del presente acto administrativo en 26 folios.

ARTÍCULO SEGUNDO: La presente Resolución será socializada a todo el personal de la entidad para su conocimiento y aplicación.

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

Dada en Ibagué, a los 29 JUL 2019

PUBLÍQUESE, COMUNIQUESE Y CÚMPLASE

CIELO CONSTANZA MOICA SUSUNAGA
Gerente General (E)

Elaboró: Carlos Darío Marulanda Ocampo – Prof. Especializado III – Gestión Tecnológica

Revisó: Prof. Universitario

Vo.Bo.: Cielo Constanza Moica Susunaga – Directora Administrativa y Financiera

Vo.Bo.: Maria Victoria Bobadilla Polanía - Secretaria General

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

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

TABLA DE CONTENIDO

1. INTRODUCCION

Las políticas de seguridad definidas en el presente documento están dirigidas a los funcionarios de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, las cuales serán de obligatorio cumplimiento, a fin de proteger la información y otros activos informáticos de amenazas y vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información.

El Grupo Tecnológico y de Sistemas de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, reconoce la importancia de la información como un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, por lo tanto, es un compromiso la adecuada gestión de la información y la protección como estrategia orientada a la continuidad de la Empresa, 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 y regulatorios vigentes teniendo concordancia con la misión y visión de la empresa.

Para la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, la protección de la información hace alusión a 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 acorde con las necesidades de los diferentes grupos de interés.

2. OBJETIVOS

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

- Coordinar armónicamente las soluciones de TI de mediano y largo plazo en cuanto a tecnología, sistemas de información y la información, necesarios para la gestión dentro de la entidad.
- Documentar la configuración de las redes de comunicación que se tiene 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 por parte de los 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.
- La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL. implementa, ejecuta y mejora de forma continúa el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos de acuerdo a las necesidades y a los requerimientos regulatorios.

3. DEFINICION DE SEGURIDAD DE LA INFORMACION

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 buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. Se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información.

La información es considerada un activo esencial en las actividades de la organización, es por ello que 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 aicantarillado IBAL SA ESP OFICIAL.

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. TERMINOLOGIA 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).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daño un sistema o a la organización. (ISO/IEC 27000).

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

Amenaza: 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).

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

Antivirus: Antivirus es una 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, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Contraseña: Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña.

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

Riesgo: El riesgo es el efecto de la incertidumbre sobre los objetivos.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam.

Virus: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Administrador de equipo: Persona responsable de configurar, administrar controladores de dominio o equipos locales, sus cuentas de usuario, asignar contraseñas, permisos y ayudar a los usuarios a solucionar problemas de red.

Administrador de Bases de Datos (DBA): Persona responsable de los aspectos ambientales de una base de datos.

Backups: Es una 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: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Confidencialidad: Acceso a la información por parte únicamente de quienes esté 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: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

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.

Hardware: Se refiere a las características técnicas y físicas de las computadoras.

Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o Exactitud de la información de la organización. Es un 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 un computador) dentro de una red que utilice el protocolo IP.

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

Redes: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Servidores: Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

Sistemas de Información: Es un 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 pc. El software controla la operación del hardware.

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.

UTM: La gestión unificada de amenazas, que comúnmente se abrevia como UTM , es el termino de seguridad de la información que se refiere a una sola solución de seguridad y , por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red.

6. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alta Dirección de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, entendiendo 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, todo 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 objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de 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.*

PRINCIPIOS

Por consiguiente, se determinan los principios de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información alineado con el Sistema de Gestión de Seguridad de la Información de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI 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 (ej.: proveedores o usuarios), o como resultado de un servicio interno en outsourcing.*
- *Protegerá la información creada, procesada, transmitida o resguardada por sus procesos la Empresa, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
- *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.*

7. POLITICAS Y CONTROLES

7.1 POLITICAS 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 en el Comité Institucional de Gestión de Desempeño MIPG, como instancia orientadora de la implementación de la estrategia de gobierno en línea, de las siguientes funciones de seguridad de la información:

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 Nombre de la entidad.
5. Recomendar roles y responsabilidades específicos que se relacionen 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 de esta revisión 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 INFORMACION

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, personal 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 GESTION DE ACTIVOS

7.3.1 Política de Generación y Restauración 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 actualizados 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 esta 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 es por medio de esta que se integran todos los elementos activos de una red de comunicaciones.

Es importante señalar que 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.

ACTIVIDADES COPIA DE RESPALDO ARQUITECTURA CLIENTE/SERVIDOR Y EQUIPOS DE COMUNICACIÓN.

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 .

Bases de datos software SOLIN ERP:

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. Se realizarán copias de seguridad cuando los equipos de cómputo sean enviados a mantenimiento, previniendo así la perdida de información.
4. El Grupo Tecnológico y de sistemas como evidencias de las copias de seguridad cuenta con el registro GT-R-003 Seguimiento copias de respaldo.
5. 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, este servicio de almacenamiento está asociado a una cuenta de Gmail, la cual es administrada única y exclusivamente por el Grupo Tecnológico y de Sistemas.

7.3.2 Políticas para el Manejo de los Datos

Uso Compartido

Política: El usuario que autoriza el uso compartido de carpetas es responsable por las acciones y el acceso a la carpeta de la información compartida.

El usuario que autoriza la carpeta compartida debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta.

El usuario que autoriza la carpeta compartida debe asegurarse 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, anti spam, 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.

El Grupo Tecnológico y de Sistemas propenderá que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

El grupo tecnológico y de sistemas, a través de sus funcionarios, velara que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, anti spam, antimalware y que los usuarios posean las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

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.

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.

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 definió, que para la integridad de la información almacenada en las bases de datos corporativas se generaran Copias de respaldo de la Información de manera automática, mediante la producción de información espejo en dos servidores y almacenamiento redundante. Para lo cual se estableció como procedimiento la ejecución de las tareas programadas de Windows y de SQL, que de manera autónoma produzca copia de la información almacenada en las bases de datos sobre un servidor de Backup y copia de ella la genere en un espacio de almacenamiento

en la nube (google drive), este proceso se realiza con una periodicidad diaria al final del día.

Controles: Estos controles están documentados en el Instructivo Administración de Bases de Datos y Seguridad de la Información GT-I-005, 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, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información del IBAL, en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible, debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

Protección de Documentos para su Distribución

Política: los documentos que son distribuidos o compartidos con terceros, tendrán con 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 ELECTRONICO

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.

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

Las creaciones de los correos institucionales se hacen desde el cpanel del sitio web, es decir, desde el Hosting y se harán con terminación @ibal.gov.co. La configuración de los correos se hace también desde el Hosting dando espacio de almacenamiento de acuerdo a la necesidad.

Para creación y configuración de un nuevo correo institucional se debe realizar solicitud escrita mediante oficio dirigido al Grupo Tecnológico y de Sistemas 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 ser 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, garantizando la seguridad de la información, por cuanto 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 Ingles 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 dispositivo móviles asignados para el desempeño de sus labores. La descarga de software estará a cargo de la persona o grupo de personas definido por el grupo Tecnológico y de Sistemas, por lo tanto, los usuarios de internet no están autorizados para descargar software, música, juegos, películas, protectores de pantalla, etc. Así como efectuar pagos, compras de bienes o servicios a través de los canales de acceso a internet del IBAL SA ESP OFICIAL a título personal o de la Entidad, salvo cuando medie autorización. Los Usuarios de Internet no están autorizados para descargar herramientas que comprometan la seguridad con actos como monitoreo de datos, sondeo, copias, prueba de firewalls o hacking entre otros.

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 bloquearan 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 para lo cual asignará un usuario y una contraseña a cada funcionario. Esta mensajería instantánea deberá ser utilizada para fines empresariales y netamente laborales por lo tanto los usuarios de mensajería (spark) 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 demás funcionarios del IBAL y el personal provisto por terceras partes.

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 el Grupo Tecnológico y de Sistemas se recibe la información en medio magnético, se copia la información en el directorio de publicaciones en el computador del analista de sistemas, luego se procede a subir a la página Web mediante la utilización del programa seleccionado para ello y siguiendo los procedimientos establecidos en el instructivo para publicación en la página Web y los lineamientos establecidos en el manual de comunicaciones CR-M-001.

Los usuarios que deben modificar o publicar información en la página web se les asignarán una clave de acceso restringiendo sus posibilidades de actualización de

acuerdo a su perfil o área de trabajo, se asignó clave de acceso a las áreas relacionadas en el instructivo GT-I-001.

La administración de los contenidos de la página institucional está a cargo del área de comunicaciones, quienes serán los encargados de verificar los contenidos que pueden o deben ser publicados. Esto deberá estar acorde al manual de comunicaciones CR-M-001

7.6 CONFIGURACION Y ADMINISTRACION DE LAS REDES

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

Política: Cambios de configuración de red solo lo realizará el Grupo tecnológico y de sistemas, por lo tanto, 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 Ley, se prohíbe la instalación de software no autorizado. Para lo cual el grupo tecnológico y de sistemas, realizará revisión periódica 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 presentar o comprobar que algún funcionario del IBAL está llevando a cabo estos procedimientos sin autorización, dichas situaciones serán notificadas a la oficina de control disciplinario.

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

CONFIGURACION GENERAL REDES WAN Y LAN. Ver Instructivo GT-I-002

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

7.7 ADQUISICION 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, además el centro autorizado para efectos de la garantía debe estar ubicado o tener representación en la Ciudad de Ibagué.

Mantenimiento de Equipos, impresoras y scanner: Actividad Documentada en el Procedimiento Gestión Tecnológica GT-P-001

Para el adecuado funcionamiento de los computadores y periféricos, de forma que su rendimiento sea adecuado y el almacenamiento de la información sea confiable, es necesario brindarles un mantenimiento continuo y adecuado de manera periódica que garantice un óptimo funcionamiento, con el fin de no paralizar las labores diarias de los funcionarios y que permitan un alto grado de confiabilidad y respaldo.

Cuando se presenten fallas en el hardware, el usuario deberá reportarlo al Grupo Tecnológico y de sistemas, allí se diligencia el formato GT-R-001, donde se llevará el registro de los diferentes daños, las soluciones y los tiempos de respuesta. No se autoriza para que ningún usuario final repare, modifique los computadores, impresoras, periféricos o software instalados en ellos

Estos servicios son los que resuelven incidencias concretas a los usuarios y están directamente relacionados con los equipos o cualquier elemento que ellos utilizan.

Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos sin previa autorización de la Oficina de informática.

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

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

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 los cuales se les controlarán los privilegios de acceso, de conformidad con los roles y perfiles establecidos.

Controles:

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, El jefe del área correspondiente realizará la solicitud escrita especificando el perfil requerido para dicho usuario, detallando las diferentes opciones a las que deberá tener acceso. En caso de solicitar acceso a más de un aplicativo se debe especificar por cada uno de ellos los permisos a los que va a tener derecho.

Será responsabilidad del jefe de cada área, reportar al grupo tecnológico y de sistemas el retiro de funcionarios para poder inhabilitarlos en el sistema de información y bloquear sus ingresos. el grupo tecnológico y de sistemas será responsable de recibir los equipos de trabajo fijo y/o portátil para generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les sea formalmente solicitado.

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. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

El Grupo Tecnológico y de Sistemas se encargará de la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información del IBAL, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario. Para lo cual deberá existir solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario, donde se especifique el perfil, los permisos y niveles que deban asignarse.

El Grupo Tecnológico y de Sistemas, como responsable de la administración de los sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

El Grupo Tecnológico y de Sistemas debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

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, posibilitando que otra persona la use o el uso inadecuado del usuario para hacer cambios en el sistema.

En el sistema de información queda almacenado en un registro el nombre del equipo, la IP y usuario del ERP con el que se ingresó al sistema. Cada usuario es consciente de que debe cuidar su usuario y clave porque es único e intransferible.

El Sistema de Información tanto en aplicativos como en el sistema operativo permite el cambio de clave cuando el usuario lo desee, procedimiento que es socializado con los funcionarios del IBAL. Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los Funcionarios serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas

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 FISICO

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 FISICA 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 REGISTRO Y AUDITORIA

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

Los Log 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 la Norma NTC-ISO/IEC 27001, la 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 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.

9. CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCIÓN DEL CAMBIO REALIZADO
2019-07-16	0	N/A