1. **AREA:** GERENCIA GENERAL
2. **FECHA:** Febrero 27 de 2023
3. **ACTO NUMERO:** **004**

4.TEMA
Por el cual se actualizan las reglas y mecanismos de seguridad para los sistemas de información e infraestructura tecnológica al interior del **amb S.A. E.S.P.**

El Gerente General del Acueducto Metropolitano de Bucaramanga S.A. ESP, de conformidad a sus facultades legales y estatutarias, por medio del presente acto establece las reglas y mecanismos de seguridad aplicables a los sistemas de información e infraestructura tecnológica del Acueducto Metropolitano de Bucaramanga S.A. ESP, teniendo en cuenta las siguientes

CONSIDERACIONES:

a. Que según lo dispuesto en el numeral 3 del artículo 47 de los Estatutos Sociales del Acueducto Metropolitano de Bucaramanga S.A. ESP, es función del Gerente General, dirigir, coordinar, vigilar y controlar las relaciones laborales y la ejecución de funciones o programas que al personal le corresponde.

b. Que el Acueducto Metropolitano de Bucaramanga S.A. ESP provee a su personal de medios técnicos e informáticos, como instrumentos de trabajo que permitan rapidez y eficacia en la prestación de sus servicios.

c. Que entre estos medios se incluyen los equipos, programas y sistemas de Información que facilitan el uso de las herramientas informáticas, el acceso a una red interna o intranet y una red externa o internet, así como la utilización de un buzón de correo electrónico o email, impresoras y scanner.

d. Que los sistemas de información deben servir para facilitar y agilizar la realización de los procedimientos administrativos, operativos, comerciales y de proyectos, así como para proporcionar información completa, homogénea, actualizada y fiable de la actividad para el funcionamiento del Acueducto Metropolitano de Bucaramanga S.A. ESP.

e. Que el uso constante, habitual, homogéneo y normalizado de tales medios

técnicos e informáticos debe constituir la regla general de comportamiento de todos los trabajadores y usuarios de éstos al interior del Acueducto Metropolitano de Bucaramanga S.A. ESP, no quedando, en consecuencia, tal uso al libre arbitrio o la discrecionalidad y criterio de sus usuarios.

f. Que, como resultado de la creciente conectividad, los sistemas de información e infraestructura tecnológica son más sensibles ya que están expuestos a un número creciente de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos respecto a su seguridad y por lo tanto requieren de una mayor conciencia y entendimiento de aspectos de seguridad, así como la necesidad de desarrollar una "cultura de seguridad" al interior del Acueducto Metropolitano de Bucaramanga S.A. ESP.

g. Que el Acueducto Metropolitano de Bucaramanga S.A. ESP, como empresa responsable y garante del cumplimiento de la normativa vigente sobre derechos de autor y protección de datos personales, requiere la actualización e implementación de su política de seguridad informática, con el fin de ajustarla a la actualidad legislativa del tema.

h. Que según los artículos 103 - 5,11; 104 - 8; 107 - 1,2,17; el Reglamento Interno de Trabajo del Acueducto Metropolitano de Bucaramanga S.A. ESP, es deber de los trabajadores de la empresa y usuarios de los medios técnicos e informáticos mantener, resguardar, velar y responder por la integridad de los bienes que le fueron dados para su uso, de conformidad con la labor asignada por esta.

DISPONE:

1. **GLOSARIO:**

a. **Autenticidad:** La información es lo que dice ser y ha sido creada, manipulada, accedida o eliminada por quien dice haberlo hecho.

b. **Disponibilidad:** Capacidad de acceder la información o utilizar un servicio con la misma siempre que se necesite.

c. **Confidencialidad:** Mantener el secreto o la privacidad de los datos, es decir, preservar e impedir cualquier revelación no autorizada.

d. **Integridad:** Propiedad de encontrarse, en relación con la información, en el mismo estado en que fue producida, sin haber sufrido modificaciones o supresiones parciales o totales no autorizadas.

e. **SII++:** Sistema de información integrado del Acueducto Metropolitano de Bucaramanga S.A. ESP

f. **Usuario:** Trabajador, contratista, practicante, aprendiz, personal en misión y visitantes a los que el amb S.A. ESP suministre medios técnicos e informáticos como instrumento de trabajo.

2. OBJETIVO GENERAL

Establecer una Política de Seguridad de información para garantizar la protección de los Sistemas de Información e infraestructura tecnológica del Acueducto Metropolitano de Bucaramanga S.A. ESP.

3. OBJETIVOS ESPECIFICOS

a. Establecer reglas y mecanismos para la autenticación de los usuarios de los servicios ofrecidos por El Área de Tecnología de Información.
b. Asegurar la integridad, disponibilidad y confidencialidad de la información.
c. Garantizar la legalidad del software adquirido por el Acueducto Metropolitano de Bucaramanga S.A. ESP y asegurar la propiedad intelectual e Industrial de los desarrollos realizados al interior de la empresa.
d. Proteger los equipos de cómputo y la información corporativa, mediante la ejecución de esta política.

4. NATURALEZA Y FINALIDAD

El presente Acto de Gerencia establece la política de seguridad de los sistemas de información e infraestructura tecnológica del Acueducto Metropolitano de Bucaramanga S.A. ESP y de los activos que la sustentan, también establece medidas para la protección de los datos de los usuarios en el cumplimiento de la Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y así mismo las demás leyes y normas que consagren la reglamentación pertinente a la política de seguridad de los sistemas de información e infraestructura.

5. ALCANCE

Este documento aplica a todos los trabajadores, proveedores y personal que posea algún tipo de vínculo con el Acueducto Metropolitano de Bucaramanga S.A. ESP y que utilicen los sistemas de información e infraestructura tecnológica de la empresa.

Se establecen las normas de seguridad de los Sistemas de Información e infraestructura tecnológica en el Acueducto Metropolitano de Bucaramanga S.A. ESP, teniendo en cuenta que cada usuario es un actor importante para garantizar

la seguridad, por lo que cada uno, de acuerdo a las funciones que desempeña, debe asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información.

6. SANCIONES EN CASO DE VIOLACIÓN O INCUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLOGICA

En el caso de constatarse alguna violación de las normas establecidas en la presente política de seguridad por parte de alguno de los Usuarios de los medios técnicos e informáticos del Acueducto Metropolitano de Bucaramanga S.A. ESP, se aplicarán las medidas disciplinarias contenidas en el Reglamento Interno de Trabajo o las legal o contractualmente establecidas respectivamente así como también en aquellas normas internas de prevención, control y verificación existentes en el Acueducto Metropolitano de Bucaramanga S.A. ESP, por el incumplimiento de las obligaciones como trabajador del amb S.A. ESP o contractuales según condición del usuario de los medios técnicos e informáticos al interior de la empresa.

7. REGLAS Y MECANISMOS

Este documento presenta las Políticas de Seguridad de los sistemas de información e infraestructura tecnológica, cuyo contenido agrupa los siguientes aspectos:

Seguridad Lógica
Seguridad en las comunicaciones
Seguridad de las Aplicaciones
Seguridad Física
Seguridad del Conocimiento

7.1. SEGURIDAD LÓGICA

Cualquier usuario debe identificarse para acceder a los recursos de red o a las aplicaciones.

AUTENTICACIÓN.

El Área de Tecnología de Información ofrece servicios de SII++, directorio activo, correo electrónico corporativo, impresoras, portal Web, intranet, internet que serán revisados de manera periódica.

Todos los trabajadores, contratistas, practicantes, personal en misión y visitantes (usuarios) para acceder a la red del Acueducto Metropolitano de Bucaramanga S.A. ESP, deberán aceptar el servicio y acuerdos de confidencialidad definidos por el Acueducto Metropolitano de Bucaramanga S.A. ESP, los cuales reflejan los compromisos de protección y buen uso de los sistemas de información y la infraestructura.

La autorización para el acceso a los sistemas de información debe ser aprobada por el jefe inmediato, y ejecutada por el Área de Tecnología de la Información, quien determina los controles y privilegios de acceso que se pueden otorgar a los trabajadores y/o usuarios.

El Área de Gestión Humana deberá reportar al área de tecnología de la información los retiros, traslados e inclusión de nuevo personal a la Empresa, puesto que es primordial actualizar usuarios de directorio activo, SII++, cuentas de correo corporativo y el inventario de los equipos de cómputo.

Para el servicio de correo electrónico corporativo el trabajador y/o usuario debe realizar la doble autenticación por multifactor, la cual consiste en la verificación que el usuario que está ingresando a la plataforma de correo electrónico es a quien realmente se le asignó este servicio.

CONTRASEÑAS.

La Gerencia General delega la administración y limita el uso de cuentas de administrador o con privilegios especiales en las redes del amb al Área de Tecnologías de la Información y al Área de Recursos Informáticos.

Se establece una política de contraseñas para reforzar la identificación y autenticación de los usuarios y así evitar problemas de seguridad derivados de un incorrecto manejo de las contraseñas, se seguirán estos lineamientos:

a. La contraseña es personal e intransferible. Todo trabajador y/o usuario debe mantener su contraseña en secreto, asumiendo la responsabilidad de las consecuencias derivadas de su revelación a otra persona. Recomendando no comunicarlas o anotarlas en lugares visibles y fácilmente accesibles.
b. Cualquier situación que comprometa la confidencialidad de las contraseñas debe ser inmediatamente comunicada a El Área de Tecnología de la Información.
c. La oficina de Control de Gestión y El Área de Tecnología de la Información, podrán bloquear el acceso ante la sospecha de un riesgo en la seguridad del sistema de información, o si tiene constancia del

incumplimiento de la política de seguridad.

d. El cambio de contraseña del usuario directorio activo es cada 60 días.

e. Los requisitos mínimos para crear o cambiar las contraseñas son;
   - ✓ Longitud mínima de 14 caracteres
   - ✓ Mayúsculas (de la A a la Z)
   - ✓ Minúsculas (de la a a la z)
   - ✓ Dígitos de base 10 (del 0 al 9)
   - ✓ Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %)

   Las contraseñas deben quedar de mínimo 14 caracteres, debe tener mínimo una letra mayúscula, mínimo un carácter numérico y mínimo un carácter alfanumérico, no debe incluir el nombre ni apellido del usuario en la contraseña.

f. Para el inicio de sesión del servicio de correo electrónico adicional a la contraseña, es requerido incluir un método de comprobación de identidad multifactor el cual podrá ser número de teléfono de celular o número fijo

7.2 SEGURIDAD EN LAS COMUNICACIONES

TOPOLOGÍA DE RED.

El Área de Tecnología de la Información del Acueducto Metropolitano de Bucaramanga S.A. ESP asegura la integridad, disponibilidad y confidencialidad de los datos transmitidos, Así mismo garantiza que los puertos físicos, lógicos y elementos de red estén monitoreados con el fin de prevenir accesos no autorizados.

CONEXIONES EXTERNAS

El Área de Tecnología de la Información controla las actividades de usuarios externos del Acueducto Metropolitano de Bucaramanga S.A. ESP a fin de proteger la infraestructura tecnológica. Esta conexión debe solicitarse mediante la mesa de servicios del Área de Tecnología de la Información, y debe venir acompañada del acuerdo de confidencialidad para acceso remoto, debidamente firmado y autorizado por el jefe inmediato o el interventor del contrato.

El trabajador y/o usuario que haga uso de la conexión VPN debe tener instalado en el equipo donde se realiza la conexión remota, un software antivirus, preferiblemente licenciado, con sistema operativo Windows 10 o última versión del sistema operativo MAC OS o Linux, ancho de banda sugerido de internet de 25 megas. De no cumplir los requisitos no se podrá dar acceso a la conexión remota.

Horario de conexión de la VPN: La conexión VPN estará habilitad de lunes a viernes de 7 am -11:50 am y 1:00 pm – 5:00 pm, salvo excepciones que tendrán un permiso especial otorgado por el líder de infraestructura de la información para laborar en otros horarios que no afecten los proceso de backup.

USO DE INTERNET, INTRANET Y CORREO ELECTRONICO CORPORATIVO.

a. El correo electrónico corporativo y la navegación WEB constituyen parte de los servicios puestos a disposición de los trabajadores y demás del Acueducto Metropolitano de Bucaramanga S.A. ESP y demás usuarios para el desempeño de sus funciones, y/o actividades, por lo que su utilización está exclusivamente encaminada a la ejecución propia de sus funciones o actividades.

b. El proveedor de cuentas de correo no mantiene copias de respaldo de los correos de cada trabajador o usuario, por lo tanto, es responsabilidad de cada uno mantener copias de seguridad y respaldo de sus correos electrónicos.

El descargue de archivos de internet a su equipo a través del correo electrónico corporativo o del navegador es responsabilidad del usuario, por lo tanto, no se deben bajar archivos de dudosa procedencia ni acceder a links que le envíen por correo electrónico sin antes confirmar con el área de Tecnologías de la información.

c. La Intranet es un medio de comunicación interno y un sistema para la gestión de la información, que beneficia el trabajo de las personas por lo que se hace necesario darle un uso adecuado.

d. El acceso a Internet es restringido y será autorizado a través de La Dirección respectiva, siendo responsabilidad del jefe inmediato su autorización, solicitándolo por la mesa de servicios del Área de Tecnología de la Información, para el usuario que requiere este servicio.

e. La cuenta de correo electrónico corporativo, propiedad del Acueducto Metropolitano de Bucaramanga S.A. ESP, asignada al trabajador o usuario para el desempeño de sus funciones o actividades durante el período de vigencia de su contrato laboral, practica universitaria, prestación de servicios, dado el caso no se registre actividad de la misma en 90 días calendario, se procederá con la suspensión de la misma o cuando la relación laboral u otra contractual se termine o se suspenda, se finalizará el servicio.

PROHIBICIONES:

1. Se prohíbe el uso de internet para actividades diferentes a las funciones

específicas del cargo.

2. Se prohíbe el buzón del correo electrónico corporativo para uso personal.
3. Se prohíbe la utilización de redes sociales y otros similares, para fines diferentes a las actividades propias del negocio.
4. Se prohíbe Toda transmisión de contenidos susceptibles de ser considerados delictivos, atentatorios contra la dignidad, el honor, la imagen o la intimidad de las personas, incluidos los de propiedad intelectual e industrial, así como cualesquiera otros inadecuados o no relacionados con el desempeño de las funciones propias del cargo.
5. Se prohíbe la utilización del correo electrónico corporativo para el intercambio no autorizado de información de propiedad de Acueducto Metropolitano de Bucaramanga S.A. ESP, de sus clientes y/o de sus trabajadores, con terceros. En virtud de la Ley 1581 de 2012 Reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y aquellas que lo adicionen o modifiquen.
6. Se prohíbe Toda utilización de contenidos provenientes de Internet que cuyo régimen de explotación y, en su caso, otorgamiento de los oportunos derechos de uso a favor de terceros, no se haya comprobado.
7. Se prohíbe Toda conexión remota desde el exterior del Acueducto Metropolitano de Bucaramanga S.A. ESP que no haya sido autorizada, con la salvedad de los servicios corporativos que sean habilitados para su uso remoto. Esta autorización sólo se concederá cuando la función asignada al cargo lo requiera, y tras tener garantías suficientes de que no se verán afectados los niveles de seguridad de los sistemas de Información del Acueducto Metropolitano de Bucaramanga S.A. ESP.
8. Se prohíbe la navegación por sitios con las siguientes características:

   - ✓ Alto contenido de gráficos, videos y fotografías (congestión en un alto porcentaje a la red), que no tenga relación con las funciones específicas del cargo.
   - ✓ Los sitios de contenido pornográfico, inmoral, ilegal, subversivo, sitios no deseados o de dudosa calidad y contenido.
9. Se prohíbe abrir correos de dudosa procedencia y/o asunto sospechoso; algunos archivos pueden contener virus que afectan los equipos y la red en general.

FIREWALL

El firewall de la empresa presenta una postura de negación preestablecida, configurado de manera que se prohíben todos los protocolos y servicios queponen en riesgo la seguridad de la información, habilitando estrictamente lo necesario.

El Firewall registra la actividad de uso del internet corporativo de los trabajadores y demás usuarios para fines estadísticos y de aplicación de controles de seguridad para garantizar el uso adecuado del servicio.

La gestión de la seguridad perimetral de la red de datos se realiza mediante el firewall con contingencia de redundancia.

Además, el Firewall administra el servicio de red inalámbrica por medio de dispositivos distribuidos en lugares estratégicos de las gerencias para el suministro de Wifi para dar acceso al internet corporativo. Donde se establece 3 tipos de configuración de redes inalámbricas, las cuales son:

- Red inalámbrica corporativa: Esta red inalámbrica tiene como objetivo brindar acceso a internet a los trabajadores y demás usuarios de la empresa de acuerdo a su perfil de internet configurado a su cargo, solo podrá ser usada por los trabajadores o usuarios, previa autorización del jefe inmediato, tiene dos controles de seguridad que son; contraseña única de conexión, que se cambia cada 6 meses y la cuenta del directorio activo del empleado.
- Red inalámbrica sala de juntas: Proporciona internet a los trabajadores o visitantes que estén reunidos en la sala de juntas. Esta red está separada con otro servicio de internet contratado y no presenta restricción de página web. La contraseña de acceso se le otorga a la secretaria de gerencia general y asistente de gerencia general quienes serán las encargadas de brindar la contraseña a las personas que requieran de su uso en la sala de juntas.
- Red inalámbrica invitados: Esta red inalámbrica otorga acceso a internet a través de una contraseña única que es proporciona por correo electrónico a los líderes de área, líderes de proceso y gerentes. Esta contraseña se cambia cada 6 meses,
- Red inalámbrica auditorio: La red inalámbrica del auditorio proporciona internet para los eventos realizados en el auditorio del amb a través de una contraseña única que será entregada al líder de servicios generales. Esta contraseña se cambia cada 6 meses,

Los protocolos de seguridad en las contraseñas de redes inalámbricas del amb son de tipo de encriptación de autenticación WPA2-PSK AES,

7.3 SEGURIDAD DE LAS APLICACIONES

El Acueducto Metropolitano de Bucaramanga S.A. ESP garantiza que los trabajadores y demás usuarios hacen uso el software legal de conformidad con las obligaciones de los tratados y la legislación Colombiana, en cumplimiento de la ley 23 de 1982 sobre derechos de autor, y demás leyes y decretos que la han modificado o modifiquen, así como la Ley 603 de 2000 y el Decreto 1474 de 2002 "Por el cual se promulga el Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor", por tanto la instalación de cualquier tipo de software en el Acueducto Metropolitano de Bucaramanga S.A. ESP es función y responsabilidad exclusiva de El Área de Tecnología de Información; cualquier software instalado sin autorización será responsabilidad del usuario, quien debe asumir los costos de legalización del mismo y las multas a que hubiera lugar entre otras particularidades.

SOFTWARE

a. Todo contratista o tercero que conecte su equipo a la red LAN, debe presentar previamente los soportes de licenciamiento como factura de compra, caja y/o licencia. El Área de Tecnología de la Información conserva copia de estos documentos.
b. Los usuarios de los técnicos e informáticos al interior del amb son responsables por el estado de la etiqueta de licenciamiento, pegada en la carcasa del equipo, ya que cuando se rompe, la empresa pierde el derecho de propiedad sobre el software del equipo, haciéndolo ilegal. En tal caso, el costo de la licencia será asumido por dicho el usuario.

DESARROLLOS Y SOLUCIONES REALIZADAS POR PERSONAL ADSCRITO AL ACUEDUCTO METROPOLITANO DE BUCARAMANGA S.A. ESP Y CONTRATISTAS.

El Acueducto Metropolitano de Bucaramanga S.A. ESP, en cumplimiento de lo dispuesto en la Ley 23 DE 1982 y sus modificaciones y enespecial en lo atinente al tema de propiedad intelectual, Industrial y derechos de autor en el ámbito informático, no solamente en el área de Sistemas sino en la Empresa en general, elabora e implementa una política que define los criterios, deberes y obligaciones de la misma y de todos los trabajadores, contratistas y practicantes, aprendices,

etc., que de una u otra forma producen diferentes clases de insumos y productos, tanto de hardware como de Software, dentro del Acueducto Metropolitano de Bucaramanga S.A. ESP.

Todo esto con fin de promover, motivar, regular y resguardar la propiedad Intelectual e industrial a favor del Acueducto Metropolitano de Bucaramanga S.A. ESP, proveniente de invenciones y creaciones intelectuales, tales como: patentes de invención, modelos de utilidad, diseños y dibujos y planos de obra, marcas comerciales, secretos empresariales, desarrollos de software y/o hardware, esquemas de trazado o topografía, circuitos integrados indicaciones geográficas, desarrollo de prototipos, autómatas y sistemas automatizados, nombres de dominio, información no divulgada, programas de computación y, en general, cualquier otro mecanismo que la ley establezca para la protección de las obras del talento o del ingenio o desarrollos, generados en el Acueducto Metropolitano de Bucaramanga S.A. ESP, por personal de su dependencia, investigadores, contratados a honorarios, y alumnos en práctica, pasantes o como producto de una tesis de grado.

SEGURIDAD DE BASES DE DATOS

Los archivos y registros de todas las Bases de datos de la empresa, los directorios donde se encuentran almacenados y la aplicación que los administra deben tener controles de acceso.

a. El jefe inmediato y/o Interventores de la empresa, deben reportar a El Área de Tecnología de la Información los usuarios del SII++ que no están activos. Además, debe revisar periódicamente los accesos contenidos en las plantillas utilizadas en su área de trabajo.
b. Cuando un usuario de los medios técnicos e informáticos es trasladado de Área funcional, el jefe inmediato debe reportar a El Área de Tecnología de la información los accesos del SII++ que deben ser retirados a ese usuario y su nuevo jefe inmediato debe solicitar los permisos o accesos al SII++ que se requieran para sus nuevas funciones.
c. Cada usuario de los medios técnicos e informáticos, utiliza plantillas con opciones que le permiten leer, escribir, o modificar las Bases de datos del SII++, por tal razón, es directamente responsable por las transacciones que realiza, en ningún caso podrá modificar irresponsablemente la Base de datos para beneficio propio o de terceros.
d. El usuario de los medios técnicos e informáticos al interior de la empresa no podrá entregar información de las Bases de datos a terceros. Excepto quienes por la naturaleza de su cargo y funciones deben suministrarlos, lo anterior de

conformidad con la ley 1581 de 2012 y sus modificatorios.

ANTIVIRUS.

En todos los equipos del Acueducto Metropolitano de Bucaramanga S.A. ESP debe existir un agente antivirus ejecutándose permanentemente y en continua actualización; toda información referente a incidentes de virus se canalizará por El Área de Tecnología de la Información.

Se prohíbe compartir directorios en los equipos de cómputo. De ser necesario compartir información, utilice la unidad K/Públicos, en la cual se puede almacenar la información que es considerada temporal, el contenido de esta carpeta se borra diariamente.

Prohibición: Ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

BACKUP

El Área de Tecnología de la Información realizará copias de seguridad del sistema integrado (SII ++) y demás información corporativa del servidor de archivos. Según el esquema de backup Establecido en el documento: "P SI 007-009 Procedimiento para la realización de Backup"

Además, el usuario dispone de un espacio para almacenamiento de información institucional, en la unidad J: de cada usuario de directorio activo, dicha unidad está incluida en el esquema de backup, aquellos documentos almacenados por fuera de esta unidad no serán objeto de respaldo

7.4 SEGURIDAD FISICA

El área segura del centro de cómputo se protege mediante controles de entrada: Carnets de proximidad y huella digital en dispositivos biométricos lo anterior asegura que solamente se permite el acceso a (3) personas autorizadas: Jefe de área de tecnología de la información, Líder infraestructura del sistema y administrador de la red del amb.

Se restringe la entrada al Área de Tecnología en las instalaciones del amb tanto para empleados como contratistas y visitantes en horas no laborales, en caso de requerirse el ingreso de empleados o contratistas en horario no laboral, debe ser autorizado por medio del formato de ingreso F SAM 702-013 o F SAM 702-003; los

trabajadores deben estar registrados en el Sistema de Accesos, la identificación se realiza con la huella digital en dispositivos biométricos y/o carnets de proximidad a la entrada del edificio donde se encuentran los equipos de cómputo los cuales son asignados a cada empleado.

El ingreso de visitantes se registra en la portería mediante la herramienta SICA (Sistema Control de Acceso), se utiliza una tarjeta de proximidad para la entrada en cada edificio, la tarjeta está configurada para la activación de las puertas, el Servidor de accesos gestiona el control de entrada a las locaciones.

El supervisor interno de la empresa de seguridad verifica el control de acceso físico a las instalaciones del amb mediante un Circuito Cerrado de Cámaras que monitorea todas las áreas de la empresa de manera permanente, de manera que todos los trabajadores, contratistas y visitantes están siendo grabados y monitoreados permanentemente dentro de las instalaciones del amb.

Los trabajadores y terceros incluyendo contratistas y subcontratistas, que tengan acceso a los equipos de la infraestructura tecnológica Acueducto Metropolitano de Bucaramanga S.A. ESP no podrán fumar, beber o consumir ningún tipo de alimentos cerca de los equipos. En caso de daño el empleado debe asumir el costo total o reemplazar el dispositivo con las mismas características.

La limpieza y mantenimiento preventivo de los equipos es responsabilidad de El Área de Tecnología de la Información.

a. Prohibiciones:

- ✓ Se prohíbe el ingreso de equipos de cómputo personales a las instalaciones del Acueducto Metropolitano de Bucaramanga S.A. ESP, excepto para los visitantes autorizados por El Área de Tecnología de la Información, cuyo registro se hará en la portería de la empresa.
- ✓ Se prohíbe la conexión de equipos de cómputo y portátiles personales a la red de datos corporativa. Salvo las autorizaciones por El Área de Tecnología de la Información, para lo cual se debe demostrar la propiedad del software licenciado.
- ✓ Se prohíbe ubicar objetos sobre los equipos de cómputo y/o pegarles adhesivos.
- ✓ Se prohíbe la conexión de celulares y otros aparatos electrónicos en los equipos.
- ✓ Se prohíbe la conexión de impresoras, scanner y demás multifuncionales que no pertenecen al servicio Departamentalizado de impresión.

- ✓ Se prohíbe la conexión de aparatos electrónicos en las tomas de energía reguladas (color naranja).
- ✓ Se prohíbe abrir y manipular los componentes hardware de los equipos, esta actividad solamente puede realizarse por los trabajadores del Área de Tecnología de la información.
- ✓ Se prohíbe el traslado de los computadores de escritorio por parte de los usuarios; esta labor es responsabilidad única del área de tecnología de la información. Cuando un equipo portátil deba ser llevado fuera de la ciudad de Bucaramanga, se recomienda que este hecho sea informado al Área de Almacén y Bienes para el manejo de la póliza del seguro.
- ✓ Se prohíbe hacer transferencia de equipos o periféricos entre los usuarios del amb sin informar al Área de TI y al Almacén General para temas de seguros y control de inventario devolutivo.

PUESTOS DE TRABAJO

En el Acueducto Metropolitano de Bucaramanga S.A. ESP existe una adecuada protección física y mantenimiento permanente de los equipos e instalaciones que conforman los activos Informáticos de la empresa.

a. Cuando se ausenten de su lugar de trabajo habitual, los usuarios de los medios técnicos e informáticos deberán:
   - ✓ Ocultar aquellos documentos o soportes de información susceptibles de ser sustraídos con facilidad, o que contengan información cuya confidencialidad pueda verse comprometida.
   - ✓ Bloquear la pantalla o el acceso a su computador.
   - ✓ Cerrar todas las sesiones y apagar íntegramente el equipo, incluyendo pantalla, al finalizar su jornada laboral.
   - ✓ Guardar las memorias y discos extraíbles, para evitar exponer la información corporativa que pueden contener.
b. El fondo y protector de pantalla deben corresponder al logo-Símbolo de la imagen institucional del Acueducto Metropolitano de Bucaramanga S.A. ESP.
c. Se prohíbe el almacenamiento y reproducción de archivos de música MP3, películas en los equipos de la Empresa. Este comportamiento constituye violación de la normativa sobre derechos de autor.
d. Solo personal autorizado podrá tener acceso al área del Centro de cómputo.
e. Los cuartos donde se ubican los elementos activos de red de cada edificio, deberán permanecer bajo llave, y fuera del alcance del personal no

autorizado.

f. La instalación, traslado y configuración de computadores, elementos de red, servidores, periféricos integrados a la red corporativa del Acueducto Metropolitano de Bucaramanga S.A. ESP será realizada únicamente por personal de El Área de Tecnología de la Información.
g. Se prohíbe retirar cualquier elemento hardware que sea propiedad del Acueducto Metropolitano de Bucaramanga S.A. ESP, excepto los autorizados por El Área de Tecnología de la Información.
h. Los usuarios no podrán modificar las configuraciones de trabajo en los equipos de cómputo.

Los equipos de cómputo que se prestan a los practicantes serán siempre rotados al interior de la empresa. Estos equipos no quedarán fijos en ninguna oficina y el área de tecnologías de la información dispondrá de ellos

GESTIÓN DE MEDIOS REMOVIBLES.

Discos duros externos, USB y unidades lectoras de CD/DVD estarán habilitados en aquellas máquinas donde se requieran, con previa autorización del jefe Inmediato, este control previene la entrada de virus por estos medios y la extracción de información no autorizada

El Área de Tecnología de la Información ha implementado controles para asegurar que sólo los usuarios autorizados pueden utilizar los medios de almacenamiento removibles. Mediante el acuerdo de confidencialidad. Cuando un usuario es trasladado de Área funcional, los permisos son retirados automáticamente y deben ser solicitados, si los requiere, por parte de su nuevo jefe inmediato.

8. SEGUIMIENTO

El área de tecnologías de la información del Acueducto Metropolitano de Bucaramanga S.A. ESP velará por la correcta aplicación y efectivo cumplimiento de esta Política de Seguridad de la Información.

La Gerencia General y la Gerencia Financiera y de Recursos, podrán disponer de medidas preventivas y de controles tendientes a la identificación de los responsables de la vulneración de las normas contenidas en esta Política.

Cada Gerente de área, Líder de área, líderes de procesos 2 y 3, deberá informar sobre los cambios en los accesos del Sistema de Información Integral, autorizar

los recursos informáticos e informar al Área de tecnología de la información cuando se requieran suspender o restringir los accesos a dichos recursos.

El SII++ ofrece una herramienta para consulta de los accesos que tienen asignados por usuario para el control de los jefes inmediatos.

9. **PUBLICACION**

El presente Acto de Gerencia se publicará en la Intranet Acueducto Metropolitano de Bucaramanga S.A. ESP y se trasladará a los Gerentes de Área, Lideres de Área, Lideres de procesos 2 y 3, para su general divulgación y aplicación, así como a las Áreas de Gestión Humana y Control de Gestión para la aplicación de las disposiciones que son de su competencia.

El presente Acto de Gerencia rige a partir de la fecha de su expedición y deroga todas las disposiciones anteriores que han sido objeto de modificación, así como aquellas que el sean contrarias.

Para constancia firma,

ALEJANDRO ESTRADA CARMONA

Gerente General amb. S.A E.S. P

Elaboró y proyectó: JEGarcia, Líder de área Tecnologías de la Información

Revisó: MLArias, Líder Gestión Jurídica y Representación Judicial