EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTÁ EAAB – E.S.P.

Resolución Número 0740
(Agosto 21 de 2018)

POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTÁ, EAAB- ESP

El Gerente de Tecnología de la Empresa de Acueducto y Alcantarillado de Bogotá - E.S.P, en ejercicio de las facultades delegadas por el Gerente General, a través del artículo 1º de la Resolución 0196 de 2017, y

CONSIDERANDO:

Que el artículo 15 de la Constitución Política establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. También tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Igualmente, respecto de la recolección, tratamiento y circulación de datos se respeta la libertad y demás garantías consagradas en la Constitución.

Que la Ley 1581 de 2012, desarrolló el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información personal que se haya recogido sobre ellas en bases de datos o archivos de entidades públicas o privadas.

Que el Decreto 652 de 2011 establece que "Las entidades y organismos distritales usarán la NORMA TÉCNICA DISTRITAL DEL SISTEMA INTEGRADO DE GESTIÓN PARA LAS ENTIDADES Y ORGANISMOS DISTRITALES NTD-SIG 001:2011 en conjunto con los requerimientos específicos de estándares o especificaciones de cada uno de los subsistemas de gestión aplicables según la naturaleza de la entidad y organismo".

Que el Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017, consolida los elementos requeridos para que una organización pública funcione de manera eficiente y transparente, atendiendo 16 Políticas de Gestión y Desempeño dentro las que se encuentran la "Seguridad digital y Gobierno Digital", integrada con el subsistema de seguridad de la información y con el Modelo Integrado de Gestión y Planeación MIPG con sus 4 líneas de defensa responsables por la gestión de riesgos y actividades de control.

Que mediante la Resolución 305 del 2008, modificada por la Resolución 004 de 2017, la Comisión Distrital de Sistemas -CDS se estableció la Política básica de Seguridad de la Información en el Distrito Capital en la que se refiere a la adopción de las políticas de seguridad y custodia de los datos e información, y al establecimiento de los procedimientos para el adecuado uso y administración de los recursos informáticos de los cuales se valgan para cumplir con sus funciones administrativas, operativas y misionales. Las entidades, organismos y órganos de control del Distrito Capital deberán atender la normatividad y lineamientos que formulen las entidades nacionales sobre el particular, incluyendo los que han sido formulados y los que llegue a formular el MINTIC, así como los que emitan otras autoridades competentes del orden nacional (por ejemplo, el Ministerio de Defensa, la Dirección Nacional de Inteligencia y el DNP, que son citados por el CONPES 3854 de Seguridad Digital como autoridades en la materia) y que sean aplicables a la respectiva entidad.

Que, de acuerdo con las normas citadas, corresponde a la EAAB-ESP adoptar la Política General de Seguridad y Privacidad de la Información con el objetivo de proveer un ambiente seguro en el tratamiento de la información, preservando sus características esenciales de Confidencialidad, Integridad, Disponibilidad y Privacidad.

Que, en el artículo 1º de la Resolución 0196 de 2017, se delegó en los Gerentes la representación legal en todos los asuntos relacionados con las actividades propias de la respectiva área, de conformidad con las responsabilidades establecidas en el Acuerdo No.11 de 2013.

RESUELVE:

ARTÍCULO PRIMERO. - Adoptar la Política de Seguridad y Privacidad de la Información en la EAAB-ESP, mediante la cual se compromete con la protección de la información de la organización, de sus colaboradores y de sus usuarios, la cual es vital para la sostenibilidad de la EAAB-ESP y para la prestación de los servicios misionales.

ARTÍCULO SEGUNDO. – Definiciones. Para los efectos de la presente resolución se adoptan las siguientes definiciones:

a) **Acuerdo de Uso de la Información y de los Servicios Informáticos:** Es el acuerdo aceptado por los usuarios de los servicios informáticos en el cual se establecen sus derechos y deberes.

b) **Aplicaciones Informáticas:** Conjunto de programas de computador (software) que apoya las actividades de gestión de información de los servicios en los procesos de negocio de la Empresa y que hacen parte de los servicios informáticos.

c) **Colaborador:** Persona natural o jurídica que ejecuta una función de trabajo autorizada y amparada por un vínculo formal con la EAAB-ESP.

d) **Contexto autorizado de operación:** Ambiente donde se establece cómo y dónde deben ser utilizadas las aplicaciones móviles para garantizar la postura de seguridad de la Empresa.

e) **Componentes del modelo de seguridad de la información:** Grupo de elementos de Gobierno, Riesgo y Cumplimiento que operacionalizan la Política de Seguridad y Privacidad de la Información, tales como Activos de información, Procesos, Procedimientos, Manuales, Instructivos, Arquitectura, Programa de sensibilización, y Plan Estratégico de seguridad de la información y de tecnología.

f) **Cuenta de Acceso:** Identificación y contraseña a través de la cual un Usuario de la Información accede a un servicio, aplicación o recurso informático.

g) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, que haya sido entregado a la EAAB-ESP con un fin específico.

h) **Dispositivo móvil:** Equipo portátil con capacidad de almacenar, procesar o transmitir datos, incluyendo, pero no limitado a computadores portátiles, discos duros portables, unidades flash USB, teléfonos inteligentes y tabletas.

i) **Incidente de Seguridad de la Información:** Son todos los hechos o actos de desviación a esta política que afecten la información de la empresa.

j) **Información:** Datos que se representan almacenados en forma electrónica, magnética, en papel, u otros medios impresos o visuales. Constituyen formas conocidas de representación de datos: las imágenes, la voz, el video, los programas de computador, los mensajes de correo, el texto y las conversaciones asociadas al chat y otras formas que aparezcan con desarrollos tecnológicos informáticos.

k) **Plataforma Informática/Tecnológica:** Infraestructura de software, hardware, comunicaciones y seguridad que soportan los diferentes sistemas o aplicativos o aplicaciones de información.

l) **Recurso informático:** Cualquier componente físico (hardware) o lógico (software) empleado para almacenar, manipular, procesar o transmitir alguna forma de datos. Las cuentas de acceso son recursos informáticos.

m) **Servicios Informáticos:** Servicios de sistemas/aplicativos/aplicaciones de información, aprovisionamiento y/o suministro de recursos informáticos, actividades de soporte técnico humano para el apoyo de la gestión de alguna forma de datos a los procesos de EAAB-ESP. Los servicios de la EAAB-ESP están destinados principalmente a apoyar los procesos de negocio de la Empresa. Por ejemplo: el correo electrónico, Internet, Citrix, SAP.

n) **Sistema/aplicativo/aplicación de Información:** Cobija todo sistema utilizado para generar, enviar, recibir, archivar o procesar alguna forma de datos.

o) **Sistema Integrado de Gestión SIG:** Mecanismo de gestión que permite dirigir y evaluar el desempeño institucional en términos de los Sistemas de Gestión de la Calidad (SGC), Control Interno (SCI), Gestión Documental y Archivo (SIGA), Gestión de Seguridad de la Información (SGSI), de Seguridad y Salud Ocupacional (S&SO), Responsabilidad Social (SRS) y la Gestión Ambiental (SGA).

p) **Plan de continuidad de negocio:** Plan logístico que incluye actividades, personas, recursos, instalaciones y herramientas tecnológicas frente a cada proceso de negocio para la práctica de cómo la Empresa debe recuperar sus funciones críticas parcial o totalmente interrumpidas por un evento no deseado o desastre mayor.

q) **Responsable o Determinador:** Es el funcionario de nivel directivo de la EAAB-ESP que debido a su cargo o función es responsable del proceso que origina la información.

r) **Teletrabajo**: Forma de organizar y / o realizar el trabajo y / o comunicarse entre trabajadores y la Empresa, utilizando tecnología de la información, sin requerirse la presencia física del trabajador en un sitio habitual, de conformidad con la reglamentación interna de la EAAB-ESP.

s) **Usuario**[1]: Persona natural o jurídica que se beneficia con servicios provistos por la EAAB-ESP, bien como propietario del inmueble en donde se presta o como receptor directo de servicio, en cuyo caso se denomina también consumidor o cliente.

t) **Usuario de la Información:** Empleados, Contratistas, Subcontratistas, Colaboradores y en general toda persona natural o jurídica que hace uso de la información o es custodio de esta y a la que se le haya asignado un recurso informático (digital o físico) y/o cuenta de acceso para la utilización y/o administración de un sistema de información.

ARTÍCULO TERCERO. - Protección de la Información. Independientemente del medio en que se encuentre la información al interior de la Empresa, por ser vital para su funcionamiento y constituir un activo con valor[2] estratégico, requiere las garantías administrativas y jurídicas para su conservación y uso, por lo que deberá ser administrada adecuadamente para asegurar su integridad, confidencialidad, disponibilidad y privacidad.

Los activos de información de propiedad de la EAAB-ESP o los que esta custodie están a disposición de los Usuarios de la Información, para su uso en una función específica o necesidad de trabajo, sin que esto altere en ningún momento: 1) La propiedad de la EAAB-ESP sobre dichos activos; 2) La responsabilidad que tiene de custodiar información.

Todos los Usuarios de la Información deberán depositar la información de la EAAB-ESP en los repositorios oficiales y centrales de la Empresa.

Cada uno de los activos de información tendrá un Responsable o Determinador, quien: 1) Identificará y clasificará plenamente la información que produce o custodia, 2) Definirá y mantendrá el nivel de protección, 3) Autorizará y vigilará su buen uso y 4) Reportará cualquier hecho o acto que afecte el nivel de protección.

ARTÍCULO CUARTO. – Ciclo de vida de la información. Comprende la generación, creación o recolección, certificación, almacenamiento, procesamiento, presentación, utilización, transmisión, transporte, comunicación, retención y destrucción de la información, en donde se vigilará su adecuada protección acorde con su sensibilidad e importancia, y se tomarán las acciones correctivas requeridas.

[1]De acuerdo con lo establecido por la Cláusula Primera del CONTRATO DE CONDICIONES UNIFORMES PARA LA PRESTACIÓN DE LOS SERVICIOS PÚBLICOS DOMICILIARIOS DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTA ESP.

[2]Costo de su obtención o reconstrucción.

Cada Usuario de la Información es responsable por la protección, adecuado uso, gestión y devolución de la información que se le entregue o tome para realizar su función de trabajo dentro del ciclo de vida de la información.

Los Responsables o Determinadores de la información, deberán divulgar su sensibilidad y criticidad a cada uno de los Usuarios de su Información y detallarán como mínimo:

- Condiciones de confidencialidad y privacidad.
- Custodios de la información.
- Auditores del uso de la información.
- Entrega y recepción información.
- Control de documentos y registros.
- Si contiene Datos personales y/o sensibles.
- Devolución de la información.
- Disposición y/o Destrucción de la información, de conformidad con la ley.

Para la devolución de la custodia de la información y recursos informáticos a cargo de un Usuario de la Información, se suscribirá un Acta de Paz y Salvo de Datos y de Recursos Informáticos, entre el Custodio de la información y el Ordenador del Gasto o Superior Jerárquico.

ARTÍCULO QUINTO. – Tratamiento de Información personal. La información personal que recolecte la Empresa en el ejercicio de su función deberá ser utilizada para los propósitos expresos para los cuales fue solicitada, tomando las medidas para preservar su vigencia, exactitud, integridad, confidencialidad y finalidad.

Cada vez que una persona suministre información personal a la EAAB-ESP, deberá ser informado expresamente de la Política de Tratamiento de Datos Personales, que adopte la EAAB- ESP.

ARTÍCULO SEXTO. – Responsabilidad frente a la protección de la Información. La protección y uso apropiado de la información, independientemente del medio en que ésta se encuentre, es una obligación y responsabilidad de todos y cada uno de los Usuarios de la Información de la EAAB-ESP.

Para la dirección y coordinación de actividades relacionadas con la seguridad de la información de la EAAB-ESP, se definen tres líneas de defensa o niveles de protección: 1) El Responsable o Determinador de la protección y uso de la Información “Primera Línea”,

2) El Oficial de Seguridad de la Información a cargo de la Coordinación del SGSI, quién define y desarrolla el modelo de protección de la información del Subsistema; El Comité de Seguridad de la Información que tendrá dentro de sus principales funciones la de ser el determinador de los temas de seguridad y privacidad de la información a nivel empresarial y quién podrá definir roles adicionales que se consideren necesarios para el desarrollo y operación del modelo de seguridad y privacidad de la Información, como línea estratégica de sostenibilidad del proyecto "Segunda Línea", y 3) La Auditoría que verifica el cumplimiento de las responsabilidades frente al SGSI y la Política de Seguridad y Privacidad de la Información "Tercera Línea"

ARTÍCULO SÉPTIMO. – Gestión de riesgo de la información. La EAAB-ESP dispondrá de un proceso continuo de gestión de los riesgos de seguridad de la información, alineado con el Sistema Integrado de Gestión SIG, con el fin de identificar, evaluar, tratar, monitorear y reportar los riesgos asociados con los procesos, personas, sistemas de información, datos e infraestructura física que se relacionen con la disponibilidad, integridad, confidencialidad y privacidad de la información.

El Subsistema de Seguridad de la Información SGSI, en coordinación con cada área de la organización, establecerá, formalizará, entrenará y comunicará todos los procedimientos y controles que permitan coordinar, dirigir y orientar las actividades tendientes a minimizar los riesgos en el tratamiento de la información, los cuales serán de obligatorio cumplimiento por todos los Usuarios de la Información.

ARTÍCULO OCTAVO. - Gestión tecnológica. Para reducir los riesgos que se identifiquen en la plataforma tecnológica, se deberá realizar la planeación, implantación, mantenimiento y monitoreo de cada uno de sus componentes, incluyendo, pero no limitándose a: 1) Cumplimiento de la Arquitectura de Seguridad de la Información, 2) La definición de roles y perfiles segregados según el procedimiento establecido, 3) La asignación y establecimiento de controles de acceso y la asignación de privilegios con base en una necesidad de negocio, 4) La implantación de software de protección contra código malicioso, 5) La habilitación de filtros de acceso y contenido en Internet, 6) La segmentación de las redes de datos acorde con el nivel riesgo y, 7) La realización de pruebas de vulnerabilidades técnicas a la plataforma tecnológica, entre otros.

Todos los procesos y proyectos que se desarrollen en la EAAB-ESP que involucren el manejo de información, deberán incluir la revisión expresa y el cumplimiento de requisitos de seguridad de la información con el fin que se incorporen los controles necesarios que traten los riesgos a niveles aceptables asociados al ciclo de vida de las soluciones resultantes de los nuevos proyectos.

Cada Usuario de La Información que vaya a acceder a los servicios tecnológicos de la Empresa, deberá suscribir el Acuerdo de Uso de la Información y Servicios Informáticos.

Cada proceso de administración de sistemas y de tecnología de la información debe identificar y tratar a niveles aceptables sus riesgos conforme lo establece la presente Política de Seguridad y Privacidad de la Información.

ARTÍCULO NOVENO. – Plan de Continuidad-. La EAAB-ESP adoptará y aprobará mediante acto administrativo planes de continuidad de negocio con el fin de garantizar la contingencia, recuperación y respaldo de la información como parte integral de cada proceso de la Empresa, con el objeto de disminuir los riesgos de interrupción y/o pérdida de la información y/o disminución del desempeño de los servicios de información que soportan el negocio y la operación.

ARTÍCULO DÉCIMO. - Confidencialidad y privacidad. Cada área será responsable por vigilar que se establezca con cada uno de los Usuarios de la Información las condiciones de confidencialidad y uso en caso de que la información que se va a acceder, registrar o actualizar sea clasificada, reservada, sensible o sea personal.

Lo anterior con el propósito que quede establecido el compromiso del Usuario de la Información ante la Empresa de proteger la información que le ha sido entregada para realizar una actividad o función, orientando a la debida diligencia y debido cuidado acorde con los niveles de clasificación de la información establecidos por la EAAB-ESP y la legislación aplicable.

Compromiso que deberá ser reconocido y firmado expresamente desde el establecimiento de una relación laboral, de servicio, comercial o de cooperación entre la EAAB-ESP y un Usuario de la Información.

ARTÍCULO DÉCIMO PRIMERO. - **Acuerdo de uso de la información y de servicios informáticos.** La EAAB-ESP establecerá con cada uno de los Usuarios de la Información un acuerdo de uso de los recursos y servicios informáticos, en donde se definirá claramente lo que puede o no hacer un Usuario de la Información con las herramientas, recursos y servicios informáticos provistos por la EAAB-ESP para el desarrollo de las actividades para las cuales fue contratado y una cláusula de confidencialidad de la información que vaya a acceder, registrar o actualizar.

El Acuerdo de uso deberá ser firmado expresamente en aceptación por el Usuario de la Información, como requisito para la asignación de cualquier recurso o servicio informático.

ARTÍCULO DÉCIMO SEGUNDO. - Mejoramiento permanente. La EAAB-ESP impulsará el mejoramiento permanente del Subsistema de Gestión de Seguridad de la Información con sus componentes y los recursos y servicios informáticos, en procura de proteger la información, asegurar la continuidad de las operaciones informáticas que soportan el negocio, y la disminución de los riesgos asociados al indebido manejo de la información y de la infraestructura informática.

ARTÍCULO DÉCIMO TERCERO. - Debido registro. La EAAB-ESP en su labor de vigilancia del buen uso de su información garantizará el registro de la actividad que se genere a partir del tratamiento de la información mediante los recursos, servicios y aplicativos informáticos, con el fin de detectar y solucionar anomalías, y detectar el uso indebido de la información.

ARTÍCULO DÉCIMO CUARTO. - Seguridad física y del entorno. Los Directivos de cada área de la EAAB-ESP deberán procurar un nivel de protección proporcional a la clasificación de privacidad y criticidad de la información que se procese y administra en su área.

ARTÍCULO DÉCIMO QUINTO. - Control de Acceso a la Información. Cada Usuario de la Información de la EAAB-ESP debe disponer de un medio de identificación y su acceso se otorgará a través de autenticación individual. El tratamiento de la información de la Empresa se otorgará y mantendrá con base en una necesidad de negocio demostrada, preservando siempre el menor privilegio.

ARTÍCULO DÉCIMO SEXTO. - Terceros que accedan a información de la EAAB-ESP. Los Terceros que por razones de negocio estén autorizados a acceder o a efectuar tratamiento de información propia de la EAAB-ESP deben cumplir con la presente Política de Seguridad y Privacidad de la Información.

ARTÍCULO DÉCIMO SÉPTIMO. - Información de la Empresa en redes externas. La información de la Empresa debe preservar su mismo nivel de protección cuando pasa a través de redes diferentes a la red de datos privada de la EAAB-ESP.

ARTÍCULO DÉCIMO OCTAVO. - Auditoría y seguimiento. La EAAB-ESP vigilará el cumplimiento de la presente política mediante la inspección del registro de la manipulación de la información por parte de los Usuarios de la Información con el fin de detectar el uso indebido, reportando desviaciones a los Directivos.

ARTÍCULO DÉCIMO NOVENO. - Incidentes en seguridad de la información. Todas las áreas de la EAAB-ESP están obligados a reportar los incidentes al SGSI, y gestionarlos hasta su cierre

ARTÍCULO VIGÉSIMO. - Programa de creación de cultura en el uso de la información. La EAAB-ESP contará con un programa de cultura de uso de la información a cargo de las áreas de Comunicaciones y de Gestión Humana, que refleje la Política de Seguridad y Privacidad de la Información con sus componentes, los riesgos que esté enfrentado la organización, los progresos, las medidas tomadas, los resultados y lo que espera de cada persona.

ARTÍCULO VIGÉSIMO PRIMERO. – Uso de dispositivos móviles y teletrabajo. Teniendo en cuenta que el uso de dispositivos móviles expone la información a nuevos riesgos que comprometen su nivel de seguridad, estos deben ser identificados, evaluados, tratados, monitoreados e informados a sus responsables.

Cada aplicación y/o dispositivo móvil, previa puesta en operación, debe ser objeto de evaluación que verifique el cumplimiento de la presente Política y el contexto de uso. El Responsable o Determinador de la información debe aprobar expresamente su uso y el contexto de operación, para efectos de que no se comprometa la seguridad de la Empresa. El uso de estos medios será controlado y se otorgará con base en una necesidad demostrada de negocio, el que será verificado y mantenido regularmente por las áreas de negocio dueñas de los servicios.

Los usuarios autorizados para el uso de estos medios deben: 1) Ser entrenados en el servicio y los peligros a que se expone la información de la Empresa y el papel que juegan como primera barrera de contención ante dichos riesgos, y 2) firmar el Acuerdo de uso de la información y servicios informáticos.

ARTÍCULO VIGÉSIMO SEGUNDO. – Autorregulación. Todas las áreas de la EAAB-ESP están en la obligación de identificar, aplicar y hacer cumplir la presente normatividad.

En el análisis de aspectos de cumplimiento se incluirán entre otros: los derechos de propiedad intelectual, los tiempos de retención/conservación de registros, la intimidad, habeas data y la protección de datos personales, así como el uso adecuado de recursos de procesamiento, el uso de criptografía, la recolección de evidencia y respuesta a incidentes de seguridad y los demás requisitos jurídicos y técnicos aplicables a los activos de información.

ARTÍCULO VIGÉSIMO TERCERO. - **Medidas disciplinarias.** Cualquier infracción a la presente política que ponga en riesgo la información objeto de protección, deberá ser puesta en conocimiento de las autoridades disciplinarias y/o judiciales a las que haya lugar. Los Contratistas tendrán responsabilidades contractuales derivadas los acuerdos de confidencialidad, de uso de la información y de los recursos informáticos, así como las demás consecuencias que dicho incumplimiento genere.

ARTÍCULO VIGÉSIMO CUARTO. - Vigencia. La presente resolución rige a partir de la fecha de su publicación y deroga las demás que le sean contrarias, en especial la Resolución 1127 del 23 de diciembre de 2009.

Dada en Bogotá, D.C. a los veintiún (21) días del mes de agosto de dos mil dieciocho (2018).

PUBLÍQUESE Y CÚMPLASE

LUIS HUMBERTO JIMÉNEZ MORERA
Gerente de Tecnología