POLÍTICA	
Tipología: Política de gestión	**Página: 1 de** 6
Nombre: Política de seguridad y privacidad de la información	**Versión: 03**

Control de cambios **(se lleva el control de las versiones y la justificación de las mismas)**

VERSIÓN	FECHA DE APROBACIÓN	RESPONSABLE DEL CAMBIO	CONTROL DE CAMBIOS	FIRMA
01	23-12-2009	Jorge Enrique Pizano Callejas Gerente General	Versión inicial según resolución 1127 de 2009	
02	22-06-2017	Pedro Buitrago Aguilar Gerente de Tecnología	Adición tratamiento de datos personales	
03	20-12-2018	Lady Johanna Ospina Corso Gerente General	Modificaciones: Descripción, objetivos, líneas de defensa e indicadores	

Descripción

La EAAB-ESP está comprometida a proveer un ambiente seguro en el tratamiento de la información, preservando sus características esenciales de confidencialidad, integridad, disponibilidad y privacidad de activos de información y de la información vital de la organización para la sostenibilidad de la Empresa, aplicando las mejores prácticas de seguridad y privacidad de información.

Justificación

La EAAB-ESP define y establece la política de seguridad y privacidad de la información con el fin de declarar las responsabilidades y conductas que debe ser observada por cada una de las áreas responsables de la protección y uso de la información, sus funcionarios, colaboradores, usuarios de información, de recursos y servicios informáticos; proteger la información de los procesos organizacionales para la prestación de sus servicios; adoptar y desarrollar el Subsistema de Gestión de Seguridad de la Información (SGSI); precisar las medidas y controles que debe observar la

Elaboró: Álvaro Pinzón Morales	**Revisó:** Luis Humberto Jiménez Morera–Gerente de Tecnología	**Fecha Revisión:** 18 de diciembre de 2018
Responsable: Ricardo Abad Chacón – Director de Servicios de Informática	**Aprobó**: Lady Johanna Ospina Corso -Gerente General (e)	**Fecha Aprobación:** 20 de diciembre de 2018

organización en búsqueda del buen uso de la información y la disminución en los niveles de exposición al riesgo para el cumplimiento legal y regulatorio nacional y distrital.

Alcance

Aplica para todos los procesos de la EAAB-ESP y toda información como documentos físicos y electrónicos, los datos en los sistemas de información y los datos personales, que la Empresa reconoce como activos de información teniendo en cuenta su clasificación según la normatividad vigente, vital para el funcionamiento de la Empresa y para la prestación de servicios públicos domiciliarios.

Directrices

La construcción de la política se basó en:

1. Que es una declaración de alto nivel de la posición de la entidad referente a la protección de seguridad y privacidad de la información.
2. Que tiene en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales.
3. Que está alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI.
4. Que tiene coherencia entre los principios de seguridad de la información y la gestión documental.

Normatividad

1. Ley 1341 de 2009. “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”. Congreso de Colombia.
2. Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”. Congreso de Colombia.
3. Ley 1712 de 2014. “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”. Congreso de Colombia.
4. Decreto 1377 de 2017. “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”. Presidencia de la República.

5. Decreto 886 de 2017. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos". Presidencia de la República.
6. Decreto 1499 de 2017. "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015". Presidencia de la República.
7. Decreto 1008 de 2018. "Por el cual se establecen los lineamientos generales 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, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". Ministerio de Tecnologías de la Información y las Comunicaciones.
8. Decreto 591 de 2018. ""Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones". Alcaldía Mayor de Bogotá.
9. Resolución 305 de 2008. "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalidad del gasto, conectividad, infraestructura de datos espaciales y software libre". Comisión Distrital de Sistemas.
10. Circular externa No. 02 de 2015. "La cual define las características en las cuales las organizaciones privadas y públicas deberán reportar y registrar el tratamiento y controles internos sobre sus bases de datos con información personal". Superintendencia de Industria y Comercio –SIC.
11. Circular 007 de 2015. "La cual define lineamientos generales para establecer, implementar, mantener y mejorar continuamente el sistemas de gestión de seguridad de la información en entidades distritales". Alta Consejería Distrital de Tecnologías de Información y las Comunicaciones – ADTIC.
12. Resolución 740 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"

Roles y responsabilidades

ROLES	RESPONSABILIDADES
Directivos – Responsables o determinadores de los activos de información	**Primera línea de defensa** Definir los criterios de protección y buen uso de los activos de información, para lo cual deberá: 1. Identificar y clasificar los activos de información que se originan en sus procesos en las herramienta de gestión de riesgos – GRC de la Empresa. 2. Definir, aprobar y divulgar las pautas de protección y uso determinadas de acuerdo a los riesgos asociados para sus activos de información. 3. Autorizar expresamente el acceso a la información, ya sea mediante formulario SIMI o el registro definido para la información física.

	4. Elaborar planes de continuidad a los procesos críticos del área. 5. Vigilar y reportar desviaciones e incidentes de seguridad y tomar acciones y controles establecidos para sus activos de información. 6. Autogestionar la seguridad, protección y gestión de riesgos de la información. 7. Realizar el autocontrol y reportar el estado de los indicadores de la gestión de seguridad y privacidad de la información.
Funcionarios, terceros o colaboradores de EAAB-ESP	**Primera línea de defensa** 1. Acatar la política de seguridad y privacidad de la información y procedimientos corporativos que de ella se deriven o de los acuerdos de uso y/o confidencialidad a los que esté comprometido. 2. Proteger y dar buen uso de los activos de información de acuerdo a la clasificación aprobada por el área dueña del mismo. 3. Informar a la instancia encargada los eventos de incumplimiento de la política de seguridad y privacidad de la información o de los procedimientos corporativos que de ella se deriven y ésta al Comité de Gestión y Desempeño Institucional.
Comité de Gestión y Desempeño Institucional	**Segunda línea de defensa** 1. Formalizar, divulgar, analizar y hacer cumplir el gobierno del Subsistema de Gestión de Seguridad de la Información, junto con cada uno de sus componentes. 2. Asegurar, aprobar y verificar la implementación de las directrices en materia de seguridad digital y de la información junto con cada uno de sus componentes para el uso y protección adecuada de la información.
Líder Subsistema de Seguridad de la Información (SGSI) – Gerente de Tecnología	**Segunda línea de defensa** 1. Diseñar, desarrollar, implementar, monitorear, mejorar, evaluar, reportar a la organización y verificar el buen funcionamiento del Subsistema de Seguridad y Privacidad de la Información. 2. Las demás que establezca la normatividad vigente.
Equipo de trabajo del Subsistema de Seguridad de la Información (SGSI)	**Segunda línea de defensa** 1. Acompañar y asesorar a las áreas para que los responsables de la protección y uso de la información puedan cumplir con las actividades del Subsistema de Gestión de Seguridad de la Información. 2. Apoyar al líder del Subsistema de Gestión de Seguridad de la Información con los planes, actividades y/o seguimientos a los mismos.
Oficina de Control Interno y Gestión	**Tercera línea de defensa**

	1. Verificar el cumplimiento de las responsabilidades frente al SGSI y frente a la política de seguridad y privacidad de la información.

Objetivos e indicadores

Objetivo 1:

1. Promover y aplicar la seguridad, privacidad y gestión de riesgos para la protección de información de los procesos de la entidad.

Indicadores

No.	Nombre del indicador	Fórmula de cálculo	Descripción
1	Autoevaluación de cada área del porcentaje de socialización de controles de protección de información	No. de áreas con controles de protección de la información socializados / No. total de áreas *100	Porcentaje de áreas que han identificado, clasificado y divulgado expresamente los controles que protegen su información. Los controles hacen referencia a las medidas de protección y uso de los activos de información.
2	Autoevaluación de cada área del porcentaje de actualización y depuración de cuentas y permisos a sistemas de información mediante formulario SIMI	No. de áreas con actualización y depuración de cuentas y permisos / No. total de áreas *100	Porcentaje de actualización de cuentas por área que han revisado y actualizado las cuentas y permisos de funcionarios a sistemas de información mediante formulario SIMI.

Objetivo 2:

2. Desarrollar planes de continuidad de la operación ante eventos de interrupción que surjan.

Indicadores

No.	Nombre del indicador	Fórmula de cálculo	Descripción
1	Porcentaje de áreas con avances en el desarrollo de planes de continuidad de proceso	No. de áreas que han elaborado y actualizado el documento “Plan de continuidad” y que han recibido aprobación del SGSI / No. total de áreas *100	Porcentaje de áreas que han desarrollado planes de continuidad. Los planes de continuidad son los documentos que determinan cómo actuar (actividades, personas, recursos, instalaciones y herramientas tecnológicas) frente a cada proceso de negocio en caso de eventos que

			interrumpan la operación normal. Indican cuáles son las actividades que son indispensables para mantener la operación en un período de tiempo mientas se reestablecen las condiciones normales de operación.

Objetivo 3:

3. Gestionar la protección y tratamiento de los datos personales.

Indicadores

No.	Nombre del indicador	Fórmula de cálculo	Descripción
1	Porcentaje de cumplimiento de las áreas responsables de ejecución de cuatro actividades comprometidas en la protección de datos personales ante la SIC	No. de áreas que cumplen con cada pauta con respecto a cada base de datos / No. total de áreas *100	Cumplimiento de aplicación de las pautas de la Ley 1581 de 2012 y Decreto 1266 de 2013 de protección de datos personales para las bases de datos registradas para vigilancia ante la SIC: 1. Adecuación de procedimientos y canales reglamentarios del tratamiento de datos personales para recolección, acceso, conservación, uso y actualización. 2. Gestión de las peticiones en el tratamiento de datos personales. 3. Gestión de incidentes de datos personales. 4. Presentación semestral de informe de peticiones de tratamiento e incidentes de seguridad.