Que una vez hecho esto y previo a la verificación de (i) no estar dentro de las causales de inhabilidad e incompatibilidad del orden constitucional o legal para ejercer cargos públicos mediante Formato de Hoja de Vida - DAFP), (ii) carecer de antecedentes judiciales, fiscales y disciplinarios de Personería y Procuraduría, y (iii) haber diligenciado el registro de hoja de vida y Declaración de Bienes y Rentas en el Sistema de Información Distrital del Empleo y la Administración Pública – SIDEAP, se tiene que la señora **SANDRA MARÍA LEÓN MEDRANO** identificada con cédula de ciudadanía 55.166.255 cumple con los requisitos legales y funcionales establecidos para el ejercicio del empleo Auxiliar Administrativo Código 407 Grado 09 asignado a la Dirección de Ingeniería de Tránsito de la planta global de empleos de la Secretaría Distrital de Movilidad que se encuentra en vacancia temporal.

Que por lo anterior se considera procedente nombrar en provisionalidad a SANDRA MARÍA LEÓN MEDRANO en la respectiva vacancia temporal existente dentro de la planta global de empleos de la Secretaría Distrital de Movilidad.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Nombrar dentro de la planta de empleos de la Secretaría Distrital de Movilidad a **SANDRA MARÍA LEÓN MEDRANO** identificada con cédula de ciudadanía 55.166.255 mediante nombramiento en provisionalidad en empleo Auxiliar Administrativo Código 407 Grado 09 asignado a la Dirección de Ingeniería de Tránsito de la planta global de empleos de la Secretaría Distrital de Movilidad que se encuentra en vacancia temporal.

ARTÍCULO SEGUNDO: El nombramiento de que trata el artículo anterior es de carácter PROVISIONAL y hasta por el término de la situación administrativa de encargo otorgada mediante Resolución No. 049 del 15 de febrero de 2019 a la siguiente funcionaria:

FUNCIONARIO TITULAR	CÉDULA	DENOMINACIÓN	CODIGO	GRADO	DEPENDENCIA	IDENTIFICACIÓN DE DEPENDENCIA
AIDA NELLY LINARES VELANDIA	41.758.778	AUXILIAR ADMINISTRATIVO	407	09	DIRECCIÓN DE INGENIERÍA DE TRÁNSITO	407-09-01

PARÁGRAFO: Antes de cumplirse la condición resolutoria correspondiente del nombramiento provisional efectuado mediante el presente acto administrativo, el nominador, por resolución motivada, podrá darlos por terminados de conformidad de conformidad con la potestad normativa establecida por el artículo 2.2.5.3.4 del Decreto 1083 de 2015 Único Reglamentario del Sector de Función Pública (modificado por el Decreto Nacional 648 de 2017) y los criterios definidos por la jurisprudencia Constitucional y Contencioso Administrativa.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los siete (7) días del mes de junio de dos mil diecinueve (2019).

JUAN PABLO BOCAREJO SUESCÚN
Secretario Distrital de Movilidad

EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTÁ - ESP

Resolución Número 0520

(Junio 7 de 2019)

POR MEDIO DE LA CUAL SE DEFINEN LOS OBJETIVOS DE CONTROL QUE SE DEBEN APLICAR EN EL USO DE LA INFORMACIÓN DE LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTÁ -ESP

EL GERENTE DE TECNOLOGÍA (E) DE LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE BOGOTÁ-ESP, en ejercicio de sus facultades estatutarias, en especial las recibidas en numeral 5 del artículo 61 del Acuerdo 11 de 2013 de la Junta Directiva, para definir normas técnicas y estándares para ser aplicados y fortalecer la gestión de la Empresa en todos los procesos y,

CONSIDERANDO:

Que el Decreto 1499 del 2017 del Departamento Administrativo de la Función Pública que modifica

el Decreto 1083 de 2015, en lo relacionado con los Sistemas de Gestión, requiere que la Empresa defina las pautas del manejo de la información en cuanto a transparencia, acceso a la información pública, lucha contra la corrupción y seguridad digital.

Que de acuerdo con lo previsto en el literal k del artículo 17 de la Ley 1581 de 2012, la Empresa deberá definir políticas y procedimientos para garantizar el adecuado cumplimiento de dicha ley por parte de los responsables del tratamiento de datos personales.

Que los artículos 38 y 62 de la Ley 1952 de 2019 – Código General Disciplinario, señala los deberes de custodiar, cuidar, evitar e impedir la sustracción, destrucción, ocultamiento o utilización indebida de la documentación e información que por razón de su empleo, cargo o función conserve el servidor público bajo su cuidado o a la cual tenga acceso.

Que de acuerdo con lo previsto en el numeral 3 del artículo 2.2.22.3.3 el Decreto 1499 del 2017, dentro de los objetivos de MIPG se encuentran "Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua"

Que el artículo 2.2.22.3.5. del Decreto en mención estableció el Manual Operativo del Sistema de Gestión-MIPG por el Consejo para la Gestión y Desempeño Institucional el cual fue emitido en agosto de 2018 y por el cual se rige la EAAB-ESP de acuerdo con la Resolución 1260 de 2018 que adoptó el modelo integrado de planeación y gestión-MIPG.

Que el Manual Operativo del Sistema de Gestión MIPG establece las responsabilidades frente a la primera línea de defensa correspondiente a cada área de la EAAB - ESP.

Que en consecuencia cada área y su funcionario de nivel directivo de la EAAB-ESP se encargarán del mantenimiento efectivo de controles, de la gestión operacional, de la identificación, evaluación, control y mitigación de riesgos, de la implementación de acciones correctivas y de la detección de deficiencias de control.

Que de conformidad con la Resolución 740 de 2018 - Política General de Seguridad y Privacidad de la Información, la EAAB ESP debe formular controles que protejan su información acorde con su valor e importancia, y preservar su nivel de protección durante su ciclo de vida.

En mérito de lo expuesto, la EAAB ESP,

RESUELVE:

ARTÍCULO PRIMERO. - OBJETO: Establecer los objetivos de control que debe cumplir la Empresa en el manejo de la información acorde con los niveles de clasificación que ha analizado cada Responsable o Determinador.

ARTÍCULO SEGUNDO. - Definiciones: Para los efectos de la presente Resolución se entenderá por:

a) **Activo de información:** Agrupación de elementos de información, homogéneos en riesgo y en condiciones de uso, categorizados por el nivel de criticidad y por el de transparencia y con acceso definido.

b) **Colaborador:** Persona natural o jurídica que ejecuta una función de trabajo autorizada y amparada por un vínculo con la Empresa.

c) **Control:** Directriz, medida o práctica para gestionar el riesgo, que puede ser de naturaleza administrativa, técnica o de gestión legal.

d) **Criticidad:** Es el grado de vinculación de la información en la operación de los procesos en la Empresa. Se calcula en función del valor de la confidencialidad, la integridad y la disponibilidad de la información.

- **Criticidad Baja:** la información genera impacto de funcionamiento en la gestión de una sola dependencia de la Empresa.
- **Criticidad Media:** la información genera impacto de funcionamiento en más de una dependencia de la Empresa.
- **Criticidad Alta:** la información afecta la imagen de la Empresa y/o tiene consecuencias legales o financieras y/o afecta entidades externas.

e) **Cuenta de Acceso:** identificación y contraseña a través de la cual un usuario de la información accede a un servicio, aplicación o recurso informático.

f) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art. 3).

g) **Documento oficial:** Elemento del registro de la Empresa, que surgen de la información gestionada continuamente. Son regulados por el subsistema de Gestión Documental de la Empresa.

h) **Incidente de seguridad:** Son todos los hechos o actos de desviación a la política de seguridad y Privacidad de la Información que afecte la Empresa o a una persona.

i) **Información:** Datos, documentos o notas de trabajo.

j) **Información digital:** Información que se representan en forma electrónica y que residen en

medios digitales o en la nube. Son ejemplos: 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 en un futuro como resultado de desarrollos tecnológicos.

k) **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (art. 6, literal b de la Ley 1712 de 2014).

l) **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el art. 6, literal c de la Ley 1712 de 2014.

m) **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el art. 6, literal d de la Ley 1712 de 2014.

n) **Infraestructura Informática o Tecnológica:** Componentes de programas (software) y equipos (hardware) de comunicaciones, cómputo, red, almacenamiento, impresión y protección que soportan los diferentes sistemas o aplicativos o aplicaciones de información. También denominado recurso informático.

o) **Medios Digitales:** Elementos donde se almacena o fluye la información digital. Constituyen formas conocidas los equipos portátiles, computadores personales, discos duros, unidades flash, unidades USB, teléfonos inteligentes, tabletas y otras formas que aparezcan con desarrollos tecnológicos.

p) **Medio físico:** Elemento donde se representa información impresa mecánica o manualmente, como papel, otros medios impresos o visuales, fotocopias o cualquier tipo de documento físico.

q) **Nivel de Clasificación:** Categorías de criticidad y confidencialidad de la información fijadas por el Responsable o Determinador, de acuerdo a la normatividad vigente y que son:

- **Por Transparencia:** pública, pública clasificada o pública reservada.
- **Por criticidad:** baja, media o alta.

r) **Objetivo de control:** Es el aspecto del riesgo que se va a tratar.

s) **Responsable o Determinador:** Es el funcionario de nivel directivo de la EAAB-ESP que, en razón de su cargo o función, es responsable del proceso que origina la información.

t) **Servicios Informáticos:** Servicios que se proveen como una combinación de componentes humanos y de infraestructura informática o tecnológica. Como por ejemplo: servicios de sistemas, aplicativos o aplicaciones de información, aprovisionamiento y/o suministro de recursos informáticos, actividades de soporte técnico humano. (Atendiendo lo establecido en el literal m del art. 2 de la Resolución 740 de 2018)

u) **Sistema, aplicativo o aplicación de Información:** Cobija componentes de infraestructura informática para generar, enviar, recibir, archivar o procesar alguna forma de datos. (Atendiendo lo establecido en el literal n del art. 2 de la Resolución 740 de 2018)

v) **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 la misma.

ARTÍCULO TERCERO: - OBJETIVOS DE CONTROL
Los objetivos de control de la información de la EAAB-ESP son los siguientes:

1. Protección de la confidencialidad de información.
2. Protección de la confidencialidad en los medios donde se encuentra o fluye la información.
3. Protección de la confidencialidad de la información como elemento probatorio.
4. Protección de los sitios donde se encuentran medios de información.
5. Protección de la confidencialidad cuando se imprime información.
6. Protección de la confidencialidad mediante la autorización de uso.
7. Protección de la confidencialidad en el uso de la información por terceros.
8. Registro de uso de información para demostrar la preservación de la confidencia.
9. Protección de la confidencialidad en el uso interno de la información.
10. Protección de la confidencialidad de la información en copias.

11. Protección de la confidencialidad en la disposición de la información.
12. Gobierno en el uso de la información.
13. Protección de la confidencialidad en la transmisión digital.
14. Protección de la confidencialidad de la información en el transporte de medios.
15. Protección de la información en la entrega del puesto de trabajo.
16. Protección de la confidencialidad de la información en el reporte a entidades externas.
17. Reporte de violaciones a la confidencialidad de la información.
18. Protección contra la pérdida o alteración de información en medios digitales removibles.
19. Protección contra la pérdida o alteración de la información mediante copias de respaldo.
20. Restauración de la información por pérdida o alteración.
21. Disponibilidad de la información ante eventos de interrupción de servicios.
22. Protección contra la pérdida o alteración de la información mediante copias de respaldo en la nube.
23. Custodia de información.
24. Protección contra la adulteración de información como elemento probatorio.
25. Protección contra la adulteración de la información.
26. Protección del capital intelectual por el uso de software de terceros.
27. Protección del capital intelectual de EAAB-ESP de software propio.
28. Reporte de violaciones a los controles contra pérdida y alteración de la información.

PARÁGRAFO PRIMERO: Los objetivos de control señalados en el presente acto administrativo se desarrollarán en el formato denominado "MPFT0209F01 Condiciones de uso de la información" donde se presentarán los controles mínimos exigidos por EAAB-ESP según cada nivel de clasificación de la información y según el medio donde resida la información.

ARTÍCULO CUARTO: - El Responsable o Determinador implementará los controles de cada objetivo de control en el marco del procedimiento "MPFT0209P Clasificación y protección de la información" o del que lo modifique o sustituya.

ARTÍCULO QUINTO: - Los objetivos de control en el uso de la información son de obligatorio cumplimiento por cada Usuario de la información. Cada Responsable o Determinador de la información vigilará permanentemente su aplicación a partir de la fecha de divulgación. Cualquier desviación será resuelta por cada área como un incidente de seguridad y deberá ser puesta en conocimiento del Subsistema de Seguridad de la Información – SGSI.

ARTÍCULO SEXTO: - El Responsable o Determinador divulgará la lista de sus activos de información y los controles a los Usuarios de la información.

ARTÍCULO SÉPTIMO. – Los controles en el uso de la información estarán disponibles para consulta en la Empresa y serán divulgados dentro los planes de inducción de funcionarios.

ARTÍCULO OCTAVO - La presente Resolución rige a partir de la fecha de expedición.

Dada en Bogotá, D.C., a los siete (7) días del mes de junio de dos mil diecinueve (2019).

PUBLÍQUESE Y CÚMPLASE.

WILLIAM ALBERTO SASTOQUE JIMÉNEZ
Gerente de Tecnología (E.)

DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

Resolución Número 499

(Diciembre 28 de 2018)

Por la cual se adopta la Guía para la evaluación de propuestas y/o solicitudes de creación de los Distritos Especiales de Mejoramiento y Organización Social – DEMOS y se toman otras decisiones

LA DIRECTORA DEL DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO
En uso de sus atribuciones legales y en especial las conferidas por el Acuerdo 018 de 1999 y por los Decretos Distritales 138 de 2002 y 540 de 2018, y

CONSIDERANDO:

Que de conformidad con el artículo 3º del Acuerdo Distrital 018 de 1999, le corresponde al Departamento Administrativo de la Defensoría del Espacio Público – DADEP, sin perjuicio de las atribuciones de