Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

EMPRESA PÚBLICA CASA PARA TODOS EP

RESOLUCIÓN ADMINISTRATIVA No. EPCPT-2020-294

CONSIDERANDO:

Que, el artículo 229 de la Constitución de la República del Ecuador define como *servidores públicos a todas las personas que en cualquier forma o a cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público, y señala que sus derechos son irrenunciables*;

Que, la Ley Orgánica de Empresas Públicas, en el artículo 3, establece que: *"Las empresas públicas se rigen por los siguientes principios:*

1. Contribuir en forma sostenida al desarrollo humano y buen vivir de la población ecuatoriana;
2. Promover el desarrollo sustentable, integral, descentralizado y desconcentrado del Estado, y de las actividades económicas asumidas por éste.
3. Actuar con eficiencia, racionalidad, rentabilidad y control social en la exploración, explotación e industrialización de los recursos naturales renovables y no renovables y en la comercialización de sus productos derivados, preservando el ambiente;
4. Propiciar la obligatoriedad, generalidad, uniformidad, eficiencia, universalidad, accesibilidad, regularidad, calidad, continuidad, seguridad, precios equitativos y responsabilidad en la prestación de los servicios públicos;
5. Precautelar que los costos socio-ambientales se integren a los costos de producción;
6. Preservar y controlar la propiedad estatal y la actividad empresarial pública".

Que, el artículo 10 de la Ley Orgánica de Empresas Públicas, establece que: "*La o el Gerente General de la empresa pública será designado por el Directorio, de fuera de su seno. Ejercerá la representación legal, judicial y extrajudicial de la empresa y será en consecuencia el responsable de la gestión empresarial, administrativa, económica, financiera, comercial, técnica y operativa. (...)*";

Que, el artículo 11 del mismo cuerpo legal prescribe que: "*El Gerente General, como responsable de la administración y gestión de la empresa pública, tendrá los siguientes deberes y atribuciones: (...) 4. Administrar la empresa pública, velar por su eficiencia empresarial; (...) 8. Aprobar y modificar los reglamentos internos que requiera la empresa, excepto el señalado en el numeral 8 del artículo 9 de esta Ley; (...)*";

Que, el artículo 9 y el literal a), numeral 1) del artículo 77 de la Ley Orgánica de la Contraloría General del Estado *dispone como responsabilidad de la máxima autoridad de cada organismo del sector público, el establecimiento de políticas, métodos y procedimientos de control interno para salvaguardar sus recursos;*

Que, el literal e) del artículo 77 de la norma ibídem dispone que las máximas autoridades de las instituciones del Estado son responsables de los actos, contratos, o resoluciones emanados de su autoridad y establece para éstas, entre otras atribuciones y obligaciones específicas la de: *"e) Dictar los correspondientes reglamentos y demás normas secundarias necesarias para el eficiente, efectivo y económico funcionamiento de sus instituciones (…)".*

Que, mediante Decreto Ejecutivo No. 622 de 17 de marzo de 2015 publicado en el Registro Oficial No. 474 de 7 de abril de 2015, se crea la Empresa Pública Nacional de Hábitat y Vivienda EP, como una persona jurídica de derecho público, con patrimonio propio, dotada de autonomía presupuestaria, financiera, económica, administrativa, operativa y de gestión, acorde con los objetivos establecidos en el Sistema Nacional Descentralizada de Planificación Participativa y disposiciones de la Ley Orgánica de Empresas Públicas y dicho

Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

decreto ejecutivo;

Que, mediante Decreto Ejecutivo 976 se reformó el Decreto Ejecutivo No. 622, en lo referente al objeto de la Empresa, estableciendo que: "*(...) La Empresa Pública Nacional de Hábitat y Vivienda EP tiene por objeto elaborar e implementar programas, planes y proyectos referidos a la mejora del hábitat y el acceso a la vivienda, desarrollo de infraestructura hotelera con sujeción al Plan Nacional de Desarrollo, las políticas nacionales sectoriales y las instrumentos de planificación empresarial que le son propios. (...)*";

Que, mediante Decreto Ejecutivo Nro. 11, del 25 de mayo de 2017, publicado en el segundo suplemento del Registro Oficial número 16 del 16 de junio del 2017 se modificó la denominación de la Empresa Pública de Hábitat y Vivienda EP a Empresa Pública " Casa para Todos" EP y se le encarga la ejecución del Programa "Casa para Todos", bajo la coordinación del Ministerio de Desarrollo Urbano y Vivienda y como un componente de la Misión Toda una Vida.

Que, mediante Decreto Ejecutivo Nro. 101, se reemplaza el artículo 8 del Decreto Ejecutivo Nro. 11 de 25 de mayo de 2017, por el siguiente: "*Modifíquese la denominación de la Empresa Pública de Vivienda EP a Empresa Pública "Casa para Todos" EP. Encárguese de la ejecución del Programa "Casa para Todos" y como un componente de la Misión "Toda una Vida", a la Empresa Pública "Casa para Todos" EP y a la Empresa Pública de Desarrollo Estratégico Ecuador Estratégico EP*"

Que, *mediante Acuerdo Nro 025-2019 de 20 de Septiembre de 2019 el MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACIÓN, expide el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva*

Que, mediante memorando Nro. EPCPT-EPV-2020-0021-M de 23 de enero de 2020, la máxima autoridad, designa el Comité de Seguridad de la Información.

Que, con Resolución DIR-EPCPT-0034-2020 de 21 de julio de 2020, el Directorio de la Empresa Pública Casa Para Todos, resolvió designar al Arq. Edison Gregorio Antonio Morán Acuña como Gerente General Subrogante;

Que, es necesario implementar las regulaciones existentes, a fin de dar mayor seguridad jurídica dentro de la institución y adoptar un "proceso de gestión de seguridad de la información"; orientado a mantener la integridad, disponibilidad y confidencialidad de la información.

En ejercicio de las atribuciones que le confiere la Ley Orgánica de Empresas Públicas y el Estatuto del Régimen Jurídico de la Función Ejecutiva:

RESUELVE:

Expedir la **POLÍTICA GENERAL DE SEGURIDAD DEL INFORMACIÓN**

Artículo 1.- Beneficiarios.- La presente política será de estricto cumplimiento para los profesionales y servidores que de alguna manera presten servicios con la Empresa, con el fin de garantizar y resguardar la información a cargo de la EPCPT.

La Empresa Pública Casa Para Todos EP, a través de la presente considera a la información como un activo de alto valor institucional, por lo cual debe seguir parámetros adecuados para garantizar la seguridad de la información confidencial, critica, y sensible sea en medio (físico o digital) en el que se encuentre.

Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

Los parámetros mínimos con los que se definirá el "Sistema de Gestión de Seguridad de la Información", serán: confidencialidad, disponibilidad, e integridad; adicionalmente serán considerados parámetros de autenticidad, trazabilidad, etc.

Artículo 2.- Objeto.- Establecer los lineamientos, sobre los cuales se desarrollará el Sistema de Gestión de la Información, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de los activos de información definiendo el uso de la normativa legal vigente; así como, la aplicación de normas y buenas prácticas especializadas en seguridad de la información.

Artículo 3.- Alcance.- Está política, se aplicará a todos los servidores y funcionarios de la Empresa Pública Casa Para Todos EP a nivel nacional, así como a las entidades externas y ciudadanía en general que maneje o acceda a información crítica o sensible de la institución.

Artículo 4.- **Vigencia.-** La presente política entrará en vigencia, una vez sea aprobada mediante resolución administrativa. La revisión y actualización por parte del Comité de Seguridad de la Información será al menos cada 12 meses, salvo en los casos que amerite una revisión anticipada.

Artículo 5.- **Glosario de términos y definiciones.-** Para efectos de esta política el glosario de términos y definiciones utilizadas, será el siguiente:

a. Activo de información: Es todo activo de alta validez para la Empresa que maneja información crítica o sensible.

b. Autenticidad: Propiedad de que una entidad es lo que afirma ser.

c. Confiabilidad: Es la garantía de que la información es la apropiada para la administración de la entidad, ejecución de transacciones y para el cumplimiento de sus obligaciones.

d. Confidencialidad: Propiedad de que la Información no está disponible o divulgada a individuos, entidades o procesos no autorizados.

e. Custodio de información: Personas o grupos de personas que administran, controlan la información, distribuyen información, estos proveen los controles físicos y lógicos, administran los accesos a los usuarios de información, basados en lo especificado por el propietario de Información.

f. Disponibilidad: Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

g. GAP Analysis (Análisis de madurez}: El gap análisis es un servicio que permite identificar la distancia (brecha) existente en la institución frente a las buenas prácticas y normas en temas de seguridad de la información.

h. Hardening: Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

i. Información: Grupo de datos procesados, supervisados, ordenados y estructurados con un sentido o mensaje, que puede ser utilizado para generar un conocimiento.

j. Información critica: Información indispensable para la operación de la institución.

k. Información sensible: Información cuyo contenido debe ser únicamente conocida por las personas autorizadas.

l. Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos.

m. Propietario de información: Los propietarios de información, pueden ser una persona o grupo de personas,

que generan o tienen bajo su custodia activos de información, determinan la clasificación, etiquetado y manipulación; autorizan el acceso y los controles necesarios a implementar por parte de los custodios sobre dichos activos de información.

n. Responsables de la aplicación de los procesos institucionales: Se refiere a las máximas autoridades representantes de los procesos institucionales.

o. Usuarios de información: Personas o grupos de personas, que acceden o administran información, para los fines que fueron autorizados determinados por el propietario de información. Por tal motivo, el usuario de deberá cumplir con todas las directrices de seguridad de la información.

Artículo. 6.- Compromisos y principios-. La Empresa Pública Casa Para Todos EP, los servidores y funcionarios en general, y el personal externo que presta servicios a la institución, adquieren los compromisos y principios que rigen la implementación del Sistema de Gestión de Seguridad de la Información, teniendo como fin el precautelar la seguridad de la información propia y de terceros, obtenida directa o indirectamente como parte de su gestión y actividades institucionales.

Artículo 7.- **Política General de Seguridad de la Información.-** La Empresa Pública Casa Para Todos EP a través de las Gerencias y Direcciones, deberá cumplir lo siguiente:

a. Establecer lineamientos para la identificación y levantamiento de sus activos de información crítica.

b. Determinar los objetivos del Sistema de Gestión de Seguridad de la información alineados a su Planificación Estratégica Institucional, así como los requerimientos y necesidades del contexto ínterno y externo.

c. Preservar y mantener la confidencialidad, integridad y disponibilidad de sus activos de información críticos, gestionando adecuadamente los riesgos productos de las diferentes amenazas y la correcta identificación de sus vulnerabilidades.

d. Establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, considerando un marco adecuado de gestión de riesgos.

e. Reconocer y mantener el cumplimiento de los requerimientos dispuestos por leyes, reglamentos, normas, relacionados a la Seguridad de la Información.

f. Definir los lineamientos para clasificar y etiquetar adecuadamente los activos de información.

g. Mantener la información crítica y sensible, que no esté clasificada con carácter de confidencial hasta su etiquetado formal. Dicho tratamiento deberá ser establecido en un proceso o procedimiento de clasificación de la información que por su extensión no se incluye en el presente documento.

h. Disponer la no divulgación y reproducción, de información catalogada como confidencial y/o restringida sin la autorización explícita para dicho efecto.

i. Disponer la propiedad de la Empresa Pública Casa Para Todos EP sobre la información que gestiona o genera por la ejecución propia de sus actividades.

j. Disponer que la propiedad de la información considerará como tal a las patentes, técnicas, modelos, invenciones, metodologías, conocimiento y experiencia, procesos, algoritmos, programas, ejecutables, diseños, información financiera, información de evaluaciones y estudios, etc.; asi como la información, productos, servicios resultantes de consultorías y proyectos desarrollados para la institución por parte de proveedores o consultores, entre otros.

k. Mantener la implementación de controles físicos de acceso a personal autorizado donde se administre

Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

información crítica o sensible.

l. Incluir acuerdos de confidencialidad en los contratos con terceros (proveedores, consultoras, etc.) que prestan servicios, así como de todos los servidores y funcionarios de la institución.

m. Definir y delegar los roles y responsabilidades, sobre los activos de información críticos considerándose para el efecto la designación de propietarios, custodios y usuarios de información por parte de los responsables de la aplicación de los procesos institucionales.

n. Definir o delegar las funciones y responsabilidades a un comité competente como órgano rector del proceso de seguridad de la información.

o. Definir la inclusión de acuerdos de intercambios de información, en los que se incluyan los lineamientos, así como los acuerdos o cláusulas de confidencialidad, firmado a su vez por las máximas autoridades de las partes involucradas en procesos de intercambio de información.

p. Establecer métricas y lineamientos para la medición de la eficacia del Sistema de Gestión de Seguridad de la información, así como la gestión adecuada de los riesgos en dicha materia.

q. Fomentar una cultura organizacional en temas de seguridad de la información, a través de planes de capacitación y concientización.

r. Definir los roles y responsabilidades del personal frente a la seguridad de la información.

Artículo 8.- Organización Interna de Seguridad de la Información.- Para el cumplimiento de lo previsto en esta resolución, se han definido los siguientes roles y responsabilidades como parte de la gestión de Seguridad de la Información:

1. Comité de Seguridad de la Información..- Para el cumplimiento de lo previsto en esta resolución el Comité de Seguridad de la Información tendrán a su cargo entre otras las siguientes funciones:

i. Revisar y aprobar la Política General de Seguridad de la Información.

ii.Fomentar el compromiso de la Empresa en temas de seguridad de la información.

iii. Definir y aprobar la estructura de la seguridad de la información, los roles y responsabilidades del personal involucrado en seguridad de la información.

iv. Conocer, definir y aprobar los marcos de referencia, normas, metodologías, políticas, etc.

v. Determinar y aprobar el alcance e implementación del Sistema de Gestión de Seguridad de la Información de la EPCPT.

vi. Conocer y aprobar la Metodología de Gestión de Riesgos de Seguridad de la Información; definir y delegar los equipos responsables del análisis y cálculo de matriz de riesgos de seguridad de la información.

vii. Determinar el rango de impacto econórmico a causa del riesgo, que estaría dispuesto a correr la Empresa por temas de seguridad de la información.

viii. Analizar y aprobar la información obtenida de la evaluación del GAP Análisis de Seguridad de la Información, así como de otras fuentes que permitan determinar el estado de madurez y las decisiones a tomar en temas de seguridad de la información.

ix. Analizar y aprobar los proyectos orientados a la reducción de brechas de seguridad de la información, así

como los costos y recursos necesarios para su implementación.

x. Velar por el estricto cumplimiento de las normas, políticas, procesos y procedimientos definidos en temas de seguridad de la información.

xi. Conocer y aprobar las mallas curriculares de los eventos de capacitación y concientización dirigidos a los servidores de la institución en materia de seguridad de la información.

xii. Las responsabilidades determinadas en la conformación del comité, así como las demás inherentes a las atribuciones propias en temas de seguridad de la información que determine la normativa legal vigente.

xiii. Delegar a un responsable del proceso de seguridad de la información, quien hará las funciones del Oficial de Seguridad de la Información.

2. Experto en Seguridad de la Información - Oficial de Seguridad de la Información.- El Comité de Seguridad de la Información delegará un responsable del proceso de seguridad de la información, siendo sus principales funciones las siguientes:

i. Elaborar, actualizar y proponer al Comité de Seguridad de la Información la Política General de Seguridad de la Información, para su aprobación.

ii. Elaborar y ejecutar el Plan de comunicación de los beneficios de la Seguridad de la Información a nivel nacional.

iii. Mantener actualizado el inventario general de activos de Información.

iv. Elaborar, actualizar y difundir las normas, políticas, metodologías, y demás documentos de seguridad de la información, alineados a las normas, reglamentos internos y leyes vigentes.

v. Establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información, considerando un marco adecuado de gestión de riesgos, conforme el alcance definido en esta política

vi. Supervisar que las decisiones tomadas por el Comité de Seguridad de la Información, sean ejecutadas por las partes involucradas.

vii. Coordinar las actividades de levantamiento del GAP Análisis de Seguridad de la Información.

viii. Coordinar el levantamiento de los activos de información y su clasificación.

ix. Coordinar la inclusión de temas de Seguridad de la Información en la implementación del Plan Estratégico y de Negocios.

x. Diseñar y supervisar los niveles de implementación del Sistema de Gestión de Seguridad de la Información, así como dar seguimiento a las acciones preventivas y correctivas.

xi. Promover proyectos orientados a reducir las brechas de seguridad de la información institucional.

xii. Asesorar a las áreas o partes involucradas en el levantamiento e identificación de riesgos de seguridad de la información, así como la coordinación en la generación de planes de tratamiento de los mismos.

xiii. Coordinar con los involucrados la identificación y reporte de incidentes de riesgos de seguridad de la información más relevantes.

xiv. Proponer al Comité de Seguridad de la Información, las mallas curriculares de eventos de capacitación en

materia de seguridad de la información, así como coordinar y evaluar la ejecución de los mismos.

xv. Dar lineamientos en la suscripción de convenios, acuerdos y compromisos de confidencialidad relacionados con la utilización de información crítica o sensible en eventos de capacitación y en programas de cooperación interinstitucional.

xvi. Revisar y monitorear el estado de resolución de eventos de seguridad de la información con las partes involucradas.

vii Identificar mediante un GAP Análisis, el alcance de controles a implementar en la Empresa.

xviii. Gestionar la contratación de los proyectos de ethical hacking, a realizarse en la Empresa.

xix. Tomar conocimiento de los resultados del ethical hacking interno y externo y análisis de vulnerabilidades realizados periódicamente por el responsable de seguridad informática sobre los recursos tecnológicos.

xx. Verificar los resultados periódicos de la ejecución del ethical hacking interno/externo sobre la infraestructura tecnológica efectuadas por el responsable de seguridad informática.

xxi. Realizar periódicamente como parte del ethical hacking, la fase de pruebas de ingeniería social.

xxii. Identificar convenientemente las partes interesadas, requisitos y canales de comunicación con grupos de interés de la institución, así como entes y organismos externos en ámbitos de la seguridad de la información.

3. Responsables de la aplicación de los procesos institucionales.- En el marco de la presente política deberá cumplir con las siguientes funciones y responsabilidades:

i. Realizar el levantamiento de los activos de información a su cargo, con asesoría del responsable de Seguridad de la Información.

ii. Participar en los equipos destinados para el análisis de riesgos de seguridad de los activos de información a su cargo.

iii. Determinar conjuntamente con el responsable de Seguridad de la Información/Informática los controles a implementar para asegurar los activos de información, considerando para el efecto los niveles, perfiles y roles de acceso o modificación de la información crítica y sensible para la institución, así como la clasificación de la información.

iv. Asignar las responsabilidades del propietario, custodio y usuarios de la información en la administración de activos de información críticos y sensibles.

v. Instruir al personal a su cargo, sobre el buen uso de los activos de información críticos.

vi. Cumplir y hacer cumplir al personal a su cargo los parámetros de confidencialidad, disponibilidad e integridad de los activos de información.

4. La Gestión de Talento Humano.- En el marco de la presente política deberá cumplir con las siguientes funciones y responsabilidades:

í. Validar la información que forma parte de los procesos de contratación de nuevo personal e incluir dentro de sus competencias controles para garantizar la seguridad de la información.

ii. Definir conjuntamente con los líderes de los procesos, los cargos o puestos críticos en los cuales se maneja información crítica y sensible, definiendo los procesos de selección que se seguirán en dichos casos para

garantizar la seguridad de la información.

iii. Incluir en los procedimientos de selección de personal, para los cargos en los que se maneja información crítica o sensible, la verificación de antecedentes penales, de acuerdo a las leyes, regulaciones y normas, e información confidencial a la que acceden.

iv. Incluir en los procedimientos de vinculación de nuevos servidores o funcionarios, talleres de concienciación en temas de seguridad de la información, así como la difusión de la Política General de Seguridad de la Información, y la normativa interna.

v. Diseñar y ejecutar eventos de capacitación y de concientización en materia de seguridad de la información, en función de las mallas curriculares aprobadas por el Comité de Seguridad de la Información, previo trámite de su incorporación en el Plan Institucional de Capacitación.

vi. Coordinar los programas de capacitación de los servidores públicos en temas de seguridad de la información de forma periódica durante su permanencia en la instalación.

vii. Incluir dentro del proceso de contratación la firma del acuerdo o compromiso de confidencialidad de la información crítica y sensible de la Empresas.

viii, Instrumentar los procedimientos administrativos previos a la aplicación de sanciones por el incumplimiento de la Política General de Seguridad de la Información, y demás referentes a seguridad de la información.

ix. Durante la vinculación del personal, la Gestión de Talento Humano, deberá realizar de forma periódica la firma de acuerdo de confidencialidad de todo el personal.

x. Como parte de los procesos internos de la Gestión de Talento Humano, conjuntamente con la Gestión de Tecnologías de la Información y el Experto en Seguridad de la Información - Oficial de Seguridad de la información, deberán determinar los procedimientos a seguir en la desvinculación del personal, alineados a los siguientes parámetros:

a. Clasificar la baja del personal.
b. Comunicación de las bajas de personal.
c. Gestión de las bajas de personal.

5. Gestión de Tecnologías de la Información.- En el marco de la presente política deberá cumplir con las siguientes funciones y responsabilidades:

i.Delegar los equipos internos para la ejecución de análisis de riesgos tecnológicos de la Dirección Administrativa.

ii. Elaborar e implementar el Plan de Seguridad Informática, considerando el análisis de riesgos tecnológicos identificados en los activos de información de la Dirección Administrativa, elementos relacionados procedentes del GAP Análisis y de las políticas estratégicas y operativas relacionadas con el aseguramiento tecnológico.

iii. Mantener un responsable de Seguridad Informática, el cual tendrá como uno de sus roles principales el enlazar las estrategias de la organización y de la Coordinación General de Tecnología con los requerimientos de seguridad.

iv. Disponer el establecimiento de la base del correcto funcionamiento de la infraestructura tecnológica, así como el monitoreo constante que permita identificar oportunamente anomalías y posibles incidentes o eventos de seguridad en infraestructura que soporta los procesos del negocio.

Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

v. Disponer el establecimiento de procedimientos operativos que permitan asegurar los diferentes componentes tecnológicos orientados al procesamiento y gestión de los diferentes activos de información dentro del ámbito de su competencia.

vi. Disponer el desarrollo e implementación de metodologías de desarrollo seguro, en los que se establezca adicionalmente los parámetros necesarios para adquisición, mantenimiento y desarrollo del software en todo el ciclo de vida.

Artículo 9.- **Sanciones-.**

i. Las sanciones a aplicarse serán las dispuestas en la normativa legal vigente, dependiendo de la gravedad del evento.

ii. De exponerse información crítica y sensible que sobrepase las atribuciones de la Empresa Pública Casa Para Todos EP, se considerará lo dispuesto en las Leyes, Decretos, Normas vigentes para dicho efecto.

iii Para efectos de terceros, que gestionen información crítica o sensible de la Empresa Pública Casa Para Todos EP se aplicarán las sanciones dispuestas en las cláusulas establecidos en los contratos.

DISPOSICIONES GENERALES

PRIMERA.- La ejecución de la presente Política Institucional es de cumplimiento obligatorio para todos los servidores y funcionarios de la Empresa Pública Casa Para Todos EP.

SEGUNDA.- De considerarlo pertinente el Comité de Seguridad de la Información, determinará los equipos, funciones y responsabilidades necesarias para el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información.

TERCERA.- El incumplimiento a lo previsto en la presente resolución será sancionado de conformidad con la legislación vigente.

DISPOSICIÓN FINAL.- La presente resolución entrará en vigencia a partir de su expedición.

Comuníquese y Cúmplase.- Dado y firmado en San Francisco de Quito**.**

Documento firmado electrónicamente

Mgs. Edison Antonio Morán Acuña
GERENTE GENERAL, SUBROGANTE

Copia:
Señora Ingeniera
Paola Daniela Obando Llerena
Especialista de Talento Humano

Señor Ingeniero
José Luis Melo Espinoza
Director Financiero

Señor Ingeniero
José Luis Melo Espinoza.
Director Administrativo, Encargado

Señor Magíster

Resolución Nro. EPCPT-EPV-2020-0134-R

Quito, D.M., 20 de octubre de 2020

Ahmad Nicolas Amhaz Ruiz
Director de Planificación y Seguimiento

Señor Ingeniero
Mario Alvarez Méndez
Director de Infraestructura, Encargado

Señor Ingeniero
Mario Heriberto Álvarez Méndez
Director de Gestión Territorial

Señor Abogado
William Darwin Cuñas Reinoso.
Jefe de Transferencia de Dominio, Subrogante

nof

Firmado electrónicamente por:
EDISON GREGORIO ANTONIO MORAN ACUNA