# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## Empresa Municipal de Renovación Urbana EMRU E.I.C.

## Versión 2:2019

## Contenido

## 1. OBJETIVO

Definir los lineamientos y directrices que se deben seguir por parte los colaboradores y terceros de la Empresa Municipal de Renovación Urbana EMRU E.I.C., con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

## 2. Objetivos Específicos

a) Minimizar el riesgo de los procesos de la Empresa Municipal de Renovación Urbana EMRU E.I.C.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el Sistema de Gestión de la Seguridad de la Información.
g) Proteger los activos de información.
h) Establecer la Políticas, procedimientos e instructivos en materia de información.
i) Fortalecer la cultura de seguridad de la información en la Empresa Municipal de Renovación Urbana EMRU E.I.C.
j) Garantizar la continuidad del negocio frente a incidentes.

## 3. Alcance

La presente política debe ser cumplida por todos los colaboradores (contratistas, funcionarios de planta) y terceros de todos los procesos de la Empresa Municipal de Renovación Urbana EMRU E.I.C., y, adicionalmente, por los ciudadanos, persona natural o jurídica, nacional o extranjera que sin tener relación laboral o contractual con la entidad tengan acceso a sus instalaciones y/o servicios tecnológicos.

Propender que los servicios tecnológicos y de comunicaciones se ofrezcan con calidad, confiabilidad, confidencialidad, integridad, disponibilidad y eficiencia, optimizando y priorizando su uso para asegurar su correcta funcionalidad, brindando un nivel de seguridad óptimo que permitan:

Evitar la materialización de los riesgos identificados.
Cumplimiento legal y normativo.
Disminuir las amenazas a la seguridad de la información y los datos.
Evitar el comportamiento inescrupuloso y uso indiscriminado de los recursos.
Cuidar y proteger los recursos tecnológicos.
Concientizar a la comunidad sobre la importancia del uso racional y seguro de la infraestructura informática, sistemas de información, servicios de red y canales de comunicación.

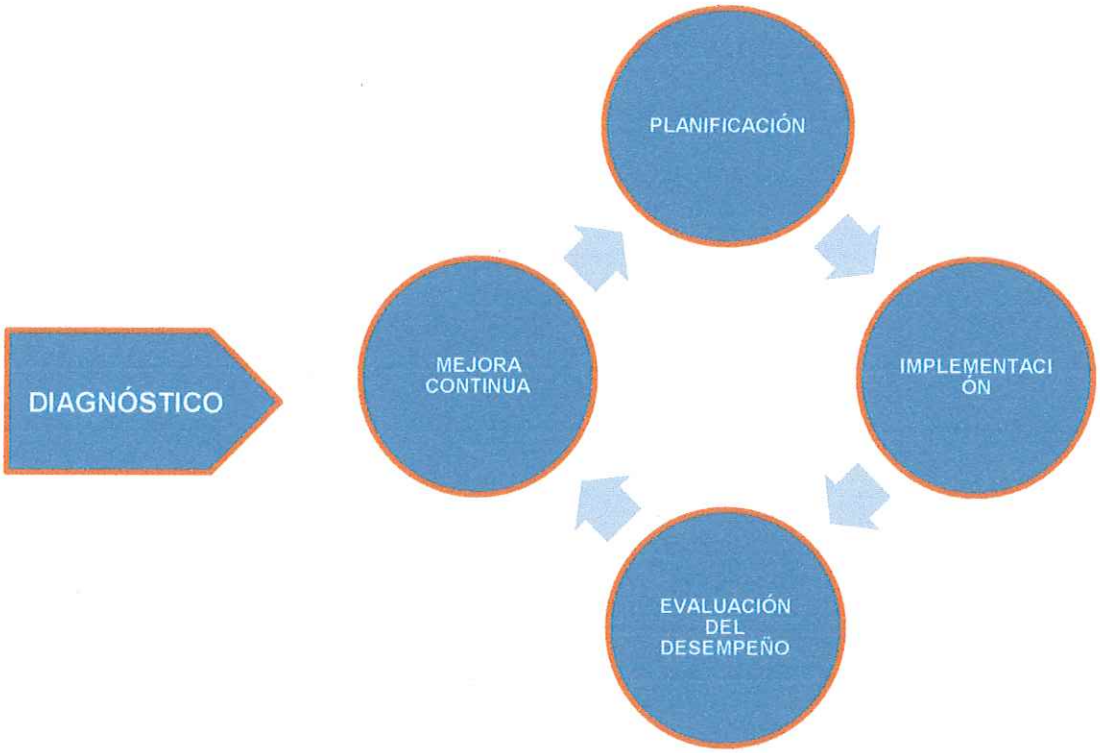
Se aplica a todos los dispositivos que hacen parte de los Servicios tecnológicos y equipos de cómputo de la entidad.

## 4. MARCO NORMATIVO

| NORMA | EPÍGRAFE |
|---|---|
| Constitución Política de Colombia de 1991, Articulo 15 | "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetar los y hacerlos respetar. De igual modo, tiene 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" |
| Ley 527 de 1999 | "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" |
| Ley 734 de 2002, Artículo 34 | "Por la cual se expide el Código Disciplinario Único". Ley 1266 de 2008. "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" |
| Ley 1273 de 2009 | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "***de la protección de la información y de los datos***" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones |
| Ley 1581 de 2012 | "***Por la cual se dictan disposiciones generales para la protección de datos personales***". |
| 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***" |
| Decreto Nacional 1078 de 2015 | "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". Título 9, Sección 2, Artículo 2.2.9.1.2.1 Componente 4 Seguridad y Privacidad de la Información |
| Decreto Nacional 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" |
| Decreto Nacional 612 de 2018 | "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado" |
| Decreto Nacional 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***" |

## 5. MARCO DE REFERENCIA

*El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información[1].*




FUENTE: MINTIC. – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la Empresa Municipal de Renovación Urbana EMRU E.I.C.

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf Pág. 20

## 6. Definiciones

**Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Confidencial:** Significa que la información no está disponible o revelada a individuos, entidades o procesos no autorizados.

**Disponibilidad de la información:** La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

**Integridad:** Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento los cuales deben ser exactos.

**Política:** Declaración de alto nivel que describe la posición de la empresa sobre un tema específico.

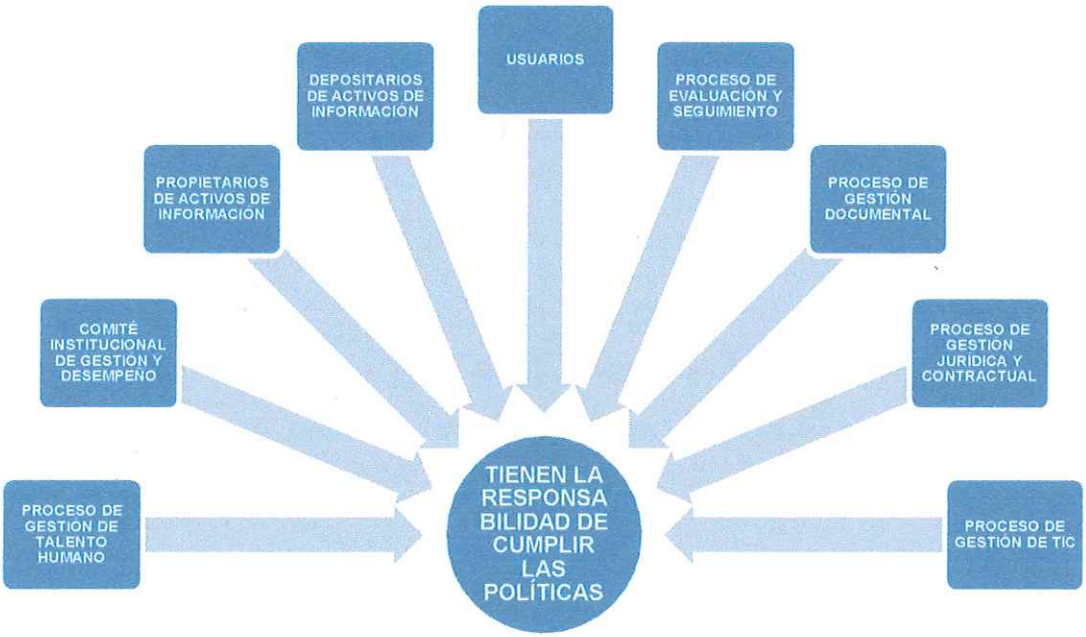
**Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la empresa en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

**Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas,

planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

## 7. Roles y Responsabilidades

Todos los Empleados Públicos, Trabajadores Oficiales, Contratistas y Grupos de Interés que hagan uso de los activos de información de la Empresa Municipal de Renovación Urbana EMRU E.I.C., tienen la responsabilidad de cumplir las políticas establecidas para el uso aceptable de los activos de información.




DIBUJO: Identificación de Responsables. Fuente Interna.

### Asignación de responsabilidades relativas a la Seguridad de la Información

**El Comité Institucional de Gestión y Desempeño:** es responsable de revisar y aprobar semestralmente las actualizaciones de la Política General de Seguridad de la Información y dará los lineamientos para la implementación del sistema de gestión de la seguridad de la información.

**Los propietarios de Activos de Información**: son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definir qué usuarios debe tener permisos de acceso a la información de acuerdo a sus funciones y competencia. Tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

**Los depositarios de Activos de Información:** son responsables de gestionar la seguridad de la misma; controlar que los permisos de acceso a la información de acuerdo a las definiciones realizadas por el propietario en el inventario de activos de información.

**El proceso de Gestión de TIC:** debe seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación almacenamiento y mantenimiento de los sistemas de información y los recursos de tecnología de la empresa. Sera el depositario del inventario de activos de información.

**El proceso de Gestión Jurídica y Contractual:** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la empresa con empleados y con terceros.

**El proceso de Gestión de Talento Humano:** cumplirá la función de notificar a todo el personal que se vincula y desvincula laboralmente a la Empresa Municipal de Renovación Urbana EMRU E.I.C., de las obligaciones respecto del cumplimiento de la política de seguridad de la información y de todos los estándares, procesos, procedimientos, prácticas y guías del sistema de gestión de la seguridad de la información. Será responsable de gestionar las capacitaciones necesarias en materia de seguridad con el apoyo y según los lineamientos dados por el Comité de Seguridad de la Información.

**El proceso de Gestión Documental:** será el responsable del manejo de la información que puede estar en diferentes tipos de medios y es conveniente que haya una persona responsable de la seguridad y gestión de esta información con el fin lograr una óptima administración y gestión de los archivos que conforman el acervo documental y registros del Modelo Integrado de Planeación y Gestión "MIPG", asegurando la actualización oportuna de los mismos y la disponibilidad para todos los involucrados de la Empresa, mediante una eficiente organización, control y consulta de los documentos, aplicando la normatividad vigente y garantizando su custodia y almacenamiento a largo plazo.

**El proceso de Evaluación y Seguimiento:** es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información y de la implementación del modelo de seguridad se seguridad y privacidad de la información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la

información establecidas por esta Política.

**Los Usuarios de la información y de los sistemas utilizados para su procesamiento:** son responsables de conocer y cumplir la Política de Seguridad de la Información vigente al igual que mantener la seguridad de la información institucional generada en el lugar de trabajo y en su entorno.

## 8. Nivel de Cumplimiento

Los trabajadores oficiales, Contratistas y Grupos de Interés, deben cumplir el 100% de la política, para lo cual deben velar por el cumplimiento de los siguientes principios:

- ✓ Operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores de la empresa.
- ✓ Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- ✓ Proteger la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ Proteger la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes).
- ✓ Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ Implementar el control de acceso a la información, sistemas y recursos de red.
- ✓ Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- ✓ Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- ✓ Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- ✓ Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

## 9. Políticas de dispositivos móviles

Se debe llevar un registro y control de todos los dispositivos móviles que posee la Entidad.

Se debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.

Se debe definir un formato o acta de salida de dispositivos.

Todos los dispositivos móviles propiedad de la Empresa Municipal de Renovación Urbana EMRU E.I.C., pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

El contratista responsable del dispositivo móvil debe hacer periódicamente copias de respaldo.

Todos usuarios son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.

La EMRU EIC cuenta con una red móvil EMRU –Invitados para los usuarios que ingresen a la entidad y previa login con la contraseña asignada por el encargado de los sistemas tecnológicos.

## 10. Seguridad de los recursos humanos

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación de Colaboradores de la Empresa Municipal de Renovación Urbana EMRU E.I.C.

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo con la reglamentación.

Se deben aplicar los controles establecidos por la entidad para otorgar el acceso a la información confidencial o reservada por parte del personal que resulte vinculado a la Entidad.

El área de jurídico (contratación) son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Todos los contratistas y personal de planta de la entidad deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información.

Todos los Colaboradores y Terceros, durante el proceso de vinculación con la EMRU E.I.C., deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Todos los Colaboradores y Terceros que hacen parte de la EMRU E.I.C., deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y directrices de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

## 11. Política de uso de correo electrónico

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en la EMRU E.I.C., y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de Ministerio.

Todos los Colaboradores y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con la EMRU E.I.C. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de la entidad y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Cuando un Proceso, Oficina, Área o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través del área de Comunicaciones de la entidad o el medio formal autorizado para realizar esta actividad.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el área de Sistemas y de Tecnologías de la Información y las Comunicaciones con previa autorización del supervisor del contrato dela persona contratada, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

El servicio de correo electrónico cuenta con respaldo de información (Back up) de diferentes procesos aplicados de manera periódica y segura. (Proveedor de servicios Colombia Hosting).

Todos los contratistas y personal de planta son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de la entidad, para que de esta forma el Área de Sistemas y de Tecnología de la Información realicen el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus al área Tecnologías de la Información y las Comunicaciones, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la Oficina de Sistemas y de Tecnología de Información hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un Colaborador se retire de la entidad, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, el área jurídica debe notificar al área de Sistemas y de Tecnologías de Información la desactivación de la cuenta.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la EMRU E.I.C.

Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.

Las cuentas institucionales (Ejemplo: gerencia@emru.gov.co , recepción@emru.gov.co, comunicaciones@emru.gov.co , comunidad@emru.gov.co, controlinterno@emru.gov.co, presupuesto@emru.gov.co, contabilidad@emru.gov.co, administracion@emru.gov.co, planeacion@emru.gov.co y juridico@emru.gov.co ) deben tener una persona responsable que haga depuración del buzón periódicamente.

Todos los usuarios son los responsables de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Colaborador o Tercero

desconfíe del remitente de un correo electrónico debe remitir la consulta a la mesa de servicios de tecnología.

Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Sistemas y de Tecnologías de la Información y Comunicaciones actuará según sea el caso.

La Oficina de Sistemas y Tecnología de Información se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.

Ningún colaborador o tercero debe suscribirse en boletines en líneas, publicidad, redes social personales, o que no tenga que ver con sus actividades laborales, con el correo institucional.

El funcionario, colaborar o tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ganancias ocasionales, premios, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a la Oficina de Sistemas y Tecnologías de la Información y las Comunicaciones, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de la entidad.

## Usos no aceptables del servicio

Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido por la EMRU E.I.C.

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena del mensajes o publicidad.

Envío o intercambio del mensaje con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio del mensaje que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió del mensaje que contengan amenazas o mensajes violentos.

Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.

Divulgación no autorizada de información propiedad de la EMRU E.I.C.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Enviar correos masivos, con excepción de con nivel de director o superior, quienes sean previamente autorizados por estos para ello, o de que en calidad de sus funciones amerite la excepción.

El correo de recepcion@emru.gov.co es el único correo institucional autorizado para enviar oficios que se han codificado con las T.R.D. y se han radicado baja un consecutivo de entrada.

## 12. Política de uso de internet

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en la EMRU E.I.C., y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de la EMRU E.I.C.
Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red de la EMRU E.I.C., es el instalado por el Área de Sistemas y de Tecnología de Información, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos en la red de la entidad, previa solicitud autorizada por el Área de Sistemas y de Tecnologías de la Información y las Comunicaciones.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de la EMRU E.I.C.

La Empresa Municipal de renovación Urbana EMRU E.I.C., se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los y colaboradores y tercero de la entidad no deben asumir en nombre de la entidad, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la entidad.

### Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite. (bajar el ancho de banda del operador de EMCALI)

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de la EMRU E.I.C., y las emitidas por los entes de control.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

## 13. Política de uso de redes sociales

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la EMRU E.IC.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con la EMRU E.I.C.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet de la entidad, o aprovechar el acceso a Redes Sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los colaboradores y terceros de la entidad, deben seguir los procedimientos y planes de comunicaciones interna y externa.

## 14. Política de uso de recursos tecnológicos

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, cambio de contraseñas, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por la Oficina de Sistemas y de Tecnologías de la Información y las Comunicaciones.
Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud al área de Sistemas y de Tecnología, la cual respaldará la información y documentos que se consideren de las funciones asignas a su cargo.

El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de estos.

En caso de que un equipo de cómputo presente un mal funcionamiento, el usuario responsable por el equipo de cómputo deberá reportarlo de inmediato a través del Área de Sistemas y de Tecnología. El Área de Sistemas y de Tecnología hará una evaluación del equipo para determinar el tipo de daño y la reparación que se requiere.

## Telefonía y dispositivos móviles

Se considera "usuarios de dispositivos móviles" a quienes por las características de sus funciones asignadas dentro de la entidad utilizan habitualmente un portátil, Smartphone, teléfono móvil, tableta, etc. dentro y fuera de la organización.

Los teléfonos móviles de la entidad se deben utilizar exclusivamente para desempeñar funciones asignadas al cargo dentro de la entidad. La entidad se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del mismo.

### Uso del Software legal y Derechos de Autor

Los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por la EMRU E.I.C.

En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software; debido a que está atentando contra los derechos de autor.

En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información.

Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por la entidad, para su distribución.

### Acceso Inalámbrico

El uso de la red inalámbrica será exclusivo para usuarios de planta y contratistas con vínculo directo con la entidad, se habilitará el servicio previa solicitud, justificación y autorización del Área de Sistemas y Tecnología. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación al Área de Sistemas y Tecnología.

## 15. Control de Acceso a Redes y Servicios en Red

Los roles y perfiles de usuarios de Redes se encuentran definidos por el Área de sistemas y de Tecnología. La entidad suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Toda actividad que requiera acceder a los servidores, equipos o a las redes de la entidad, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización del Área de Sistemas y de Tecnología de Información.

## 16. Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 90 días. Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de servicios.

Se debe mantener un registro de las 2 últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

## 17. Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar, el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes al proceso. Se comunica al Área de Sistemas y de Tecnología de Información sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

## 18. Ubicación y Protección de los equipos

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

## 19. Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

## 20. Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado de la EMRU E.I.C., sin una autorización formal.

Se debe realizar periódicamente comprobaciones puntuales para detectar el retiro no autorizado de activos de la EMRU E.I.C.

## 21. Política de Backup

Se debe realizar periódicamente un análisis de las necesidades de la entidad y de sus procesos para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.

El Área de Sistemas y de Tecnología de Información y el responsable de Seguridad de la Información junto a los propietarios de la información deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad.

Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y disponibilidad de la información.

Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.

## 22. Política de gestión de incidentes de seguridad de la información

Todos los contratistas y personal de planta tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

| Revisado por: | Aprobado por: |
|---|---|
| Lucero Messa Naranjo | Nelson Noel Londoño Pinto |
| Cargo: | Cargo: |
| Profesional Universitario Administrativo y Financiero | Gerente EMRU EIC |
| Fecha: 16 / 04 / 2019 | Fecha: 16 / 04 / 2019 |