EMPRESA DE
RENOVACIÓN Y DESARROLLO
URBANO DE BOGOTÁ
Transformamos ciudad

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ D.C.

SUBGERENCIA DE GESTIÓN CORPORATIVA

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OCTUBRE DE 2018

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	17/10/2018	Documento original

ELABORADO POR:	REVISADO POR:	REVISADO Y APROBADO POR:
Holman Eduardo Barrera Espitia Gestor Junior 3 Subgerencia de Gestión Corporativa		
Deira Galindo Contratista Subgerencia de Gestión Corporativa	Esperanza Peña Quintero Contratista Subgerencia de Planeación y Administración de Proyectos	Gemma Edith Lozano Ramírez Subgerente de Gestión Corporativa

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la Empresa de Renovación y Desarrollo Urbano de Bogotá D.C. en adelante ERU, es fundamental prestar servicios con calidad y transparencia, protegiendo preservando y administrando la integridad, confidencialidad y disponibilidad de la información en el marco de la operación de sus procesos y en cumplimiento de los requisitos legales y reglamentarios.

1. Objetivo

Brindar mecanismos de aseguramiento de los activos de información, mediante la prevención de incidentes de seguridad de la información, a través de gestión de riesgos e implementación de mecanismos de seguridad físicos y lógicos, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información.

2. Objetivos Específicos

a. Minimizar el riesgo de los procesos de la Empresa.
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 Seguridad de la Información.
g. Proteger los activos de información.
h. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
i. Fortalecer la cultura de seguridad de la información en la Empresa.
j. Garantizar la continuidad del negocio frente a incidentes.

3. Marco Normativo

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 respetarlos 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".

4. 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).

5. Alcance

Esta política aplica a toda la Empresa de Renovación y Desarrollo Urbano de Bogotá, sus funcionarios, contratistas y demás partes interesadas que intervienen en el cumplimiento de su misión y visión.

6. 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, tienen la responsabilidad de cumplir las políticas establecidas para el uso aceptable de los activos de información.

6.1 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 ERU, 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 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.

7. Nivel de Cumplimiento

Los Empleados Públicos, 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), o como resultado de un servicio interno en outsourcing.

- 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.

El no dar cumplimiento a la política de Seguridad y Privacidad de la Información, puede poner en riesgo la continuidad de la misión institucional y traerá consigo las consecuencias legales que apliquen a la normativa de la Empresa, incluyendo lo establecido en el numeral 43 Código Único Disciplinario Ley 734 de 2002.

8. Revisión

La política de Seguridad de la Información será revisada por lo menos una vez al año, o antes si existen modificaciones que así lo requieran, para garantizar que sigue siendo oportuna, suficiente y eficaz. Este proceso será liderado por la Subgerencia de Gestión Corporativa – Proceso de Gestión de TIC, y revisados y aprobados por el Comité Institucional de Gestión y Desempeño.