PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
2023

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE MANIZALES S.A.S – ERUM S.A.S.

Manizales, Centro Administrativo Municipal CAM
Calle 19 #21 - 44 Torre A pisos 7 y 13
Tels: (+57) 6 8722053• (+57) 6 8720538 • (+57) 6 8720630
contacto@erum.gov.co • www.erum.gov.co

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno.

Lo anterior dando cumplimiento al artículo primero del Decreto 612 del 2018 cuyo tenor literal manifiesta la integración de los planes institucionales y estratégicos al Plan de Acción de la ERUM S.A.S. vigencia 2023.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S con el propósito de proteger la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

Como es conocimiento de todos las nuevas Tecnologías de la Información y las Comunicaciones han generado un gran impacto en el ámbito Nacional y especialmente en el desarrollo de las entidades públicas, por consiguiente, se ha integrado con los diversos Sistemas de Gestión tanto de procesos internos como externos en pro del cumplimiento de nuestros diversos objetivos como Entidad industrial y comercial del estado.

Siguiendo las directrices del Marco de Referencia de Arquitectura Empresarial para la Gestión T.I. del Estado colombiano, el Plan de Seguridad y Privacidad de la información PSPI en su versión 01, se convertirá en una herramienta fundamental para la toma de decisiones en la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S siendo el resultado de un adecuado ejercicio de planeación estratégica de TI, Gobierno TI.

Con la integración de las TIC en todas las Dependencias y áreas de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, se da cumplimiento a todos nuestros objetivos mediante la integración y apoyo misional – transversal de los procesos y sus actores,

siendo la continua lucha contra la corrupción, aumento del nivel de protección y acceso a las herramientas informáticas, adquisición de tecnología acorde a nuestras necesidades, sistematización de los datos, optimización de recursos, entre otros aspectos; a través de metas a corto, mediano y largo plazo.

DEFINICIONES

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **Política para la gestión del riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer las políticas para garantizar la administración, manejo y control de la seguridad y privacidad de la información de la de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

1.2 OBJETIVO ESPECÍFICOS:

- Establecer y ejecutar acciones para la aplicación de los Planes de Tratamiento del Riesgo de Seguridad con el fin de minimizar el nivel de exposición de amenazas cibernéticas preservando la confidencialidad, integridad y disponibilidad de la información en la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S.

- Establecer políticas de seguridad y privacidad de la información de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

- Reducir la probabilidad materialización de un incidente de Seguridad de la Información en la infraestructura tecnológica de la ERUM S.A.S.

- Identificar los niveles de cumplimiento y alcance de las políticas de seguridad y privacidad de la información.

- Asignar roles y responsabilidades para garantizar la seguridad y privacidad de la información.

1.3 ALCANCE

La Gestión de Riesgos de Seguridad de la Información y sus Planes de Tratamiento aplica a todos los procesos donde se (crea, almacena y transfiere) información propiedad de la Entidad permitiendo garantizar la confidencialidad, integridad y disponibilidad de la información que emite la Empresa de Renovación y Desarrollo Urbana de Manizales, por lo tanto aplica a sus funcionarios, contratistas, terceros y la ciudadanía en general.

2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y

publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La ERUM S.A.S., se compromete a mantener una cultura de la gestión del riesgo asociada con la responsabilidad de diseñar, adoptar y promover las políticas, planes y programas donde se regulen los riesgos de los procesos mediante mecanismos enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia dando respuesta oportuna a los riesgos de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de estos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de la ERUM S.A.S.

Para llevar a cabo el plan de manera adecuada se deben tener en cuenta las siguientes opciones:

- **Evitar:** el acceso a personal no autorizado a los lugares donde se almacena la información física y digital de la entidad evitando así la perdida de documentación se prohíbe el ingreso a un área.
- **Prevenir:** planear estrategias adecuadas a que la perdida de información no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones y el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos de archivo de la información.
- **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal y tecnológico de acceso mantener copias de respaldo.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)1, ***"(…) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados"(…).***

La ERUM S.A.S para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, éstos últimos

correspondientes a:

a) Mitigar los riesgos de la entidad.
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 los funcionarios y clientes externos del Alcaldía municipal de Viterbo.
j) Garantizar la continuidad del servicio frente a incidentes.

2.2 NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.

A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información amparado en objetivos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que leaplican a su naturaleza; ellos son:

a) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
b) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
c) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, 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.

d) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, protege su información de las amenazas originadas porparte del personal.
e) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
f) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
g) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, implementa controles de acceso a la información, sistemas y recursos de red.
h) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
i) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, garantiza 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.
j) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basado en el impacto que pueden generar loseventos.
k) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, garantizará el cumplimiento de las obligaciones legales,regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

3. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1 JUSTIFICACIÓN

l) La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S con el propósito de proteger la información de la entidaden todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización

de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad**: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
b) **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacciónpara luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
c) **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
d) **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
e) **Confiabilidad de la Información**: es decir, que la información generada sea adecuadapara sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) **Información**: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
b) **Sistema de Información**: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
c) **Tecnología de la Información**: se refiere al hardware y software operados por la entidad

o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

3.2 OBJETIVO DE LA IMPLEMENTACIÓN DE LA POLÍTICA

Definir los mecanismos y todas las medidas necesarias por parte de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

3.3 ALCANCE

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, a sus recursos, procesos y procedimientos, tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

3.4 ROLES Y RESPONSABILIDADES

Es responsabilidad del Comité de Seguridad de la Información de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

El Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

a) El Secretario General
b) El Ingeniero de Sistemas o quien haga sus veces

c) El Jefe de Control Interno
d) El Subgerente Administrativo y Financiero
e) El Director de Gestión Humana y Organizacional

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la Alta dirección para su análisis y respectiva **aprobación**.

3.5 CUMPLIMIENTO

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S se reserva el derecho de tomar las medidas correspondientes.

3.6 COMUNICACIÓN

Mediante socialización a todos los funcionarios de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberáinformar a los contratistas y/o terceros en el momento que se requiera con el propósito derealizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Modelo Integrado de Planeación y Gestión MIPG para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página dela entidad www.erum.gov.co Menú "**Transparencia**" opción "**Modelo Integrado de Planeación y Gestión MIPG**" o en el siguiente enlace web: https://www.erum.gov.co/index.php/politicas-lineamientos-y-manuales.

3.7 MONITOREO

3.8

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

4. DESCRIPCIÓN DE LAS POLÍTICAS

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principalactivo de la entidad para el desarrollo de todas sus actividades, por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

4.1 GESTIÓN DE ACTIVOS

4.1.1 Política para la identificación, clasificación y control de activos de información

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S a través del Comité de Seguridad de la Información realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario debenestablecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área o dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El facilitador del proceso de Gestión de Recursos Físicos con apoyo del Ingeniero de sistemas o quien haga sus veces tienen la responsabilidad de mantener el inventario completo y actualizado de losrecursos de hardware y software de la entidad.

Pautas para tener en cuenta

Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

a) La información física y digital de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S debe tener un periodode almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdoa la disposición final definida por la entidad.
b) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen y saquen copias: verificar las áreas adyacentes a impresoras, escáneres y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.
c) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
d) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

4.2 CONTROL DE ACCESO

4.2.1 Política de acceso a redes y recursos de red.

El técnico operativo o ingeniero de sistemas o quien haga sus veces de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados através de mecanismos de control de acceso lógico.

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas de la Alcaldía Municipal cuenten con métodos de autenticación que evite accesos no autorizados.

   El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de éstos.

b) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de confidencialidad firmado previamente.

c) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

4.2.2 Política de administración de acceso de usuarios.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S establecerá privilegios para el control de acceso lógico decada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre

otros.

b) El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC, las solicitudes de accesoa dichos recursos de acuerdo con los perfiles establecidos

d) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

4.2.3 Política de control de acceso a sistemas de información y aplicativos.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que éstos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Notas para tener en cuenta

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
c) El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.
d) El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
e) El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

f) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
g) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de diseño e implementación.

4.2.4 Políticas de seguridad física.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

Notas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.
b) El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
c) La Gerencia General debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.

La Gerencia y la Alta Directiva de la ERUM S.A.S debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones dela entidad.

d) Los ingresos y egresos de personal a las instalaciones de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente conlos controles físicos implantados.
e) Los funcionarios deben portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S; en caso de pérdida del carnet, deben reportarlo a la mayor brevedad posible.
f) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

4.2.5 Política de seguridad para los equipos.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Notas para tener en cuenta

a) El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S.
b) El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de las plataformas tecnológicas de la entidad, redes de datos, equipos de cómputo y demás dispositivos disponibles al servicio de la entidad.
c) El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos decómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.
d) El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.
e) El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
f) El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.
g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de La ERUM S.A.S cuente con la autorización documentada y aprobada previamente por el área de sistemas.
h) El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.
i) El proceso Gestión de TIC es la única área autorizada para realizar movimientos y

asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de La ERUM S.A.S.

j) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la ERUM S.A.S, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por el personal autorizado o de apoyo al proceso de Gestión de TIC.

m) Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados o desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

p) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al Jefe inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

q) Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

4.2.6 Política de uso adecuado de internet.

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios paraasegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Notas para tener en cuenta.

a) El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
b) El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c) El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
d) El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
e) El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
f) Los usuarios del servicio de Internet de La ERUM S.A.S deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
i) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
j) No está permitido el intercambio no autorizado de información de propiedad de La ERUM S.A.S, por parte de los funcionarios con terceros.

5. PRIVACIDAD Y CONFIDENCIALIDAD

5.1 POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S a través del Comité de Seguridad de la Información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales La ERUM S.A.S, como responsable de los datos personales obtenidos a través de sus distintoscanales de atención, tratará la información de todas las personas que, en algún momento,por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales.

En caso de delegar a un tercero el tratamiento de datos personales, La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos,velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Notas para tener en cuenta

a) Las Unidades de Gestión (oficinas, dependencias y sedes administrativas de la ERUM S.A.S) que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular,suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos

datos personales.

d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
f) El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S de los cuales reciba y administre información.
g) El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
i) Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.
j) Los usuarios de los portales de La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

5.2 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, ha decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

5.2.1 Política de continuidad, contingencia y recuperación de la información

La Empresa de Renovación y Desarrollo Urbano de Manizales S.A.S - ERUM S.A.S proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

5.3 COPIAS DE SEGURIDAD

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de La ERUM S.A.S deben ejecutar pruebas controladaspara asegurar que las copiasde seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La Oficina de ControlInterno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Notas para tener en cuenta

a) El Comité de Seguridad de la Información, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
b) El Comité de Seguridad de la Información, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres.
c) El Comité de Seguridad de la información debe realizar los análisis de impacto a la entidad

y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) El Comité de Seguridad de la información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información

e) El Comité de Seguridad de la información, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.