

**POLÍTICAS GENERALES**

**DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN**

**Y COMUNICACIONES**

**Bogotá, D.C.,**

**OCTUBRE DE 2020**

**Contenido**

[1. INTRODUCCIÓN. 4](#_Toc51767824)

[2. OBJETIVOS. 5](#_Toc51767825)

[3. ALCANCE. 5](#_Toc51767826)

[4. COMPROMISO DE LA ALTA DIRECCIÓN. 6](#_Toc51767827)

[5. REFERENCIA NORMATIVA. 6](#_Toc51767828)

[6. GLOSARIO DE TERMINOS. 8](#_Toc51767829)

[7. ROLES Y RESPONSABILIDADES. 10](#_Toc51767830)

[7.1. Comité Institucional de Gestión y Desempeño. 10](#_Toc51767831)

[7.2. Especialista de Seguridad de la Información. 10](#_Toc51767832)

[7.3. Especialista de Seguridad Informática. 11](#_Toc51767833)

[7.4. Gerentes, Jefes de Oficina, Subdirectores. 11](#_Toc51767834)

[7.5. Propietarios de los Activos de Información. 11](#_Toc51767835)

[7.6. Gestión de Servicios e Infraestructura Tecnológica. 12](#_Toc51767836)

[7.7. Gestión de Talento Humano. 13](#_Toc51767837)

[7.8. Colaboradores. 14](#_Toc51767838)

[8. POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACION 14](#_Toc51767839)

[8.1. Propósito. 14](#_Toc51767840)

[8.2. Acciones que Afectan la Seguridad de la Información. 15](#_Toc51767841)

[9. POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN. 17](#_Toc51767842)

[9.1. Política de Protección de Datos Personales. 17](#_Toc51767843)

[9.2. Políticas de Seguridad de Protección y Respaldo de Información. 18](#_Toc51767844)

[9.3. Política de Seguridad para la Gestión de Contraseñas. 18](#_Toc51767845)

[9.4. Políticas de Escritorio Limpio y Bloqueo de Pantallas. 19](#_Toc51767846)

[9.5. Política de Responsabilidades y Control de Cambios. 19](#_Toc51767847)

[9.6. Política Buen uso de Correo Institucional. 19](#_Toc51767848)

[9.7. Política de Navegación en Internet. 20](#_Toc51767849)

[9.8. Política de Seguridad para la Gestión de Log’s. 20](#_Toc51767850)

[9.9. Política de Protección contra Software Nocivo. 20](#_Toc51767851)

[9.10. Política sobre el Uso de Equipos de Cómputo y el Acceso a la Red. 21](#_Toc51767852)

[9.11. Política de Seguridad de Gestión de Activos de Información. 21](#_Toc51767853)

[9.12. Política de Seguridad para la Gestión de Riesgos. 21](#_Toc51767854)

[9.13. Política Gestión de Incidentes de Seguridad de la Información. 22](#_Toc51767855)

[10. CUMPLIMIENTO. 22](#_Toc51767856)

[11. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD 22](#_Toc51767857)

## **INTRODUCCIÓN.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, por medio de la aplicación de las políticas de seguridad de la información contenidas en este documento, permite a la entidad mitigar posibles riesgos de seguridad de la información a los cuales puede estar expuesta. Estas políticas brindan una serie de lineamientos que, al ser adoptados por cada uno de los colaboradores de la entidad, aseguran la protección adecuada de los activos de información de cada uno de los procesos.

Estas políticas de seguridad contribuyen a crear cultura organizacional, adaptando y/o adoptando las mejores prácticas en materia de seguridad de la información. Por lo anterior, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, asegura la confidencialidad, integridad y disponibilidad tanto de la infraestructura tecnológica como de la información que contiene.

Adicional, en el presente documento se manifiesta el compromiso que la Alta dirección asume, apoyando continuamente los temas relacionados en materia de seguridad de la información, y se resalta la necesidad y propósito con los cuales se deben aplicar cada uno de los lineamientos detallados en las trece (13) políticas de seguridad, estableciendo la responsabilidad que cada uno de los colaboradores de la entidad, cumple con el aseguramiento adecuado de los activos de información

Finalmente, se establece las acciones que la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, contempla por el incumplimiento de las políticas de seguridad de la información, por parte de sus colaboradores.

## **OBJETIVOS.**

* Definir los lineamientos generales que deben ser adoptados e implementados por los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que contribuyan a una adecuada gestión de la seguridad de la información preservando la confidencialidad, disponibilidad e integridad de la información, de acuerdo con los requisitos normativos que le apliquen.
* Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.
* Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todos los funcionarios, contratistas y demás personas que interactúen con la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para minimizar la ocurrencia de incidentes de Seguridad de la Información.
* Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia

## **ALCANCE.**

Aplica para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, que tengan acceso a los recursos y activos de información, en todas sus formas (digital, impresa, escrita, y hablada), durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y está orientada a preservar la confidencialidad, integridad y disponibilidad de la información de la entidad, los cuales están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de salvaguardar la información; por lo tanto, están obligados a continuar protegiendo y cumpliendo las políticas de confidencialidad durante y una vez terminada su relación laboral y/o contractual con la entidad.

## **COMPROMISO DE LA ALTA DIRECCIÓN.**

La Alta Dirección de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, se compromete a apropiar y apoyar activamente la seguridad de la información dentro de la entidad, asignando los recursos necesarios para su desarrollo, generando las herramientas necesarias y estableciendo los controles encaminados a prevenir y administrar los riesgos que puedan afectar la seguridad de la información de la entidad.

## **REFERENCIA NORMATIVA.**

* **Constitución Política de Colombia de 1991.** Artículos 15 del Habeas Data, 20 y 74 sobre acceso a la información.
* **Ley Estatutaria 1581 de 2012:** *“Por la cual se dictan disposiciones generales para la protección de datos personales”*
* **Ley Estatutaria 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 Ordinaria 1955 de 2019, artículo 148:**“*Por el cual se expide el Plan Nacional de Desarrollo 2018-2022”.* El artículo 148 de la norma citada, estableció́ que todas las Entidades deben adelantar acciones señaladas por el Gobierno Nacional, concernientes a implementar las estrategias de Gobierno en Línea que se definen por el Ministerio de Tecnologías de la Información y las comunicaciones.
* **Ley Ordinaria 1341 de 2009:** *“por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.*
* **Ley Ordinaria 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 Ordinaria 603 de 2000:** *“****Por la cual se modifica el artículo 47 de la Ley 222 de 1995”*:**Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuérdese: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.
* **Decreto Reglamentario 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.*
* **Decreto Reglamentario 103 de 2015, Compilado en el Decreto 1081 de 2015:** *“Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.*
* **Decreto Reglamentario 2573 de 2014:** *“por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.*
* **Decreto Reglamentario 1377 de 2013, Compilado en el Decreto 1074 de 2015:** Protección de datos, decreto por el cual se reglamente parcialmente la Ley 1581 de 2012. Añade dos nuevos capítulos al Código Penal Colombiano. Derogado parcialmente por el Decreto 1081 de 2015.
* **Norma Técnica Colombiana NTC-ISO-IEC 31000:2018**: Norma técnica de gestión del riesgo. Principios directrices.
* **Norma Técnica Colombiana NTC-ISO-IEC 27001:2013:**Norma técnica de sistemas de gestión de la seguridad de la información. Requisitos.
* **Norma Técnica Colombiana NTC-ISO-IEC 27002:2015:**Norma técnica de seguridad. Código de práctica para controles de seguridad de la información.

## **GLOSARIO DE TERMINOS.**

* **Activos de Información:** Cualquier elemento de información o que interactúe con ella que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone un agravio o coste. La naturaleza de los activos dependerá de la empresa, pero su protección es el fin último de la gestión de riesgos. La valoración de los activos es importante para la evaluación de la magnitud del 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 organización.
* **Ciberseguridad:** la ciberseguridad se define como una **capa de protección para los archivos de información**, a partir de ella, se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.
* **Disponibilidad:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.
* **BACKUP:** En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
* **Colaboradores:** Todos los servidores públicos, trabajadores oficiales, orden de prestación de servicios y todas las personas que se encuentren vinculadas a la Entidad y que deban generar algún trabajo para la misma.
* **Confidencialidad:** La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
* **Encargado de Seguridad:** Persona delegada cuyas funciones principales son asesorar en materia de seguridad de la información en la entidad y supervisar el cumplimiento de la presente Política.
* **No Repudio:** Capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje enviado por un origen determinado
* **Seguridad de la Información:** Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
* **Seguridad Informática:** Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar que se materialización las amenazas que se propagan por la red.
* **Riesgo**: Es la definición de un escenario bajo el cual una amenaza puede explotar una vulnerabilidad, generando un impacto negativo al negocio (por ejemplo, pérdida de la continuidad, incumplimiento, pérdida de ingresos, entre otros).
* **Tercero(s):** Cualquier persona natural o jurídica en calidad de proveedor, outsourcing o consultor.
* **Vulnerabilidad**: Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una organización.

## **ROLES Y RESPONSABILIDADES.**

# **Comité Institucional de Gestión y Desempeño.**

* Verificar el cumplimiento de la presente Directiva, en particular la difusión y adopción de las políticas, normas y estándares de Seguridad de la Información.
* Apoyar los programas de sensibilización, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con Seguridad de la Información.
* Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del Modelo de Seguridad y Privacidad de la Información.

## **Especialista de Seguridad de la Información.**

* Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados, ayudando con las cuestiones disciplinarias y legales necesarias.
* Gestionar, y/o supervisar pruebas de vulnerabilidad sobre los diferentes recursos tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
* Mantener y promover la actualización de las políticas de seguridad de la información.
* Definir las herramientas, metodologías y lineamientos necesarios para la implementación del Modelo de Seguridad y Privacidad de la Información.

## **Especialista de Seguridad Informática.**

* Configurar y mantener los activos informáticos relacionados con la gestión de la seguridad de la información, por ejemplo, equipo de firewall, sistemas de prevención de intrusos (IPS), enrutadores de frontera, sistemas de gestión y monitoreo, consola de despliegue de políticas de seguridad, etc.
* Generar los reportes de eventos de seguridad que sean solicitados por parte del Especialista de Seguridad de la Información, por ejemplo, aquellos relacionados al uso de un canal de comunicaciones, registro de accesos a recursos, entre otros.
* Realizar los ajustes necesarios sobre los sistemas de seguridad que gestione y que sean indicados por el Especialista de Seguridad de la Información a manera de control detectivo o correctivo.
* Dar cumplimiento a las disposiciones definidas para el uso de dispositivos institucionales.

## **Gerentes, Jefes de Oficina, Subdirectores.**

Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

## **Propietarios de los Activos de Información.**

* Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma.
* Documentar y mantener actualizada la clasificación efectuada•Definir los criterios de acceso a la información de acuerdo a sus funciones y competencia para sus colaboradores.
* Asegurar que los controles de alto nivel para proteger la información sean implementados.
* Tomar las acciones definidas en las políticas, código de ética y cualquier otro reglamento o control, frente a violaciones de la seguridad.
* Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.

## **Gestión de Servicios e Infraestructura Tecnológica.**

* Cumplir la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la entidad.
* Efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
* Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información.
* Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
* Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
* Diseñar estrategias que incorporen las tendencias y cambios tecnológicos que sean pertinentes con los objetivos misionales de la entidad.
* Evaluar y autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica y los sistemas de información de la entidad.
* Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
* Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
* Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los colaboradores; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software.

## **Gestión de Talento Humano.**

* Notificar al personal que ingresa a la entidad, sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
* Socializar a toda la entidad los cambios que se realicen en la política de seguridad de la información, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación permanente en materia de seguridad.
* Incluir en los programas de inducción y de re-inducción el tema de seguridad de la información asegurando que los colaboradores conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear.
* Incluir las funciones relativas a la seguridad de la información en la descripción de puestos de los colaboradores.

## **Colaboradores.**

* Cumplir con las políticas de Seguridad de la Información, contempladas en el presente documento.
* Velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato.
* Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
* Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
* Utilizar únicamente software y demás recursos tecnológicos autorizados.

## **POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN Y COMUNICACION**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, se compromete a mantener acciones y estrategias orientadas a la protección de la información como principal activo de la entidad, mediante un modelo de gestión sistemático de privacidad y seguridad digital, orientado a la administración del riesgo con el fortalecimiento de la integridad, confidencialidad y disponibilidad de la información, fomentando la cultura de seguridad en todos los niveles de la entidad, sus proveedores y la ciudadanía que demanda servicios.

## **Propósito.**

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a través del proceso Gestión de Servicios e Infraestructura Tecnológica, dando cumplimiento a sus funciones en lo referente a Seguridad y Privacidad de la Información y gestión del riesgo de seguridad digital (ciberseguridad), define la siguiente política y lineamientos de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información y seguridad digital de la estrategia de gobierno digital y el Modelo Integrado de Planeación y Gestión-MIPG, según lo establecido en el, el Decreto 1499 de 2017 y el Decreto 1008 de 2018; con esto la entidad vela por la integridad, confidencialidad y disponibilidad de la información y administra el riesgo sobre todos sus activos de información.

## **Acciones que Afectan la Seguridad de la Información.**

A continuación, se describen algunas acciones identificadas que afectan la Seguridad de la Información, y que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información:

* Dejar los computadores encendidos en horas no laborables.
* Permitir que personas ajenas a la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
* No clasificar y/o etiquetar la información.
* No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.
* No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
* Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
* Hacer uso de la red de datos de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
* Instalar software en la plataforma tecnológica de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, cuyo uso no esté autorizado por el proceso Gestión de Servicios e Infraestructura Tecnológica, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.
* Enviar información clasificada de la entidad por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
* Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.
* Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la entidad sin la debida autorización.
* Ingresar a la red de datos de entidad por cualquier servicio de acceso remoto sin la autorización del proceso de Gestión de Servicios e Infraestructura Tecnológica.
* Usar servicios de internet en los equipos de la entidad, diferente al provisto por el proceso de Gestión de Servicios e Infraestructura Tecnológica.
* Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, para beneficio personal.
* Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro colaborador.
* Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
* Retirar de las instalaciones de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.
* Entregar, enseñar o divulgar información clasificada de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, a personas o entidades no autorizadas.
* Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la entidad o de terceras partes.
* Ejecutar cualquier acción que difame, afecte la reputación o imagen de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, o alguno de sus colaboradores, utilizando para ello la plataforma tecnológica.
* Realizar cambios no autorizados en la Plataforma Tecnológica de la entidad.
* Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

## **POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN.**

Para la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, la información es su activo más preciado por cuanto constituye la pieza fundamental para el desarrollo de su gestión y la prestación de los servicios a partes interesadas y la ciudadanía en general; por este motivo la administración genera los mecanismos necesarios para lograr preservar la confidencialidad, la integridad, la disponibilidad, la accesibilidad, el no repudio y demás propiedades que permitan una adecuada gestión de la seguridad de la información. Por consiguiente, el presente documento despliega las directrices generales que dan desarrollo a la seguridad de la información:

## **Política de Protección de Datos Personales.**

Establecer los lineamientos para administración y tratamiento de datos personales en la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, de acuerdo con la Ley Estatutaria 1581 de 2012 y el Decreto número 1377 de 2013, compilado en el Decreto 1074 de 2015 en su capítulo 25 por medio del cual se reglamenta parcialmente, normas que dictan las disposiciones generales para la protección de datos personales y desarrollan el derecho constitucional de consultar, actualizar, corregir o restringir el acceso a sus datos personales que ostenta el titular de la información, de acuerdo a los artículos 15 y 20 de la Constitución Política de Colombia.

Las directrices de protección de datos personales se encuentran definidas y detalladas en el documento, ***EGTI-DI-003 Política de Protección de Datos Personales,*** publicada en el Sistema de Gestión de la Entidad.

## **Políticas de Seguridad de Protección y Respaldo de Información.**

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por entidad.

Las Directrices de protección y respaldo de Información, se encuentran definidas y detalladas en el documento ***EGTI-DI-003 Políticas de Seguridad de Protección y Respaldo de Información,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Seguridad para la Gestión de Contraseñas.**

Ningún usuario deberá acceder a la red o a los servicios TIC de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, utilizando una cuenta de usuario o clave de otro usuario.

Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó la clave.

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

Las directrices para la gestión de contraseñas, se encuentran definidas y detalladas en el documento ***EGTI-DI-004 Política de Seguridad para la Gestión de Contraseñas,*** publicada en el Sistema de Gestión de la Entidad.

## **Políticas de Escritorio Limpio y Bloqueo de Pantallas.**

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los colaboradores.

Los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Las Directrices para escritorio limpio y bloqueo de pantalla, se encuentran definidas y detalladas en el documento ***EGTI-DI-005 Políticas de Escritorio Limpio y Bloqueo de Pantallas,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Responsabilidades y Control de Cambios.**

La Administración de Cambios tiene como propósito realizar modificaciones en los ambientes de producción de la infraestructura tecnológica, rápidamente y sin interrupción de los servicios prestados, a través de métodos estandarizados, **evaluando el impacto de todos los cambios en la infraestructura de tecnológica, hardware y software.**

Las directrices para responsabilidades y control de cambios, se encuentran definidas y detalladas en el documento ***EGTI-DI-006 Política de Responsabilidades y Control de Cambios,*** publicada en el Sistema de Gestión de la Entidad.

## **Política Buen uso de Correo Institucional.**

Definir las pautas generales para asegurar una adecuada protección de la información de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, en el uso del servicio de correo electrónico por parte de los colaboradores.

Las directrices del buen uso de correo institucional se encuentran definidas y detalladas en el documento ***EGTI DI 007 Política Buen uso de Correo Institucional,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Navegación en Internet.**

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los colaboradores, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Las directrices para la navegación en internet se encuentran definidas y detalladas en el documento, ***EGTI-DI-008 Política de Navegación en Internet,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Seguridad para la Gestión de Log’s.**

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (Log’s) generados por los sistemas de información y comunicaciones de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Las Directrices para la gestión de Log’s, se encuentran definidas y detalladas en el documento ***EGTI-DI-009-V1 Política de Seguridad para la Gestión de Log’s,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Protección contra Software Nocivo.**

Asegurar la no propagación o instalación de software con código malicioso o nocivo el cual pueda comprometer la disponibilidad, integridad y confidencialidad de los servicios soportados por la Infraestructura tecnológica de la entidad.

Las directrices para la protección contra software nocivo, se encuentran definidas y detalladas en el documento ***EGTI-DI-010 Política de Protección Contra Software Nocivo,*** publicada en el Sistema de Gestión de la Entidad.

## **Política sobre el Uso de Equipos de Cómputo y el Acceso a la Red.**

Asegurar el buen uso de los equipos de cómputo asignados por la entidad a los usuarios, para el desarrollo de sus funciones, así como el uso adecuado de la red de datos, dando a conocer a los usuarios los riesgos asociados a la utilización inadecuada de estos recursos tecnológicos, situación que puede comprometer la integridad y confidencialidad de la información de la entidad.

Las directrices para el uso de los equipos de cómputo y el acceso a la red, se encuentran definidas y detalladas en el documento ***EGTI-DI-011 Política sobre el uso de equipos de cómputo y el acceso a la red,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Seguridad de Gestión de Activos de Información.**

Los activos de información pertenecen a la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

Los colaboradores deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la entidad, en el proceso de desvinculación, de igual manera deberán documentar y entregar a la entidad, los conocimientos importantes que posee de la labor que ejecutan.

Las directrices para la gestión de activos de información se encuentran definidas y detalladas en el documento, ***EGTI-DI-012 Políticas de Seguridad de Gestión de Activos de Información,*** publicada en el Sistema de Gestión de la Entidad.

## **Política de Seguridad para la Gestión de Riesgos.**

**Identificar las principales amenazas y vulnerabilidades a los que están expuestos los activos de información, permitiendo** **minimizar la materialización de los riesgos asociados infraestructura tecnológica y sistemas de información.**

**Las directrices para la gestión de riesgos se encuentran definidas y detalladas en el documento, *EGTI-DI-013 Política de Seguridad para la Gestión de Riesgos,*** publicada en el Sistema de Gestión de la Entidad.

## **Política Gestión de Incidentes de Seguridad de la Información.**

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

Las Directrices de gestión de incidentes de seguridad de la Información, se encuentran definidas y detalladas en el documento ***EGTI-DI-014 Política Gestión Incidentes de Seguridad de la Información,*** publicada en el Sistema de Gestión de la Entidad.

## **CUMPLIMIENTO.**

Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, tomará las acciones disciplinarias y legales correspondientes.

## **ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD**

Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, se reserva el derecho a modificar esta política cuando sea necesario. En todo caso, los cambios realizados en esta política serán divulgados a los colaboradores de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial.

Es responsabilidad de cada uno de los usuarios la lectura y conocimiento de las Políticas de Seguridad contempladas en este documento.

**REVISIÓN Y APROBACIÓN:**

|  |  |  |
| --- | --- | --- |
| **Elaborado y/o Actualizado por:** | **Validado por**  **Líderes (Estratégico u Operativo) del Proceso:** | **Aprobado:** |
| **LUIS ENRIQUE PARIS GARCIA /**  **GLORIA MENDEZ**  **Contratista / Proceso SIT** | Firma: | Firma: |
| **Acompañamiento Asesor OAP:** |
| **CHRISTIAN MEDINA FANDIÑO**  **Contratistas/ Proceso SIG** |
| **MARTHA PATRICIA GUILAR COPETE**  **(Secretaria General)** | **DIANA MARCELA DEL PILAR REYES TOLEDO**  **(Representante de la Alta Dirección)** |

**CONTROL DE CAMBIOS:**

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **DESCRIPCIÓN** | **FECHA** | **APROBADO**  **Representante de la Alta Dirección** |
| 1.0 | Elaborado por MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas: Actualización de la Resolución 558 del 14 de diciembre de 2007 y a las Normas ISO/IEC 17799: 2005, ISO/IEC 27001 | Diciembre de 2007 | Comité de Gestión Integral |
| 1.01 | Revisión no documentada en el Sistema de Gestión de Calidad:  MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas | Enero de 2008 | Proceso SIT |
| 1.02 | Revisión no documentada en el Sistema de Gestión de Calidad: MARISOL LONDOÑO LOPEZ – Profesional Especializada Sistemas. | Marzo de 2009 | Proceso SIT |
| 1.03 | Revisión no documentada en el Sistema de Gestión de Calidad:  JOSE GABRIEL GUERRA – Profesional Universitario Sistemas | Marzo de 2010 | Proceso SIT |
| 1.04 | Revisión no documentada en el Sistema de Gestión de Calidad: JOSE GABRIEL GUERRA – Profesional Universitario SIT / PAOLA MONTENEGRO - Contratista | Agosto de 2011 | Proceso SIT |
| 1.05 | Revisión no documentada en el Sistema de Gestión de Calidad: JUAN CARLOS ALBA ALBARRACÍN – Profesional Especializado SIT / JOSE GABRIEL GUERRA – Profesional Universitario SIT | Febrero de 2013 | Proceso SIT |
| 2.0 | Revisado con el Acompañamiento OAP: Se actualiza a la normatividad vigente Normas NTC-ISO/IEC 27002, ISO/IEC 27001. Por: JUAN CARLOS ALBA ALBARRACÍN – Profesional Especializado SIT / JOSE GABRIEL GUERRA – Profesional Universitario SIT | Febrero 2015 | JEFE OAP |
| 3 | Revisado y actualizado por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), se desagregaron las políticas puntuales de la POLITICA GENERAL DE TECNOLOGIA Y SEGURIDAD DE LA INFORMACION Y COMUNICACIONES, se agregó introducción, se modificó el objetivo general, se agregaron los objetivos específicos, se realizó modificación del alcance, la introducción. | Diciembre  2018 | Jefe Oficina Asesora de Planeación |
| 4 | Se incorporan roles y responsabilidades específicos, se modifican objetivos y propósitos, se incorporan acciones que afectan la seguridad de la información, se incorporan políticas específicas, se incorpora normatividad. | Octubre 2020 | Jefe Oficina Asesora de Planeación |