La movilidad es de todos

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE - UPIT

RESOLUCIÓN NÚMERO 045 DEL 24 DE MARZO DEL 2022

"Por medio de la cual se adopta la política de seguridad digital y privacidad de la información y se definen lineamientos frente al uso y manejo de la información de la Unidad de Planeación de Infraestructura de Transporte – UPIT'

LA DIRECTORA GENERAL (E) DE LA UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE –UPIT

En ejercicio de sus facultades legales y reglamentarias, en especial las consagradas en el Decreto 946 de 2014, y

CONSIDERANDO:

Que el artículo 74 de la Constitución Política de Colombia establece el derecho de todas las personas a acceder a los documentos públicos salvo los casos que establezca la Ley.

Que, la Ley 1712 de 2014 crea la ley de transparencia y del derecho de acceso a la información pública nacional, tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

Que, el Documento CONPES 3854 de 2016 establece la política nacional de seguridad digital, en la cual se aborda la seguridad digital desde el enfoque de gestión del riesgo, siendo el objetivo principal de la política: *"fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.'*

Que, el Decreto 1008 de 2018 '*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*', establece los lineamientos generales de la Política de Gobierno Digital para Colombia, y sustituye a la Estrategia de Gobierno en Línea, señala en su artículo 2.2.9.1.1.1 que la política debe ser entendida como: *"el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.'*

Que el precitado Decreto 1008 de 2018 establece igualmente los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

Que el Decreto 1499 de 2017 modificatorio del Decreto 1083 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de la Función Pública'*, adoptó el Modelo Integrado de Planeación y Gestión – MIPG, definiéndolo en su artículo 2.2.22.3.2 como 'un marco de referencia para dirigir ,planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y orga-

nismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio'

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015, sustituido por el artículo 1º del Decreto 1499 de 2017, regula las Políticas de Gestión y Desempeño Institucional entre ellas las correspondientes a Gobierno Digital y Seguridad Digital.

Que el Decreto 338 de 2022 adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, estableciendo los lineamientos generales para fortalecer la gobernanza de la seguridad digital, y crea el Modelo y las instancias de Gobernanza de Seguridad Digital.

Que para lograr el objetivo indicado se proponen acciones en los siguientes ejes estratégicos: la creación de un marco estratégico institucional claro frente a la seguridad digital, creación de las condiciones para que las partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas para generar confianza en el uso del entorno digital, el fortalecimiento de la defensa y seguridad nacional en el entorno digital nacional y transnacional y la generación de mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Que, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, a través la Resolución No. 000448 de 2022, actualiza la *"Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, y define lineamientos frente al uso y manejo de la información'*.

Que la Guía No.2, del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC (2016) *"Elaboración de la política general de seguridad y privacidad de la información'*, es un documento base elaborado por dicha Cartera dirigido a las entidades de orden nacional, territorial y privadas que buscan adoptar el Modelo de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital para Colombia, siendo un importante insumo para la formulación de la política general de seguridad de la información de la UPIT.

Que, en el artículo 5 del Decreto 946 de 2014 *"Por el cual se crea la Unidad de Planeación de Infraestructura de Transporte y se determina su estructura y funciones'*, señala que es función de la entidad, *"...10. Consolidar, unificar, actualizar y divulgar, de manera sistematizada, la información de los proyectos de infraestructura de transporte y el registro de los operadores del sector, en los términos que establezca la Unidad.'*

Que, según lo determinado en el Artículo 16 de la referida norma estatutaria son funciones de la Secretaría General de la Unidad entre otras: *"1. Asesorar a la Dirección General en la formulación de políticas, planes y programas, en lo referente al desarrollo del talento humano y la administración de los recursos financieros, económicos y físicos de la Unidad.'*, *"4. Dirigir, coordinar, controlar y evaluar las actividades relacionadas con la adquisición, almacenamiento, custodia, distribución e inventario de los elementos, equipos y demás bienes y servicios necesarios para el funcionamiento de la Unidad, velando para que se cumplan las normas vigentes sobre la materia.'* y *"9. Dirigir la identificación, el diseño y la implementación de soluciones tecnológicas acordes con las necesidades de la entidad y velar por la operación, funcionalidad y seguridad de la información sistematizada.'*

La movilidad es de todos

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE - UPIT

RESOLUCIÓN NÚMERO 045 DEL 24 DE MARZO DEL 2022

"Por medio de la cual se adopta la política de seguridad digital y privacidad de la información y se definen lineamientos frente al uso y manejo de la información de la Unidad de Planeación de Infraestructura de Transporte – UPIT'

Que, el Decreto 946 de 2014 asigna a la Oficina de Gestión de Información de la Unidad de Planeación de Infraestructura de Transporte, en su Artículo 12 la función de *"1. Asesorar a la Dirección en la recomendación de políticas, planes, programas y proyectos relacionados con el proceso de captura, procesamiento y manejo de la información de la infraestructura de transporte, que sirvan de insumo para el proceso de planificación y seguimiento al desarrollo de dicha infraestructura y la formulación de políticas públicas de transporte de corto, mediano y largo plazo.'*

Que la protección de la información busca la disminución del impacto generado sobre los activos de información de las entidades pública, a saber: funcionarios, contratistas, terceros, la información estratégica, legal, financiera, contractual; los procesos y procedimientos, las tecnologías de información, el hardware y el software, siendo objetivo primordial mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información.

Que en ese sentido, la Unidad de Planeación de Infraestructura de Transporte UPIT adoptará medidas técnicas, administrativas y operativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos de seguridad digital, y la gestión de respuesta a incidentes de seguridad digital, conforme los lineamientos del Modelo de Gobernanza de Seguridad Digital, definidos en el Decreto 338 de 2022, aplicando sus objetivos, principios y niveles, garantizando la protección de sus redes, su infraestructura tecnológica y sus sistemas de información.

Que, en virtud de lo anterior, se hace necesario adoptar e implementar la política de seguridad digital y privacidad de la información de la entidad, que permita establecer un marco de confianza en el ejercicio de sus deberes frente a otras instancias públicas y la ciudadanía en general, en estricto cumplimiento de las normas que rigen la materia, y acorde con la misión y visión que le señala el Decreto 946 de 2014.

Que, en mérito de lo expuesto,

RESUELVE:

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1. Objeto. Adoptar la política de seguridad digital y privacidad de la información de la Unidad de Planeación de Infraestructura de Transporte UPIT, la cual se constituye en la visión para afrontar los riesgos de la entidad en la gestión de la información, y las medidas de seguridad y protección que va a emprender para asegurar su disponibilidad, integridad y confidencialidad de la información misional.

ARTÍCULO 2. Ámbito de aplicación La política de seguridad digital y privacidad de la información aplica a toda la Unidad de Planeación de la Infraestructura de Transporte, sus funcionarios, contratistas y terceros y todos aquellos que tengan una relación con la entidad, a través de procesos de recolección, procesamiento, almacenamiento, recuperación, intercambio, y consulta de información. Todas las personas cubiertas por el alcance deberán dar cumplimiento al 100% de la política.

Esta política aplica a toda la información creada, procesada o usada por la Unidad de Planeación de Infraestructura de Transporte, independiente del medio, formato, presentación o lugar en el cual se encuentre.

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE - UPIT

RESOLUCIÓN NÚMERO 045 DEL 24 DE MARZO DEL 2022

"Por medio de la cual se adopta la política de seguridad digital y privacidad de la información y se definen lineamientos frente al uso y manejo de la información de la Unidad de Planeación de Infraestructura de Transporte – UPIT'

ARTÍCULO 3. Objetivos generales. Establecer los siguientes objetivos generales de la Política de Seguridad Digital y Privacidad de la Información de la Unidad de Planeación de Infraestructura de Transporte UPIT:

1. Minimizar el riesgo de vulnerabilidad en la seguridad de la información, en la ejecución de las funciones misionales de la entidad.
2. Cumplir con los principios de seguridad de la información: disponibilidad, integridad, y confidencialidad de la información.
3. Definir, formular y formalizar los elementos normativos sobre los temas de protección de la información.
4. Mantener la confianza de los ciudadanos, los empleados, los operadores del sector transporte, terceros y entidades de gobierno.
5. Apoyar la innovación tecnológica.
6. Proteger los activos tecnológicos.
7. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
8. Establecer los procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, operadores, socios, contratistas de la UPIT.
10. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.
11. Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a la misión de la entidad, y a los requerimientos normativos y regulatorios.

ARTÍCULO 4. Principios. Establecer los siguientes principios que guiarán la actuación de la UPIT para la seguridad y la privacidad de la información:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores públicos, contratistas, proveedores, socios o terceros.
2. La UPIT protegerá la información generada, procesada o resguardada por sus procesos misionales, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros o como resultado de un servicio interno en outsourcing.
3. La UPIT protegerá la información creada, procesada, transmitida o resguardada por sus procesos misionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello se establecerán controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. La UPIT protegerá su información de las amenazas originadas por parte del personal.
5. La UPIT protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos misionales.
6. La UPIT controlará la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. La UPIT implementará control de acceso a la información, sistemas y recursos de red.
8. La UPIT garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

CAPÍTULO II
POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 5. Política de acceso a la información. La UPIT garantizará la disponibilidad al público de la información de su competencia, a través de medios físicos, remotos, o locales de comunicación electrónica y a través de la web, así como prestar apoyo a los usuarios de la información que requieran asistencia para la consulta o descargue de datos.

ARTÍCULO 6. Política de seguridad física y del entorno. La política de seguridad física y del entorno de la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe señalizar las áreas seguras de acuerdo con el levantamiento del inventario de áreas seguras.
2. Las puertas y ventanas de las áreas seguras deben permanecer cerradas y bloqueadas cuando no haya supervisión o estén desocupadas.
3. Todos los puntos de acceso deben tener un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o instalación.
4. la Secretaría General de la UPIT debe establecer un sistema de control de acceso a las instalaciones de la entidad, así como a las áreas seguras y se debe documentar mediante un procedimiento, manual o guía.
5. El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. que ingresen los Servidores Públicos y Contratistas o visitantes.
6. El personal de vigilancia debe registra en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo elemento informático (pc o portátil, ratón, teclado, cargador, etc.), servidores, equipos activos de red o cualquier equipo electrónico diferentes a smartphone; en caso de que estos equipos sean propiedad de la UPIT deberán contar con autorización expresa de la Secretaría General de la UPIT en un formato de orden de salida de elementos que se diseñe para tales fines.
7. La Secretaría General y la Oficina de Gestión de la Información de la UPIT, deben controlar el ingreso a los centros de datos y centros de cableado de la entidad.
8. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben controlar el ingreso a personal ajeno a la UPIT a los centros de datos y centros de cableado, este debe estar acompañado por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno a la entidad durante el tiempo que permanezca en las instalaciones.
9. La Secretaría General de la UPIT es responsable de la identificación y organización del cableado estructurado desde los puestos de trabajo hasta los paneles de conexión (patch panel) de los centros de cableado.
10. La Secretaría General en acompañamiento de otras áreas de la UPIT debe garantizar y generar los controles para la protección de la infraestructura tecnológica y virtual ante amenazas externas y ambientales.
11. La Secretaría General de la UPIT 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.

ARTÍCULO 7. Política de Seguridad de las Operaciones. La política de seguridad de las operaciones de la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
2. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.
3. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada
4. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben velar por la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.
5. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben realizar las tareas de optimización de servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad.
6. La Oficina de Gestión de Información de la UPIT debe definir y documentar las reglas para la transferencia de software del ambiente de pruebas a producción.
7. La Oficina de Gestión de la Información de la UPIT debe garantizar que todo cambio que se deba realizar en los sistemas información en producción deba ser probados en un ambiente de pruebas antes de aplicarlos a los sistemas en producción, de acuerdo con la metodología de desarrollo de la Entidad, salvo que sean cambios de emergencia.

ARTÍCULO 8. Política de Seguridad en las Comunicaciones. La política de seguridad en las comunicaciones de la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
2. La Secretaría General y la Oficina de Gestión de la Información de la UPIT deben monitorear continuamente el canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.
3. La Secretaría General de la UPIT debe generar registros de navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.
4. La Secretaría General de la UPIT debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos
5. La Secretaría General debe realizar segmentación de Redes para Servidores Públicos, Contratistas y visitantes de la UPIT.
6. La Secretaría General de la UPIT debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.
7. La Secretaría General de la UPIT debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad.

8. La Secretaría General de la UPIT debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad.
9. La Secretaría General de la UPIT debe permitir el acceso a redes inalámbricas mediante un portal de acceso en donde permita al usuario ingresar un usuario y contraseña dentro de una red pública para visitantes (UPIT) y una privada (UPIT_INTERNA) para funcionarios.
10. La Secretaría General de la UPIT debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la entidad.

ARTÍTULO 9. Política de Organización Interna de la Seguridad de la Información. La política de organización interna de la seguridad de información de la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe mantener y documentar los contactos con autoridades de Policía, Fiscalía, Bomberos u otras entidades especializadas con el fin de contactarlos en caso de un incidente de seguridad de la información.
2. La UPIT a través de la Secretaría General y otras dependencias que se designen, deben tener contacto permanente con agentes especializados en seguridad y privacidad de la información, con el fin de compartir conocimientos en la materia.
3. Los proyectos formulados e implementados por la UPIT, en cumplimiento de su misión, deben involucrar un componente de gestión de los riesgos de seguridad, asociados a la información del proyecto. Esta gestión incluye la identificación de los riesgos, y la definición de medidas para gestionarlos. Los parámetros para la identificación de riesgos y medidas serán definidos por la Secretaría General de la UPIT.

ARTÍCULO 10. Política de Seguridad de los Recursos Humanos. Definir la política de Seguridad de los Recursos Humanos de la UPIT, relacionada con la seguridad digital y privacidad de la información, a partir de los siguientes lineamientos:

1. Todo servidor público o contratista, firmará un documento o cláusula contractual en las que se establezca un compromiso de confidencialidad y no divulgación de la información reservada o estratégica de la UPIT.
2. Una vez formalizado el proceso de vinculación, el jefe inmediato, o supervisor, debe solicitar a través de la Mesa de Ayuda la apertura del inventario y demás servicios que requiera el Servidor Público, contratista o tercero, para la ejecución de sus funciones u obligaciones contractuales.
3. La Secretaría General con el apoyo de la Oficina de Gestión de Información de la UPIT realizarán de manera permanente, un programa de concientización y capacitación en seguridad de la información.
4. Es responsabilidad del Servidor Público, contratista o personal provisto por terceros, informar de los incidentes de seguridad de la información a través de los medios dispuestos por la Secretaría General de la UPIT.
5. Es responsabilidad del Servidor Público realizar la entrega de la información propia de la UPIT, que se encuentra bajo su gestión, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones.
6. El supervisor del contrato debe custodiar la información de la UPIT bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
7. La Secretaría General debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de termi-

nación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.

8. La Secretaría General de la UPIT debe informar a la Mesa de Ayuda o canal dispuesto para tal fin, cualquier novedad de desvinculación administrativa, laboral o contractual del Servidor Público, contratista o tercero; una vez notificada la novedad la Mesa de Ayuda debe proceder a la inactivación de los servicios de acceso y servicios de red.
9. Se creará una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con la UPIT.
10. Bajo ningún parámetro se podrán restablecer los accesos a correos electrónicos; solo se podrán restablecer buzones para consulta y no se podrán emitir correos ni notificaciones desde estos buzones.
11. En caso de desvinculación laboral o contractual se deben inactivar todos los accesos a los sistemas de información y se debe solicitar la devolución del carné, tarjetas de acceso o documento que acredita como Servidor Público, contratista o tercero de la UPIT.
12. Los lineamientos de política de seguridad de los recursos humanos serán especificados mediante procedimientos, por parte de la Secretaría General de la UPIT.

ARTÍCULO 11. Política de Gestión de Activos. La Secretaría General de la UPIT establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración y uso adecuado de la información, con el objeto de garantizar su protección. Dichos lineamientos serán definidos considerando los siguientes literales.

a. **Inventario de activos**. Los activos de la Unidad de Planeación de Infraestructura de Transporte deben ser identificados, clasificados, valorados y controlados para garantizar su uso y protección. La Secretaría General de la entidad diseñará la metodología para realizar en inventario de activos.

b. **Responsabilidad por los activos**. La responsabilidad de los activos de la UPIT se define a partir de los siguientes lineamientos:
   I. Todos los procesos de la UPIT deben contar con un inventario de sus activos de información.
   II. Todos los activos de información mantenidos en el inventario deben tener un propietario
   III. La Secretaría General de la UPIT, debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.
   IV. Los Servidores Públicos, contratistas o terceros, no deben usar software no autorizado o de su propiedad en activos de la UPIT.
   V. Los Servidores Públicos, contratistas o terceros de la UPIT, deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de Entrega de Bienes y Documentos que será diseñado e implementado por la Secretaría General de la UPIT.

c. **Clasificación de la Información.** La clasificación de la información de la UPIT, relacionada con la seguridad y privacidad, se define a partir de los siguientes lineamientos:
   I. La Secretaría General y la Oficina de Gestión de la Información de la UPIT definirán los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad.

II. La Secretaría General y la Oficina de Gestión de Información, formularán el Manual de Clasificación y Publicación de la Información de la entidad, para que los responsables de esta la cataloguen y determinen los controles requeridos para su protección.
III. La Secretaría General de la UPIT, deben diseñar lineamientos para la administración de los archivos de acuerdo con lo establecido en la normatividad.
IV. Los Servidores Públicos, contratistas o terceros de la UPIT deben aplicar la clasificación de la información de la entidad.
V. Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

d. **Manejo de medios tecnológicos.** El manejo de medios de la UPIT, relacionada con la seguridad y privacidad de la información, se define a partir de los siguientes lineamientos:
I. La Secretaría General de la UPIT debe definir un procedimiento para el uso de medios removibles.
II. La Secretaría General de la UPIT debe proveer a los usuarios de la UPIT los métodos de cifrado de la información, así como administrar el software o herramientas utilizadas para tal fin, y generar la guía de uso para el usuario.
III. Es responsabilidad de cada Servidor Público, contratista o tercero tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, o pérdida de información.
IV. Se prohíbe el uso de medios removibles que contengan información reservada de la UPIT.
V. Cuando se requiera transferir un medio de almacenamiento de información de la UPIT a otras entidades se debe establecer un acuerdo de confidencialidad y seguridad, entre las partes.
VI. La Secretaría General de la UPIT debe autorizar el uso de periféricos o medios de almacenamiento externo, de acuerdo con las necesidades requeridas para el cumplimiento de las funciones y del perfil del cargo de los servidores públicos o Contratistas
VII. Los servidores públicos, contratistas o personal provisto por terceras partes deben acoger las condiciones de uso de periféricos y medios de almacenamiento establecidos por la Secretaría General de la UPIT.
VIII. Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la UPIT que sean reutilizados o dados de baja, con el fin de controlar que la información contenida en estos medios no se pueda recuperar.
IX. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la UPIT.

ARTÍCULO 12. Política de Control de Acceso. La política de control de accesos la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe suministrar y garantizar el cambio de contraseña, a los usuarios las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol. Las credenciales de acceso son de uso personal e intransferible.

2. La conexión remota a la red de área local de la UPIT debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por la Secretaría General de la UPIT.
3. La Secretaría General de la UPIT debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.
4. La Secretaría General de la UPIT debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
5. La Secretaría General de la UPIT debe realizar el cambio de contraseña de la red inalámbrica de la Entidad mínimo tres (3) veces al año.
6. La Secretaría General de la UPIT para los eventos que se realicen en la entidad debe generar usuario y clave de red Wifi, el cual debe expirar una vez finalizado el evento
7. La Secretaría General de la UPIT debe revisar que los equipos personales de los Servidores Públicos, contratistas o terceros de la entidad que se conecten a las redes de datos de la entidad, cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.
8. La Secretaría General de la UPIT debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario. El usuario de correo electrónico debe ser igual al usuario de red, y contar con single on (mismo usuario, misma contraseña en los dos (2) servicios).
9. La Secretaría General de la UPIT sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía.
10. Por defecto los usuarios creados no tienen permisos de administrador. En caso de requerirlo deben realizar la solicitud a la Mesa de Ayuda. Sólo se otorgan los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.
11. El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible.
12. Una vez finalizada la gestión de servicios prestados por terceras partes para la Entidad, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato.
13. La Secretaría General de la UPIT, con el apoyo de Mesa de Ayuda, debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la UPIT, cada vez que sea requerido.
14. Todos los accesos de servicios de red deben estar conectados a la cuenta del directorio activo, si esta caduca, todos los accesos también, como son (VPN, cuentas de usuario, servicio de impresión y telefonía, etc.)
15. La Secretaría General de la UPIT debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

ARTÍCULO 13. Política de dispositivos móviles. La política de dispositivos móviles de la UPIT se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe mantener actualizado el inventario de los dispositivos móviles autorizados.
2. Los dispositivos móviles de propiedad de los de servidores públicos, contratistas, o terceros no deben estar incluidos en el dominio upit.gov.co o

cualquiera que funcione dentro de la entidad. Para conectarse a los servicios de la red de datos deberán realizar solicitud a la Mesa de Ayuda y cumplir con los lineamientos referentes a seguridad de la información.

3. Todos los dispositivos móviles que almacenen información de la UPIT deben tener instalado un software antivirus, y sistema operativo actualizado.
4. En dispositivos móviles entregados por la UPIT, los servidores públicos no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica.
5. En caso de pérdida o robo de un dispositivo móvil de propiedad de la UPIT, los servidores públicos, tendrá que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato al personal de la Mesa de Ayuda, quienes deben realizar las acciones necesarias para la protección de la información.

ARTÍCULO 14. Política de Teletrabajo y Trabajo Remoto. La política de Teletrabajo de la UPIT, relacionada con la seguridad y privacidad de la información, se define a partir de los siguientes lineamientos:

1. La Secretaría General de la UPIT debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la UPIT, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de la información.
2. Toda información gestionada o custodiada por la UPIT, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

ARTICULO 15. Responsables. La definición, implementación y mantenimiento de la Política de Seguridad Digital y Privacidad de la Información de la Unidad de Planeación de Infraestructura de Transporte UPIT, tiene como responsables las siguientes instancias:

1. El personal encargado de la seguridad digital y privacidad de la información adscrito a la UPIT en la Secretaría General y Oficina de Gestión de la Información, quienes diseñarán, implementarán y velarán por el mantenimiento del Modelo de Seguridad Digital y Privacidad de la Información de la entidad.
2. Los funcionarios, contratistas, proveedores, operadores, entes de control y los terceros quienes deberán cumplir la Política Específicas de Seguridad Digital y Privacidad de la Información específicas.

ARTICULO 16. Implementación. El desarrollo e implementación de las políticas específicas establecidas mediante la presente resolución se realizará a través de la adopción del Manual de Seguridad Digital y Privacidad de la Información.

CAPÍTULO III
REVISIÓN, VIGENCIA Y DEROGATORIA

ARTÍCULO 17. Revisión. La política de Seguridad de la Información de la Unidad de Infraestructura de Transporte UPIT, será revisada anualmente o antes, si existen modificaciones que así lo requieran.

UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE - UPIT

RESOLUCIÓN NÚMERO 045 DEL 24 DE MARZO DEL 2022

"Por medio de la cual se adopta la política de seguridad digital y privacidad de la información y se definen lineamientos frente al uso y manejo de la información de la Unidad de Planeación de Infraestructura de Transporte – UPIT'

ARTÍCULO 18. Vigencia y Derogatoria. La presente Resolución rige a partir de la fecha de su publicación.

COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los 24 días de marzo del 2022,

YOLANDA BEATRIZ CABALLERO PÉREZ
DIRECTORA GENERAL (E)
UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE

Preparó: Libia Constanza Martínez – Profesional Especializado UPIT

VB: Claudia Marcela Pinilla Pinilla – Secretaria General de la UPIT.
Diana Carolina Reyes Cuervo – Jefe OAJ -UPIT