PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUTO DEPARTAMENTAL DE TRÁNSITO DEL QUINDÍO

ARMENIA QUINDÍO

2024

Control de Versiones

RSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	19/10/2018	Emisión
2.0	19/04/2023	Actualización
3.0	31/01/2024	Actualización

Tabla de Contenido

Tabla de Ilustraciones

1. INTRODUCCIÓN

La estrategia de Gobierno digital, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente gracias a las TIC (Ministerio de tecnologías de la información y comunicaciones, 2017).

Es por lo anterior que a través del decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en el CAPITULO 1, POLÍTICA DE GOBIERNO DIGITAL, en la SECCIÓN 1, OBJETO, ALCANCE, ÁMBITO DE APLICACIÓN Y PRINCIPIOS, ARTÍCULO 2.2.9.1.1.3. Principios: se define el componente de seguridad y privacidad de la información, como un principio que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano *(Ministerio de Tecnologías de l Información y Comunicaciones MinTIC, 2018).*

Teniendo en cuenta el decreto anterior el Instituto Departamental de Transito del Quindío identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que se establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

La protección y seguridad de los activos de información, parte del concepto fundamental de seguridad de la información la cual se desarrolla mediante el principio de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad , disponibilidad, accesibilidad de la información que se complementan con otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

En este documento se describe las políticas, normas y lineamientos técnicos de seguridad de la información definidas mediante el uso y el modelo a seguir bajo las cuales se van a implementar las políticas de seguridad de la información dentro del Instituto Departamental de Transito del Quindío (IDTQ , en las cuales se adoptaran las mejores prácticas planteadas por Mintic en su marco de referencia de la arquitectura TI, en su modelo de seguridad y privacidad de la información, basándose y apoyándose en las normas y estándares de seguridad como lo son la norma ISO 27001/2022.

2. ALCANCE

Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos y físicos, que representa los objetivos sobre los que se sustenta el Sistema de Gestión de Seguridad de la Información. Las políticas de seguridad informática y controles serán de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas y terceros que hagan uso de los activos de información del Instituto Departamental de Transito del Quindío.

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Oficina de Sistemas o el Director General de la entidad, cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos institucionales, y deberán ser documentadas formalmente.

Las políticas de seguridad informática serán objeto de evaluación semestral, aplicando mecanismos de autocontrol y autoevaluación a través de indicadores de gestión, para garantizar el mejoramiento continuo.

Por último, debemos decir que la aplicación de las políticas propuestas en este documento obedece al interés por parte del Instituto Departamental de Transito del Quindío, en diseñar, implementar y sostener el modelo de seguridad y privacidad de la información de acuerdo a las políticas y manuales establecidas por la estrategia de gobierno en digital del ministerio de tecnologías de la información y comunicaciones MinTic.

3. GLOSARIO

- **Activo de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la gobernación del Quindío.
- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Sistema de Información:** Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocios, es también el conjunto total de procedimientos, operaciones, funciones y difusión de datos o información en una organización (Universidaddel Cauca, 2017).
- **Administrador de Bases de Datos (DBA):** Persona responsable de los aspectos ambientales de una base de datos.
- **Amenaza:** Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Antivirus:** Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
- **Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento de los sistemas de información.
- **Backups:** Es una copia de seguridad de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida o robo.
- **Hardware:** Se refiere a las características técnicas y físicas de las computadoras.
- **IP:** Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP.
- **Plan de Contingencia**: Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.
- **Redes:** Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.
- **Servidores:** Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumplen la colaboración en la arquitectura cliente-servidor.
- **Software:** Programas y documentación de respaldo que permite y facilita el uso del pc. El software controla la operación del hardware.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. NORMATIVIDAD

Legislación	Tema	Referencia
Ley 527 de 1999	"Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos"	El mensaje de datos es "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entreotros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax".
Ley 1226 del 2008	"Por la cual se dictan disposiciones generales del hábeas data y se regula el manejode la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"	Se regula el manejo de la informaciónpara "todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada".
Ley 1273 del 2009	"Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente lossistemas que utilicen lastecnologías de la información y las comunicaciones".	"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados adesarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

Ley 1581 de 2012	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia en particular, al artículo 15 de la Constitución Nacional, según el cual "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley". El objeto de la ley es "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".
Decreto 2573 del 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 113 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014y se dictan otras disposiciones	El decreto 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.

Decreto 1008 de 2018	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"	Permite lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la gobernación del Quindío desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos que puedan beneficiar tanto a la entidad como a los municipios del departamento y sus comunidades.

5. JUSTIFICACIÓN

Las organizaciones se han dado cuenta que, usando las tecnologías de la información, han logrado transformar, desarrollar y llevar a cabo sus planes estratégicos a niveles más avanzados. El Ministerio de Tecnologías de la Información y las Comunicaciones - Mintic a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia de Gobierno Digital: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia de Gobierno en Línea.

La constante necesidad que tiene el IDTQ de ajustarse rápidamente a los cambios que se dan en el ambiente tecnológico, hace necesario que la administración tenga la información disponible, oportuna y actualizada para poder tomar decisiones acertadas, esperando que la tecnología informática les ayude a tener una planificación más precisa de los recursos informáticos.

6. OBJETIVOS

5.1. Objetivo General

El Instituto Departamental de Transito del Quindío en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos.

5.2. Objetivos específicos

- Fortalecer la cultura de seguridad de la información y los roles en los funcionarios, terceros, aprendices, practicantes y clientes del Instituto Departamental de Transito del Quindío.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la entidad.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad para la reducción de los riesgos.
- Describir y realizar las etapas del MSPI para la mejora e implementación del modelo.
- Realizar la respectiva comunicación del modelo de políticas de seguridad de la información a los funcionarios de la entidad y ciudadanía.

7. PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Departamental de Transito del Quindío, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información **(SGSI)** buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

Para el Instituto Departamental de Transito del Quindío la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del MSPI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes externos del Instituto Departamental de Transito del Quindío.
- Garantizar la continuidad del negocio frente a incidentes.
- El IDTQ ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Dentro de las temáticas que se tocan en este punto se encuentran por ejemplo la gestión de activos, seguridad física y ambiental, control de accesos, etc. Para abordar este punto es necesario remitirse a la "Guía de políticas específicas de seguridad y privacidad de la información" y mencionar aquellas que la Entidad haya establecido como necesarias y primordiales. De esta forma se presenta el siguiente ejemplo:

A continuación, se establecen 10 principios de seguridad que soportan el **SGSI** del Instituto Departamental de Transito del Quindío, las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

- El Instituto Departamental de Transito del Quindío protegerá la información generada, procesado resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La gobernación del Quindío garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- El Instituto Departamental de Transito del Quindío protegerá la información creada,

procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- El Instituto Departamental de Transito del Quindío protegerá su información de las amenazas originadas por parte del personal.

- El Instituto Departamental de Transito del Quindío protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- El Instituto Departamental de Transito del Quindío controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- El Instituto Departamental de Transito del Quindío implementará control de acceso a la información, sistemas y recursos de red.

- El Instituto Departamental de Transito del Quindío garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

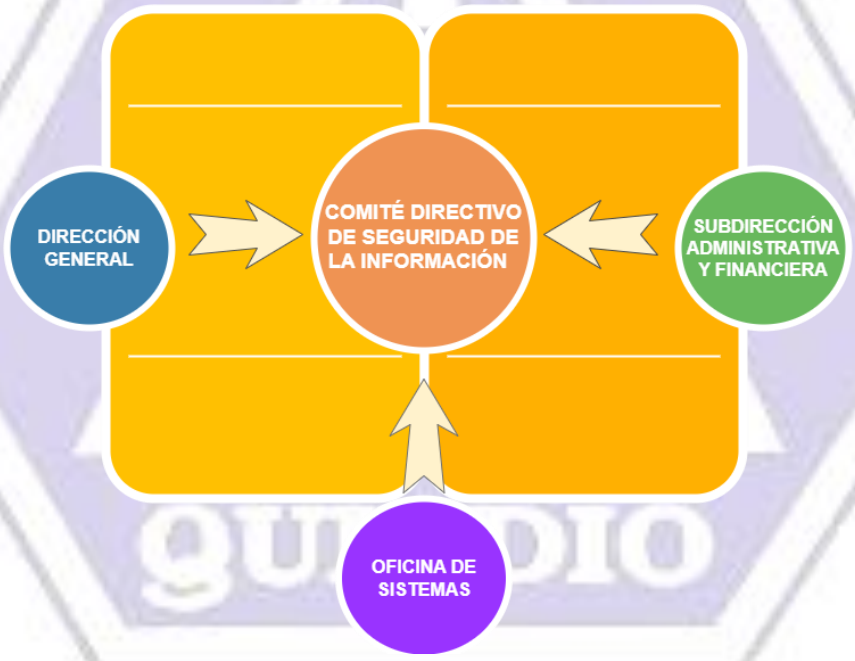
- El Instituto Departamental de Transito del Quindío garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- El Instituto Departamental de Transito del Quindío garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

8. POLITICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

8.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Dentro de esta se identifican los actores involucrados que hacen parte del comité directivo de seguridad de la información, en los cuales se encuentran el Director General de la entidad, el subdirector administrativo y financiero y la dirección Tecnologías de Información, los cuales tienen como objetivo en cada comité revisar el avance de la implementación y el cumplimiento del manual de políticas de seguridad de la información, además la retroalimentación y el mejoramiento continuo de estas mismas.



Fuente: autoría propia

8.2. Roles y Responsabilidades

El Instituto Departamental de Tránsito del Quindío, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.):

- Garantizar la existencia de una dirección y apoyo gerencial que soporte la administración y el desarrollo de iniciativas sobre seguridad de la información, a través de compromisos y uso adecuado de los recursos en la entidad.
- Formular y mantener una política de seguridad de la información que aplique a toda la organización conforme con lo dispuesto por el Instituto Departamental de Transito del Quindío.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité de Gestión y Desempeño	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.
Oficial de Seguridad Digital y Sistemas	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
	• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
	del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
• **Talento Humano**	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
• **Control Interno**	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
• **Comunicación Interna**	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.
• **Oficina Jurídica y Contratación**	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
• **Líderes de Proceso**	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
• **Todos los funcionarios y contratistas**	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

8.3. Políticas para los servicios de procesamiento de la Información

El Instituto Departamental de Transito del Quindío, será la encargada de velar y custodiar los activos tecnológicos tangibles e intangibles con los que cuenta la entidad, así como la definición de los estándares para el desarrollo, adquisición y mantenimiento de la infraestructura tecnológica, todo lo anterior siguiendo las mejores prácticas internas y normatividad vigente.

- **Desarrollo de aplicativos**

El Instituto Departamental de Transito del Quindío entiende y apoya el desarrollo propio o externo de aplicativos, más aún cuando el software que se requiere no se encuentra en el mercado o los costos de licenciamiento sobrepasan el presupuesto de la entidad, por tal motivo el desarrollo de aplicativos deberá ser autorizado por un comité integrado por el Gerente General, Oficina de Sistemas y las dependencias involucradas con la finalidad de este. Dicho software debe seguir las fases del ciclo de vida de los sistemas de información y deberá ser testeado por los funcionarios de la entidad y las dependencias que utilizarán el software.

- **Control de cambios**

Al momento que un área de la entidad requiera alguna modificación, estructural o no, sobre el software aplicativo, es necesario que la solicitud de modificación esté autorizada mediante escrito por el gerente general y personas responsables de la ejecución del proceso.

- **Control de Versiones**

El director de sistemas será el responsable de gestionar el control de las distintas versiones de desarrollo de un software, de tal forma que se garantice la confidencialidad, integridad y actualización de los documentos.

- **Publicación de Aplicativos**

Para la publicación y puesta en marcha de aplicativos nuevos estos deben estar correctamente diseñados, evaluados de forma minuciosa para evitar la redundancia en las salidas de información, supervisados y autorizados por el gerente general y la oficina de sistemas.

8.4. Política de confidencialidad de la información

Todos los servidores públicos que hacen parte del Instituto Departamental de Transito del Quindío, que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes, software y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la entidad, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso, haciendo valederas las investigaciones penales y disciplinarias a las que haya lugar.

- **Controles**

El Instituto Departamental de Transito del Quindío identificará la información considerada clasificada o reservada, índice que deberá ser divulgada de conformidad con la normatividad vigente. La Entidad establecerá controles para el intercambio de información con terceros para asegurar la reserva e integridad de la información y que se respeten los derechos de autor.

8.5. Política de Seguridad de acuerdos con terceros

Los acuerdos con terceras partes que impliquen acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de la información de la gobernación del Quindío o la adición de productos o servicios a los servicios de procesamiento de la información deben considerar todos los controles pertinentes a fin de minimizar los riesgos y de mantener la seguridad de la información y de los servicios de procesamiento.

- **Controles**

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes (International Organization for Standardization, 2014).

La Entidad identificará los riesgos para la información y servicios de procesamiento de información que involucran a terceros e implementará los controles adecuados antes de autorizar el acceso. La Entidad considerará todos los requisitos de seguridad de la información identificados, antes de dar acceso a los activos de información a partes externas.

9. GESTIÓN DE CONTROL DE ACTIVOS

9.1. Políticas de creación y restauración de copias de seguridad

El Instituto Departamental de Transito del Quindío, ha identificado los procesos operativos y de misión crítica que se manejan a través de los diferentes aplicativos de la entidad, los cuales son respaldados con copias de seguridad diarias, la frecuencia de estas copias fue establecida por la oficina de sistemas.

Controles

- Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.
- Las copias de seguridad de los aplicativos del área operativa son el **SIOT (**Sistema integrado de información para organismos de tránsito) y del área administrativa **PUBLIFINANZAS** (Software financiero de la entidad), página Web e **INTRAWEB** (Es el Software de Ventanilla Única Virtual de la Entidad). se deberán de realizar diariamente y registrasen en las bitácoras correspondientes para cada uno de los aplicativos.
- Las copias de seguridad de las bases de datos de los aplicativos, (documentos digitalizados y/o electrónicos) estarán resguardadas en medios de almacenamiento externo por el tiempo en el que se indique en las tablas de retención documental y el programa de gestión documental de la entidad.
- El Instituto Departamental de Tránsito del Quindío deberá definir y aplicar el modelo de conservación, restauración y eliminación de los archivos electrónicos, teniendo en cuenta siempre el programa de gestión documental de la entidad.

- Los servidores públicos efectuaran copias de seguridad supervisadas por el personal de la entidad, cuando los equipos de cómputo sean enviados a mantenimiento preventivo o correctivo, previniendo así la pérdida de información.
- Los Administradores de las bases de datos realizaran pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente.
- El Instituto Departamental de Tránsito del Quindío deberá de conservar las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las el almacenamiento adecuado, medidas protección y seguridad física adecuadas.

9.2.Políticas para el manejo de datos

- **Uso Compartido**

Política

El usuario o funcionario que haga parte del Instituto Departamental de Tránsito del Quindío que autoriza el uso compartido de carpetas es responsable por las acciones y el acceso a la carpeta de la información compartida.

Controles

El usuario o funcionario del Instituto Departamental de Tránsito del Quindío que autoriza la carpeta compartida debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo de permanencia en el repositorio el cual estará expuesta. A demás el usuario o funcionario que autoriza el acceso a la carpeta comprimida debe asegurarse que cuente con un antivirus autorizado o licenciado.

- **Antivirus**

Política

Todos los equipos de la entidad deben tener instalado, configurado, funcionando, actualizado y debidamente licenciado un antivirus, el cual será suministrado por la Oficina de Sistemas de la entidad.

Controles

- ✓ El antivirus se debe instalar con opción de actualización automática.
- ✓ Está prohibido que los usuarios desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.
- ✓ Los usuarios deben asegurarse de que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.
- ✓ Los usuarios que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Oficina de sistemas para que le brinden el soporte técnico de erradicación del virus.
- ✓ EI equipo de trabajo de la Oficina de sistemas de información e infraestructura tecnológica de la entidad es responsable por la actualización oportuna del software antivirus.

- **Dominio idtq.com**

Políticas

Todos los equipos de propiedad del Instituto Departamental de Tránsito del Quindío deben estar dentro del dominio idtq.gov.co, el cual será administrado desde la entidad.

Controles

- ✓ El personal del Instituto Departamental de Tránsito del Quindío, deberá conectar a los equipos de los funcionarios, vigilarlos y administrar los permisos de cada equipo, según lo designado por el encargado del área de sistemas de la entidad.
- ✓ Está prohibido que algún equipo de pertenecía de la entidad este por fuera del dominio.
- ✓ Las políticas de contraseñas de administrador del dominio, por motivos de seguridad solo las conocerán los encarados del área de sistemas.
- ✓ Las contraseñas de los equipos de los funcionarios serán suministradas por el administrador del dominio el cual es designado por el área de sistemas.
- ✓ Se realizarán controles a usuarios del dominio, con el fin de verificar si existen usuarios con permisos no autorizados y/o usuarios repetidos.
- ✓ Los equipos de cómputo adquiridos por la entidad deberán tener soporte a redes, con el fin de conectarlos al dominio del Instituto Departamental de Tránsito del Quindío.

- **Bases de Datos**

Política

Los administradores de las bases de datos del Instituto Departamental de Tránsito del Quindío, no podrá(n) manipular directamente los datos, salvo en circunstancias en las cuales los aplicativos no lo permitan, y solo lo realizará cuando medie autorización escrita del líder del proceso propietario de la información o previa autorización de la Oficina de sistemas, y con el debido soporte que requiera de la actualización respectiva.

Controles

- ✓ Se deben programar todas las tareas de afinamiento de las bases de datos y los sistemas de información de manera periódica, de acuerdo con la cantidad de solicitudes o quejas de los usuarios respecto de la disponibilidad de las aplicaciones.
- ✓ El acceso a las bases de datos de los sistemas se realizará de conformidad con las políticas de acceso.
- ✓ Las empresas externas contratadas por la gobernación del Quindío, para administrar y dar soporte a las bases de datos, deberán tener permiso autorizado por el director de sistemas para realizar cualquier modificación y/o actualización en las bases de datos de los aplicativos.
- ✓ El acceso a la información de las bases de datos solo será realizado por el personal autorizado por el encargado del área de sistemas, y mediante un documento que garantice la confidencialidad y privacidad de la información.

- **Activos de Información**

Política

La protección y seguridad de los activos de información, parte del concepto fundamental de seguridad de la información la cual se desarrolla mediante el principio rector de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información.

Controles

- El Instituto Departamental de Transito del Quindío, debe de actualizar el Inventario de los activos de información físicos cadaseis meses, además que debe contar con placa de inventario que lo identifica como activo fijo de la entidad.

- Toda la información del Instituto Departamental de Transito del Quindío, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criteriosque dicte la Oficina de TI.
- Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.
- El Instituto Departamental de Transito del Quindío implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.
- El Instituto Departamental de Transito del Quindío tiene la custodia sobre todo dato, información y mensaje generado,procesado y contenido por sus sistemas de cómputo, así como también de todoaquello transmitido a través de su red de telecomunicaciones o cualquier otromedio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.
- Debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.
- El inventario de los activos de información digitales (software, bases de datosy archivos digitales), es responsabilidad de la dirección TI.

9.3. Estrategia de preservación de archivos

Política

El instituto Departamental de Transito del Quindío, implementará las acciones para la protección y preservación de los archivos en el tiempo, teniendo en cuenta el entorno técnico para el buen funcionamiento del software y hardware.

La entidad considera fundamental dicho proceso para la recuperación en el tiempo de la información almacenada en los diferentes aplicativos, bases de datos, correo electrónico, páginas web y carpetas virtuales compartidas y servidores que poseen cada una de las áreas de la Entidad.

Controles

- ✓ El Instituto Departamental de Tránsito del Quindío, implementará técnicas de preservación digital de los documentos de gestión documental teniendo en cuenta el programa de gestión documental de la entidad y la vida útil del hardware y software de la entidad.
- ✓ El Instituto Departamental de Tránsito del Quindío, con la ayuda de los funcionarios que proveen los servicios del aplicativo de gestión documental deberán migrar los formatos antiguos de archivos (.doc, .xls, pdf) a formatos más modernos (.docx, .xlsx, pdf/A), con el fin de garantizar que la información se mantenga plena e inalterable en el tiempo.
- ✓ La oficina de gestión documental deberá establecer los tiempos de permanencia de los archivos electrónicos y bases de datos de acuerdo a sus tablas de retención documental.
- ✓ El proceso de migración de documentos debe garantizar:

  (a) Independencia del dispositivo: Debe ser representado de manera fiable en cualquier plataforma software o hardware.

  (b) Auto contenido: Debe contener todos los recursos necesarios para su representación.

  (c) Autodocumentado: Debe contener su propia descripción.

  (d) Sin restricciones: No debe haber mecanismos de protección del fichero.

  (e) Disponible: Especificación accesible cuando se requiera.

  (f) Adoptado: Un uso amplio contra los riesgos de la preservación.

- ✓ El área de sistemas deberá monitorear los aplicativos de la Entidad, incluyendo el Sistema de gestión documental y reportar los eventos de seguridad de la información al proveedor del aplicativo, para que realice las correcciones correspondientes.
- ✓ El Instituto Departamental de Transito del Quindío, a través del plan de tratamiento de riesgos deberá realizar un seguimiento a los riesgos identificados que afecten la integridad de los archivos.

9.4.Política de medios de almacenamiento externo

Política

Los funcionarios públicos que contengan información confidencial de propiedad de la entidad en medios de almacenamiento externo, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

El medio de almacenamiento externo que conecte un funcionario en su equipo asignado es responsabilidad propia, por tal motivo la información que se encuentre almacenada en estos medios, que por algún motivo sea modificada o borrada por accidente, no involucra ni compromete a la entidad ni a área de sistemas en ningún caso.

Controles

- Los medios de almacenamiento con información crítica deberán ser manipulados y enviados única y exclusivamente por la persona asignada por el Instituto Departamental de Transito del Quindío para hacer respaldos y salvaguardar información.
- Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.
- Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

- La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.
- Los equipos servidores tendrán deshabilitada la reproducción automática de dispositivos externos de almacenamiento removibles.

9.5. Políticas de uso del correo electrónico

Política

El Instituto Departamental de Transito del Quindío es la encargada de definir los nombres, estructura y plataforma que se debe utilizar para la cuenta de correo Institucional de cada area de la entidad.

Controles

Administración del Correo Institucional

- Los correos Institucionales asignados a los funcionarios, contratistas o terceros pertenecen a **Instituto Departamental de Tránsito del Quindío**, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina de tecnología y sistemas podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

Cambio de Contraseñas a Correos Institucionales

- En el mismo instante en que **Instituto Departamental de Tránsito del Quindío** cree y dé a conocer la cuenta de correo Institucional designada para cada área de la entidad, la persona a la que será entregada el correo será responsable si decide cambiar la contraseña.
- La confidencialidad y el uso del usuario y contraseña será responsabilidad de la persona a quien se le asigne.

Recepción e Intercambio de información

- El intercambio de información entre la entidad y terceros a través de correos electrónicos se hará única y exclusivamente por medio de los correos institucionales, y en ningún caso por medio de correos personales.
- El usuario responsable del correo institucional deberá evitar abrir los adjuntos de correos de origen desconocido a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.
- El correo institucional será de uso exclusivo para fines propios de la Entidad y en su uso se dará aplicación al código de ética; En consecuencia, es Prohibido utilizar el correo institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

9.6.Políticas de acceso a internet

Política

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

Controles

- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.
- El Instituto Departamental de Transito del Quindío es la responsable de la configuración apropiada e instalación de mecanismos de detección de intrusos y sistemas de protección del Hardware (firewalls), Software base, aplicativos, redes y sistemas de comunicación, a fin de evitar la intrusión y los ataques físicos.
- El uso de Internet está limitado por las políticas de seguridad del área de sistemas.
- Los Accesos a la red (Internet) serán solo de interés laboral y no personal. Se establecen horarios de uso a fin de no saturar el canal y poder hacer un buen uso del mismo.
- Las páginas de consulta común por su contenido de interés general y de carácter laboral como: SIMIT, RUNT, www.quindio.gov.co, www.idtq.gov.co, gobierno digital y demás páginas de carácter institucional, se pueden consultar encualquier momento dentro del horario laboral.
- El usuario no deberá descargar (o copiar) archivos de la red sin autorización del área

de sistemas.

- El usuario no debe ejecutar las opciones de actualización de programas que eventualmente aparecen cuando se navega en Internet.
- La comunicación estará limitada por las políticas de seguridad del área deSistemas.
- Solo se enviará y recibirá información de interés laboral.
- En ningún caso de recibir información en archivos adjuntos de dudosa procedencia o que no esté esperando, se notificará al área de sistemas, para analizar y evitar que ingresen virus al sistema.
- Al enviar información el responsable será el usuario correspondiente.
- No se deberá enviar información de tipo estadístico, informativo o información relevante de las acciones de la Dirección, Área de trabajo o del Gobierno municipal a ningún destino no autorizado.
- Para el desarrollo o modificaciones del sistema, el usuario deberá presentar su solicitud al área de sistemas para su evaluación.
- El usuario es el único responsable de desactivar o activar el acceso a su equipo.
- Se tienen correos institucionales dentro de la política de austeridad en el gasto público, se recomienda su uso para toda la comunicación interna y ahorrar tinta y papel, igualmente las carpetas compartidas por la red local (LAN) para mover y compartir información.
- El direccionamiento y la configuración asignada a los equipos dentro de la LAN es de uso exclusivo del equipo asignado al funcionario por la oficina de sistemas.Cualquier modificación al respecto, está prohibida pues genera traumatismo en elesquema de seguridad de LAN.

9.7.Políticas de publicación en el portal web

Administración de los contenidos institucionales de la página web

- La administración de los contenidos de las páginas institucionales estará a cargo del área de sistemas, solo para ser publicada, la actualización de dicha información o contenidos debe ser actualizada y registrada por cada líder del área de la entidad, según el organigrama institucional (Director Genera, Asesor Jurídico, Asesor Control Interno, Subdirector Administrativo y Financiero, Profesional Área Técnica), quien será el encargado(a) de verificar los contenidos que pueden o deben ser publicados.
- Todo contenido deberá respetar la ley de derechos de autor.
- Ningún contenido del portal WEB se puede copiar con fines comerciales, ni se puede utilizar en otros sitios WEB.

Editores de los contenidos institucionales de las paginas

- Cuando por omisión un editor del portal web deje sus contraseñas o las revele, se hará responsable de todo lo realizado con este usuario.
- El funcionario designado por la entidad para el manejo de la estrategia de gobierno digital, dentro de sus funciones deberá capacitar a los funcionarios para el cargue y administración de la información de la página web institucional.
- Solo el funcionario designado por la entidad tendrá contraseñas de administrador del portal web.
- La empresa encargada del dominio y hosting del Instituto Departamental de Transito del Quindío tendrá contraseñas de superusuario, pero dentro de sus funciones estará supeditada a cláusulas de confidencialidad de la información.

9.8.Políticas de dispositivos móviles

Política

El Instituto Departamental de Transito del Quindío permite a funcionarios y contratistas utilizar los dispositivos móviles en sus oficinas y a su vez que estos se conecten a las diferentes redes Wi-fi del área, teniendo en cuenta los siguientes controles.

Controles

- Aunque se permite el acceso a la red wi-fi de la entidad a las personas, esta se encuentra en diferente segmento de red de la red LAN de la entidad, con esto se garantiza que no existan equipos no deseados dentro de la red interna, que puedan causar algún daño a la misma.
- Las contraseñas de las redes Wi-fi se deben cambiar cada 3 meses, ya que la entidad está cambiando de personal (contratistas) constantemente.
- El Instituto Departamental de Transito del Quindío es la encargada de administrar la red Wi-fi, esta contará con todas las contraseñas Wi-fi de la entidad y podrá aplicar las restricciones de red que considere necesarias para salvaguardar los datos que genera la entidad.

9.9.Política de adquisición, desarrollo y mantenimiento de sistemas

Política

Toda adquisición de recurso tecnológico en la entidad deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por el área de sistemas.

Controles

- El área de sistemas, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

Adquisición de equipos tecnológicos

- Todos los dispositivos adquiridos deben contar con la garantía de fábrica. Esta debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento.
- Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.
- Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.
- Cuando los dispositivos tecnológicos como computadores e impresoras sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros se encuentre en Colombia.

Mantenimiento

- **Hardware**

  - ✓ El equipo de cómputo será asignado de acuerdo al puesto o función laboral en su área de trabajo. Siendo el responsable de dicha asignación el Director del Área.
  - ✓ Cada equipo está preparado con el Hardware y Software básico necesario para su funcionamiento, el usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
  - ✓ En caso de presentar una falla física o lógica se deberá notificar al área de Informática y en el caso de ser requerido enviar el equipo para su revisión y/o reparación de acuerdo al procedimiento establecido.
  - ✓ En ningún caso el usuario intentará reparar el equipo o diagnosticarlo, únicamente informar de la posible falla.
  - ✓ El usuario será el único responsable del equipo de cómputo.
  - ✓ En ningún caso, el usuario tendrá cerca alimentos, bebidas u otros materiales que puedan derramarse sobre el equipo.
  - ✓ Solo se utilizará el equipo para funciones de interés del área y de ninguna manera para asuntos personales.
  - ✓ El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo del equipo de cómputo y periféricos básicos.
  - ✓ En caso de que el usuario no tenga conocimientos y/o experiencia, se notificará al área de sistemas para su correspondiente Capacitación.
  - ✓ La adquisición de equipo será con cargo al presupuesto de cada área o de la secretaria general, las características técnicas serán proporcionadas por el área de sistemas.
  - ✓ La solicitud del equipo de cómputo será responsabilidad del área interesada, bajo las características técnicas definidas por el área de sistemas e informando a las áreas relacionadas con la asignación de los recursos.

- ✓ Toda recepción de equipo de cómputo por adquisición o donación se realizará a través del Almacén.
- ✓ Por ningún motivo se deberá violar la etiqueta de control ya que cualquier daño o cambio al hardware será responsabilidad de la persona a quien este resguardado.
- ✓ En caso de que el funcionario tenga implementada una clave de acceso al equipo asignado, ésta tendrá que ser informada al personal de la oficina de Sistemas.

- **Software**

- ✓ Cada equipo contiene el software de acuerdo a las necesidades del área de trabajo, el cual siempre debe tener el respectivo licenciamiento.
- ✓ Por ningún motivo el usuario instalará software de promoción y/o entretenimiento.
- ✓ El software no puede ser utilizado por el usuario para realizar trabajos personales.
- ✓ La adquisición o desarrollo de software será responsabilidad del área de Informática.
- ✓ El personal asignado deberá comprobar sus conocimientos o experiencia en el manejo de los programas básicos de operación de PC's.

Responsabilidad del uso del recurso tecnológico

- El recurso tecnológico asignado a cada funcionario será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización del jefe inmediato y registro de la novedad en la minuta de vigilancia.
- Los Servidores Públicos a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garantizar la seguridad física del recurso tecnológico y salvaguardar la información.
- Los servidores públicos deben dar aviso de inmediato al Almacén, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.
- Los servidores públicos deben comunicar de manera inmediata a la dirección de recursos físicos cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos etc.
- La entidad recomienda a los usuarios que no deben consumir alimentos en áreas cercanas al recurso tecnológico.
- La entidad será la responsable de Administrar las hojas de vida del recurso tecnológico, en la cual se registre todos los componentes con sus seriales, placa del equipo y el software instalado con su número de licencia respectiva.

Operaciones Básicas

- Para encender el sistema de cómputo verifique que el monitor, CPU, impresora ydemás periféricos estén debidamente instalados entre sí y conectados a la corriente eléctrica.
- Enseguida identifique los interruptores o botones de encendido y apagado presione o mueva según se requiera.

- Encienda la Impresora, regulador/no-break, monitor, y demás periféricos que tenga

instalados dejando al final el CPU.

- Para apagar el sistema presione o mueva los interruptores según se requiera en el mismo orden antes mencionado (algunos equipos requieren que se mantenga presionado el botón unos segundos).
- Encender y apagar el Sistema: Al inicio y fin de las actividades, En caso de tormentas eléctricas, Si se presentan fallas eléctricas

Legalidad del Software

- Todo software instalado en equipos de la Entidad será autorizado o instalado por la Oficina de sistemas, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.
- Los Servidores públicos no deben instalar en los equipos de cómputo de propiedad de la entidad, Software no autorizado por la oficina de sistemas.
- La Oficina de sistemas será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

9.10. Políticas de seguridad de escritorio limpio y pantalla limpia

Política

Todos los funcionarios públicos, incluidos contratistas deberán conservar el puesto de trabajo y la pantalla del equipo de cómputo limpia de documentos, archivos o dispositivos de almacenamiento removibles.

Controles

- No deberán dejarse documentos críticos en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).

- Almacenar de forma segura documentos y elementos de almacenamiento externos

(CD, DVD, USB, etc.) en cajones bajo llave, con el fin de evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

- Conforme a los niveles de clasificación de la información de cada funcionario, los archivos o carpetas deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, evitando, por ejemplo, guardarlos en el escritorio del sistema de cómputo.
- La entidad, será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado y así proteger los equipos contra accesos no autorizados.

Imagen Institucional

- Todos los equipos podrán tener como imágenes predeterminadas aquellas que sean institucionales.
- En el exterior de todos los equipos se respetará la imagen física de empaque.
- Todos los accesorios de apoyo podrán tener plasmadas imágenes institucionales.
- Cada usuario es responsable del cuidado de su herramienta de trabajo. Por lo que se recomienda limpiar continuamente el equipo externamente.

9.11. Política sobre el suso de servidores

Política

- El área de sistemas es el responsable de verificar la instalación y configuración de todo servidor que sea conectado a la red, y de implementar mecanismos de seguridad física y lógica.

Controles

- Acceso restringido solo a personal autorizado.
- Temperatura adecuada para la cantidad de equipo.
- Cuenta con protección contra descargas eléctricas.

- Ubicación física en sitio libre de daño por humedad, goteras, inundaciones y demás efectos del clima.

9.12. Política de baja sistemas de información y/o software

Política

La oficina de sistemas a través de todo su equipo técnico es el responsable de verificar y establecer que sistemas de información y/o software con los que cuenta entidad, cumplen con los criterios para ser dados de baja en la entidad.

Controles

- Vencimiento de las licencias adquiridas con anterioridad que obliguen al comprador (Instituto Departamental de Transito del Quindío) a dar de baja el software.
- Cuando la versión del software se considera obsoleta, se procede a través de la oficina de sistemas a dar el correspondiente concepto técnico antes de dar de baja.
- Cuando la versión del software presenta problemas de seguridad que comprometan la entidad, se procede a través de la oficina de sistemas a dar el correspondiente concepto técnico antes de dar de baja.

10. CONTROL DE ACCESO

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales el Instituto Departamental de Transito del Quindío determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

10.1. Política de control de acceso y administración de contraseñas

Política

Las tareas realizadas por los usuarios en cada uno de los sistemas de información de la entidad, serán controladas por medio de la creación de cuentas de usuario en el dominio DIDTQ.COM de la entidad, los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles establecidos por el Instituto Departamental de Transito del Quindío.

Controles

- Cada funcionario o contratista de la entidad que deba usar una contraseña y un ID para alguno de los sistemas de información de la entidad, debe de dirigirse a la oficina de TI y solicitar la asignación de esta.
- Cada usuario es responsable de su id y contraseña y es único e intransferible, en caso de que se acabe su vinculación con la entidad debe reportarlo a la oficina de TI para cancelar su usuario y verificar que todo esté en orden.
- Los funcionarios que usen llaves digitales en la Entidad deben ser responsables de cualquier trámite que se haga con esta además es personal e intransferible y no debe prestarse ni compartirse.
- Cuando la llave Digital esta vencida por diferentes términos, se debe comunicar al director de TI para que se realice la operación correspondiente para la activación de esta.

- Las contraseñas serán Establecidas por cada funcionario o contratista de la entidad y

estas deben ser debidamente actualizadas. Con mínimo una mayúscula, un número y un carácter especial

- Ningún funcionario o contratista de la entidad, debe acceder a información de los servidores o bases de datos sin la debida autorización de la oficia TI.
- No se permite sacar o revelar información privada de la entidad a terceros.
- Cualquier documento físico que llegue o salga de la entidad debe ser solo recibido por la persona encargada de radicación y ella asignara a su funcionario correspondiente o realizara él envió de esta a el tercero.

Seguridad y Control

- El área de sistemas auditará de manera periódica los equipos de cómputo y periféricos, así como el software instalado.
- Cualquier salida y/o entrada de información tendrá que ser bajo la responsabilidaddel jefe inmediato.
- Por ningún motivo deberán usarse equipos que no sean propiedad del Instituto Departamental de Transito del Quindío.
- En caso de que el usuario utilice un equipo que no sea propiedad del Instituto Departamental de Transito del Quindío deberá notificar al área de sistemas y el responsable de la dependencia y deberá contar con la autorización de la secretaria general para su ingreso a la sede administrativa.
- Todos los equipos permanecerán en el lugar registrado por el área de almacén.
- Solo los equipos portátiles de propiedad del Instituto Departamental de Transito del Quindío podrán desplazarse con previa autorización del responsable de la dependencia y bajo la responsabilidad total del usuario.
- Todo servidor público es responsable de salvaguardar su información, y debe hacer copias de seguridad por lo menos una vez en el mes. Las copias deben ser debidamente rotuladas, y mantenerse en lugares seguros.
- Los contratistas deberán entregar copia de seguridad de la información producidaen

desarrollo de su objeto contractual, como requisito para la liquidación de su contrato.

- Los supervisores son responsables de verificar los medios magnéticos que reciben como producto o respaldo de objetos contractuales.

Áreas Protegidas

Para la selección y el diseño de un área protegida se tendrá en cuenta el riesgo o posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, y en lo posible se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas de la entidad:

- Datacenter Principal y Centros de cableado.
- Todas las áreas donde se almacene o procese información crítica de la Entidad.

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información debe ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
- Ubicar las funciones y la infraestructura tecnológica de soporte, por ejemplo: impresoras, fotocopiadoras, scanner, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

- Agregar protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
- Implementar mecanismos de control para la detección de intrusos, los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.
- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
- Almacenar los materiales peligrosos o combustibles en lugares seguros, a una distancia prudencial de las áreas protegidas de la entidad.
- Los suministros, como implementos de escritorio, no debe ser trasladados, ubicados o almacenados en las áreas protegidas.
- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

11. PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene la descripción y los controles que el Instituto Departamental de Transito del Quindío debe comprometerse con la privacidad y confiabilidad de la información suministrada tanto por usuarios, funcionarios y contratistas, manejar está bajo absoluta reserva y cumplir con lo establecido y en los siguientes principios.

Política

La entidad, adoptará una política de confidencialidad y protección de datos personales, con el objeto de proteger la privacidad de la información personal obtenida a través de sus diferentes sistemas de información, lo anterior buscando salvaguardar la privacidad y seguridad de la información personal del usuario que interactúa con los diferentes sistemas de información de la entidad.

Finalidad y tratamiento de los datos personales de los usuarios

- **Principio de la Legalidad:** El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- **Principio de finalidad:** Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- **Principio de libertad:** El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- **Principio de veracidad o calidad:** La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- **Principio de transparencia:** Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.

- **Principio de acceso y circulación restringida:** El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
- **Principio de seguridad:** La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- **Principio de confidencialidad:** Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

El tratamiento de los datos se realizará bajo las disposiciones contenidas en la ley 1581 de 2012 (Ministerio de tecnologías de la información y comunicaciones, 2013) y el decreto 1377 de 2013 (Ministerio de tecnologías de la información y comunicaciones, 2013) demás normas que los modifiquen, adicionen, sustituyan o complementen.

El tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con el Instituto Departamental de Transito del Quindío (incluye, entre otros, funcionarios, exfuncionarios, judicantes, practicantes y aspirantes a cargos).

El tratamiento de los datos se realizará para los fines relacionados con el desarrollo del proceso de gestión contractual de productos o servicios que requiera para su funcionamiento de acuerdo a la normatividad vigente.

Derechos de los titulares de los datos personales

- Conocer, actualizar y rectificar sus datos personales frente a la entidad, como responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada a entidad como responsable y encargado del tratamiento de los datos personales, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.
- Ser informado por el Instituto Departamental de Transito del Quindío como responsable del tratamiento y encargado del tratamiento de los datos personales, previa solicitud, respecto del uso que les ha dado a los datos personales del titular.

Procedimiento para ejercer los derechos

Consultas: Sobre la información de sus datos personales se absolverán en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuese posible responder la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su solicitud, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Reclamos: Los Titulares que consideren que la información contenida en una base de datos de la entidad debe ser objeto de corrección, actualización o supresión, o que adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la **Ley 1581 de 2012**, podrán presentar un reclamo ante el Instituto Departamental de Transito del Quindío, a través de cualquiera de los canales de comunicación con los que cuenta la entidad; y éste deberá contener la siguiente información:

- Nombre e identificación del Titular.
- La descripción precisa y completa de los hechos que dan lugar al reclamo.
- La dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite.

- Los documentos y demás pruebas que se pretendan hacer valer. En caso de que la entidad no sea competente para resolver el reclamo presentado ante el mismo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

- Si el reclamo resulta incompleto, la entidad requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el peticionario presente la información solicitada, se entenderá que ha desistido de aquél.

Datos sensibles en el tratamiento de datos personales

- El Titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la entidad, relacionada, entre otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

- Si el Instituto Departamental de Transito del Quindío en algún momento va realizar uso de datos de una persona debe primero buscar la autorización con la persona solicitada en este caso para el tratamiento de sus datos e información.

- En la entidad cualquier dato o información suministrada en los sistemas de información de la institución va estar bajo absoluta privacidad y confiabilidad, por el compromiso adquirido tanto de funcionarios y contratistas además del cumplimiento de este manual.

- La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información

interna y externa que conozca de la Entidad, así como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

12. INTEGRIDAD

El Instituto Departamental de Transito del Quindío está comprometido con el buen uso del manejo e integridad de la información suministrada y que haga parte de la institución sea de actores internos o externos te, mediante la cual debe ser cumplida por funcionarios y contratistas de la entidad.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el Compromiso de administración y manejo integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información.

13. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Dentro del Plan Estratégico de Tecnologías de Información (PETI), tenemos el plan maestro o mapa de ruta el cual incluye los proyectos o planes de continuidad en las secciones de gestión de información, con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

El IDTQ debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con los clientes, proveedores y/o terceros como lo son usuarios entre otros.

Velar por el cumplimiento de los acuerdos de nivel de servicio realizados con terceros para la disponibilidad de información de estos.

Se debe cumplir con la Gestión de cambios que se realice en cuanto a servicios de información y pautas establecidas por el comité de políticas de seguridad de la información.

14. REGISTRO Y AUDITORÍA

El área de control Interno y el comité de políticas de seguridad de la información, deben participar acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

La oficina de sistemas debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de las mismas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.

La auditoría debe velar de que las mismas sean realizadas acorde a la normatividad y requerimientos legales aplicables a la naturaleza de la Entidad.

La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.

Periodicidad: La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de, auditorías periódicas alineadas a los objetivos estratégicos y gestión de procesos de la entidad que se deben realizar cada seis meses como mínimo.

15. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Grupo/Proceso de sistemas por cualquiera de los medios dispuestos para tal fin.
- Si ocurre cualquier incidente con los activos de información o seguridad de la misma debe comunicarse inmediatamente al jefe de oficina de sistemas de la entidad puede hacerse de forma manual o electrónica.
- El único encargado de solucionar o saber que hacer en el caso de estos incidentes es el jefe de oficina de sistemas de la entidad ningún funcionario o contratista debe solucionarlos.
- Se debe realizar un documento de gestión de reportes de incidentes para un inventario y una documentación clara de lo que ha pasado y la manera en se ha solucionado.
- El jefe de oficina de sistemas será el encargado de comunicar la Gestión de Incidentes al Comité de políticas de seguridad.

Fuente: autoría propia

16. CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- Todos los funcionarios y contratistas de la entidad deben tener presente este manual de políticas de seguridad de la información.
- Realizar un espacio de capacitación para compartir la información aquí establecida con todos los funcionarios de la entidad.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.

- La comunicación se realizará por parte del comité de políticas de seguridad de la información de la entidad.
- Los funcionarios y contratistas de la entidad deben cumplir con ya lo establecido dentro de este manual.
- Actualizar el manual cada seis meses y realizar su respectiva comunicación de la actualización con los funcionarios y terceros.

Adicionalmente se diseña un flyer publicitario, donde se realiza la descripción a modo general de la política de seguridad y privacidad de la información. *Ver ilustración 3*

Ilustración 3. FLYER PUBLICITARIO POLÍTICA

Fuente: autoría propia

17. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

El Instituto Departamental de Transito del Quindío indica que realizará revisiones periódicas al Sistema de Gestión de Seguridad de la Información. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

18. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro del Instituto Departamental de Transito del Quindío.

La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.

19. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal del Instituto Departamental de Transito del Quindío de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a) Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.

b) Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

c) El Grupo TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

20. BIBLIOGRAFÍA

- International Organization for Standardization. (2014). Tratamiento de la seguridad en contratos con terceros. Retrieved from https://iso27002.wiki.zoho.com.
- Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (2006, 04 03). NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Bogotá, Colombia.
- Ministerio de Tecnologías de l Información y Comunicaciones MinTIC. (2018, junio 14). MinTIc. Bogotá DC, Colombia.
- Ministerio de tecnologías de la información y comunicaciones. (2013, Junio 23). Decreto 1377 de 2013. Retrieved from http://www.mintic.gov.co/portal/604/articles - 4274_documento.pdf.
- Ministerio de Tecnologías de la información y comunicaciones. (2017). Decreto1413 del 2017. Bogotá D.C, Colombia.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Bryan Johann Aranzazu Medina Cargo: Ingeniero Contratista Fecha: 19-04-2023	Nombre: Jorge Mauricio Pardo Ruiz Cargo: Contratista Oficina Sistemas Fecha: 30-01-2024	Nombre: John Freddy Villalba Valencia Cargo: Profesional Oficina Sistemas Fecha: 31-01-2024