POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

GOBERNACIÓN DEL QUINDÍO

2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La estrategia de Gobierno en 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 la gobernación 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 la gobernación 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 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, 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.

Conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte tecnológico y legal de la Alta Dirección, y con el objetivo que estas sean una herramienta para

la definición de los estándares y procesos internos de la gobernación del Quindío, la Secretaría TIC, debe asegurar que la información disponible cumpla con los criterios de Confidencialidad, Integridad, Disponibilidad, Accesibilidad, Autenticidad, entre otros, mediante el resguardo de datos, la protección frente a accesos no autorizados, el control de acceso a otros sitios web, la adecuada utilización del correo electrónico de la Entidad, entre otros, lo anterior acorde al modelo de seguridad y privacidad de la información “MSPI”, correspondiente al eje transversal de seguridad de la información planteado por la política de gobierno digital.
Así mismo, proporcionar hardware, software y equipos de comunicaciones en condiciones de seguridad y calidad; realizar revisiones periódicas de seguridad; y garantizar la propiedad de la Información y la buena manipulación de programas de software aplicativo.

Este documento describe las políticas, normas y lineamientos técnicos de seguridad de la información definidas por la gobernación del Quindío para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la gobernación del Quindío y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

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 de la gobernación de Quindío.

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Secretaría TIC (secretario TIC o director de sistemas en su defecto), 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 de la gobernación 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

- **Seguridad de la información (SGSI):** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad (Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2006).

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad:** Condición que garantiza que la información consignada en un documento ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación (Ministerio de Tecnologías de la información y comunicaciones, 2017).

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **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.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **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).

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

- **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 llevara cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumplecon 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

Las políticas de seguridad de la Información de la Gobernación del Quindío se ciñen a la normatividad legal vigente colombiana, tal como se describe a continuación:

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, entre otros, 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 manejo de 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 información para "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 los sistemas que utilicen las tecnologías 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 a desarrollar 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. POLÍTICAS DE SEGURIDAD

La Secretaría TIC de la gobernación del Quindío, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación del modelo de seguridad y privacidad de la información, el cual busca establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la gobernación 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 la misma, 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 de la gobernación del Quindío.
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, se establecen 12 principios de seguridad que soportan el MSPI de la gobernación del Quindío:

- La gobernación del Quindío **protegerá la información** generada, procesadao 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 **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.

- La gobernación del Quindío **protegerá su información** de las amenazas originadas por parte **del personal**.

- La gobernación del Quindío **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

- La gobernación del Quindío **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La gobernación del Quindío **implementará control de acceso** a la información, sistemas y recursos de red.

- La gobernación del Quindío garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La gobernación 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.

- 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.

- La gobernación del Quindío garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

6.1 Política y Controles de Organización Interna

La gobernación del Quindío y su nivel directivo conoce y apoya la necesidad de contar con políticas de seguridad que sirvan como soporte y apoyo a los procesos institucionales. Por tal motivo se debe de tener en cuenta las siguientes recomendaciones:

- Creación de un comité de seguridad interdisciplinario conformado por el Secretario TIC, Director de sistemas de información e infraestructura tecnológica, Jefe oficina Jurídica, Director de recursos físicos, director de recursos humanos, profesional universitario responsable del archivo y un profesional universitario responsable de control disciplinario, quienes serán los encargados de tratar los temas concernientes a la seguridad de la información, formulando su propio reglamento, en el cual establecerán responsabilidades, funciones y periodicidad de las reuniones. Actuarán como invitados permanentes los administradores de los diferentes sistemas de información.

- Asignación de un responsable de la seguridad de la información (Oficial de seguridad) que vele por el cumplimiento de las políticas establecidas en este documento.

- Aprobación bajo acto administrativo el documento de políticas de seguridad de la información.

- Realización de reuniones periódicas donde se verifique el cumplimiento de las políticas, donde se hagan propuestas y se analicen las nuevas con el fin de mejorar las mismas.

6.2 Roles y responsabilidades

Comité de Seguridad de la Información

- 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 el organismo.

- Formular y mantener una política de seguridad de la información que aplique a toda la organización conforme con lo dispuesto por la gobernación del Quindío.

Director de Talento Humano

El director de talento humano cumplirá la función de notificar a todo el personal que se vincula por nombramiento o contractualmente con la gobernación del Quindío, de las obligaciones respecto del cumplimiento de la política de seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del sistema de gestión de la seguridad de la Información.

De igual forma, será responsable de la notificación de la presente política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los compromisos de confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

Director de Recursos Físicos

El director de recursos físicos cumplirá la función de vigilar y mantener la infraestructura física de la entidad, con el fin de salvaguardar la información. Será el encargado de implementar controles físicos, con el fin de minimizar los riesgos de amenazas físicas y ambientales como robos, incendios, agua, vandalismo, etc.

Por otra parte, deberá implementar los controles que crea necesarios a las instalaciones sensibles a accesos de información, tales como el data center de la gobernación del Quindío.

Por último, deberá ejercer control físico y/o electrónico sobre todas las personas que ingresan a las instalaciones de la gobernación del Quindío, dichos controles abarcan desde empleados de planta pasando por contratistas y visitantes.

Secretario TIC

cumplirá la función de darle continuidad al modelo de seguridad y privacidad de la información (MSPI), así como también de proponer cambios en dicho modelo,

generar el plan de continuidad del negocio, asignar responsabilidades dentro de la matriz de riesgos de la entidad y especificar los planes de respuesta al riesgo ante alguna eventualidad que pueda llegar a suceder.

Director de Gobierno digital

El secretario TIC cumplirá la función de darle continuidad a las políticas de información aquí generada, así como también proponer cambios en dichas políticas, generar el plan de continuidad del negocio, asignar responsabilidades dentro de la matriz de riesgos de la entidad y especificar los planes de respuesta al riesgo ante alguna eventualidad que se identifique.

El director junto con el director de asuntos jurídicos, conceptos y revisiones, tendrá la responsabilidad de generar los acuerdos de confidencialidad, tratamiento de la información y demás documentación legal a los que se haga responsable tanto empleados, contratistas y/o empresas que presten los servicios a la gobernación del Quindío y que manejen datos susceptibles de la entidad.

Director de sistemas de información e infraestructura tecnológica

El director de sistemas velará por el cumplimiento de las políticas de la información en la gobernación del Quindío, ejercerá los controles que crea necesarios en los sistemas informáticos de la entidad, propondrá nuevos controles y será el encargado de darle seguimiento a las políticas de seguridad relacionados con la protección digital de los datos de la entidad.

Director de Asuntos Jurídicos, Conceptos y Revisiones

El director de asuntos jurídicos, conceptos y revisiones, verificará el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información**.**

Jefe de la oficina de control interno

El jefe de la oficina de control interno cumplirá la función de vigilar y ejercer los controles disciplinarios necesarios para que los funcionarios de la gobernación del Quindío cumplan a cabalidad lo dispuesto en el documento de políticas de seguridad de la información.

6.3 Políticas para los servicios de procesamiento de la información

La Secretaría TIC de la gobernación del Quindío, será la encargada de velar y custodiar los activos tecnológicos tangibles e intangibles con los que cuenta la gobernación del Quindío, 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

La gobernación 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 secretario TIC, director de Sistemas de información e infraestructura tecnológica y las dependencias involucradas con la finalidad del mismo. Dicho software debe seguir las fases del ciclo de vida de los sistemas de información y deberá ser testeado por los funcionarios de la Secretaría TIC y los funcionarios de las dependencias que utilizarán el software.

Control de cambios

Al momento que una dependencia de la gobernación del Quindío requiera alguna modificación, estructural o no, sobre el software aplicativo y si el proceso involucra más de una dependencia, es necesario que la solicitud de modificación esté autorizada mediante escrito por los secretarios de despacho y personas responsables de la ejecución del proceso y el secretario TIC de conformidad con el procedimiento establecido.

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 a en las salidas de información, supervisados y autorizados por el director de sistemas

y el responsable del proceso.

6.4 Política de confidencialidad de la información

Todos los servidores públicos de la gobernación 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, so pena de las investigaciones penales y disciplinarias a las que haya lugar.

Controles

La gobernación 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 misma y que se respeten los derechos de autor.

6.5 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.

7. GESTIÓN DE CONTROL DE ACTIVOS

7.1 Políticas de creación y restauración de copias de seguridad

La gobernación del Quindío a través de la Secretaría TIC ha identificado los procesos operativos o 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 Secretaría TIC.

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 Sevenet, PCT, Siscar, Siscar Web, Estampilla Pro-hospital y pagina web e intranet, 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 como sevenet (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.

- La Secretaría TIC 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 Secretaría TIC, 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.

- La Dirección de Recursos Físicos proveerá a las Dependencias de las herramientas o recursos necesarios para efectuar las copias de seguridad.

- La Secretaría TIC conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas.

7.2 Políticas para el manejo de datos

7.2.1 Uso Compartido

Política

El usuario o funcionario de la gobernación 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 de la gobernación del Quindío que autoriza la carpeta compartida debe delimitar a los usuarios que realmente la necesitan y controlar el tiempo en el cual estará expuesta.

- El usuario o funcionario de la gobernación del Quindío que autoriza la carpeta compartida debe asegurarse que el usuario autorizado cuente con el antivirus autorizado.

7.2.2 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 Dirección de TIC de la gobernación del Quindío.

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 Secretaría TIC para que le brinden el soporte técnico de erradicación del virus.
- El equipo de trabajo de la dirección de sistemas de información e infraestructura tecnológica de la secretaria TIC es responsable por la actualización oportuna del software antivirus.

7.2.3 Dominio DQuindio

Política

Todos los equipos de propiedad de la gobernación del Quindío deben estar dentro del dominio Dquindio.com, el cual será administrado desde la Secretaría TIC de la entidad.

Controles

- El personal de la Secretaría TIC de la gobernación del Quindío, deberá conectar a los equipos de los funcionarios, vigilarlos y administrar los permisos de cada equipo, según lo designado por el director de sistemas de la entidad.
- Está prohibido que algún equipo de pertenencia de la entidad este por fuera

del dominio.

- Las políticas de contraseñas de administrador del dominio, por motivos de seguridad solo las conocerán los funcionarios de la Secretaría TIC.

- Las contraseñas de los equipos de los funcionarios serán suministradas por el administrador del dominio el cual es designado por la Secretaría TIC.

- 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 comprados por la entidad deberán tener soporte a redes, con el fin de conectarlos al dominio de la gobernación del Quindío.

7.2.4 Bases de datos

Política

El o los administradores(es) de las bases de datos de la gobernación 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 del director 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 pistas de auditoría deben permitir monitorear las conexiones a las bases de datos, las modificaciones al modelo de datos y las modificaciones a los datos, de manera directa o por medio de aplicativos.

- 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 deberá realizado por el personal autorizado por el director de sistemas, previa firma de un documento que garantice la confidencialidad y privacidad de la información.

7.3 Estrategia de preservación de archivos

Política

La Secretaría TIC 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 dependencias de la Entidad.

- La Secretaría TIC 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.

- La Secretaría TIC, 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:

    - Independencia del dispositivo: Debe ser representado de manera fiable en cualquier plataforma software o hardware.
    - Auto contenido: Debe contener todos los recursos necesarios para su representación.
    - Autodocumentado: Debe contener su propia descripción
    - Sin restricciones: No debe haber mecanismos de protección del fichero.

- Disponible: Especificación accesible cuando se requiera.
- Adoptado: Un uso amplio contra los riesgos de la preservación

- Cada vez que la Entidad obtenga nuevas versiones de software que involucren operaciones transversales, es importante por medio de la Secretaría TIC implementar un plan de migración en serie para facilitar la conversión en tiempo real.

- Cuando se adquieran nuevos equipos de almacenamiento y no acepten soportes de archivos antiguos, se debe realizan un procedimiento de verificación mediante MD5 dígitos de control, para asegurar la autenticidad e integridad de los soportes posterior al proceso de refreshing.

- La Entidad por intermedio de la Secretaría TIC y la oficina de gestión documental deberá garantizar la disponibilidad e integridad de los metadatos de los documentos y expedientes electrónicos, manteniendo de manera permanente las relaciones entre cada documento o expediente y sus metadatos.

- La dirección 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.

- La Secretaría TIC a través del plan de tratamiento de riesgos deberá realizar un seguimiento a los riesgos identificados que afecten la integridad de los archivos.

7.4 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

allí y que por algún motivo sea modificada o borrada por accidente, no involucra ni compromete a la Secretaría TIC en ningún caso.

Controles

- Los medios de almacenamiento con información crítica deberán ser manipulados y enviados al tercero única y exclusivamente por la persona asignada por la Secretaría TIC 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.

- No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Entidad, en lugares de acceso público como cibercafés, puntos vive digital o en equipos que no garanticen la confiabilidad e integridad de la información.

- 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.

7.5 Políticas de uso del correo electrónico

Política

La Secretaría TIC es la encargada de definir los nombres, estructura y plataforma que se debe utilizar para la cuenta de correo Institucional de cada dependencia o secretaria de la gobernación del Quindío.

Controles

Administración del Correo Institucional

- El uso del correo institucional es de carácter corporativo, siendo responsabilidad de los secretarios y directores su administración y control.

- Los secretarios y directores podrán delegar por escrito al funcionario que se encargará de la administración del correo.

- El tamaño del buzón, de los archivos enviados y del contenido del correo será definido por la Secretaría TIC.

Cambio de Contraseñas a Correos Institucionales

- En el mismo instante en que la Secretaría TIC cree y dé a conocer de la cuenta de correo Institucional designada para cada dependencia 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.

Exoneración de responsabilidades

- La Secretaría TIC definirá el texto de exoneración de responsabilidad que se debe incluir en los correos electrónicos, para proteger a la entidad de los contenidos de los correos electrónicos.

7.6 Políticas de acceso a internet e intranet

Política

En la gobernación del Quindío el acceso a Internet e Intranet es permitido a todos los servidores públicos para facilitar el desarrollo de los procesos propios de la Entidad, no obstante, los equipos de contratistas o personas ajenas a la entidad, deberán conectarse a una red distinta de la red local de la entidad, esta será suministrada por la Secretaría TIC.

Controles

Creación de Perfiles

La Secretaría TIC creará dos (2) perfiles de usuario con los cuales se pretende controlar el acceso a internet, descongestionar el ancho de banda y garantizar la seguridad de la información.

- Perfil No 1 VIP: Corresponde a usuarios con funciones y/o permisos para navegar en sitios no autorizados por la gobernación del Quindío.

- Perfil No 2. General: Usuarios en general, normalmente se les asigna a todos los funcionarios de la gobernación del Quindío y el cual tendrá restringido de manera predeterminada las redes sociales y el streaming de video.

- Para solicitar el acceso al perfil VIP donde se le asigne permiso a cualquier funcionario para navegar en sitios no autorizados, el funcionario o correspondiente deberá solicitarle al secretario de despacho de la dependencia que dirija un oficio a la Secretaría TIC, haciendo referencia a la solicitud anteriormente mencionada.

- La Secretaría TIC 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.

Asignación IP: La Secretaría TIC deberá tener en un archivo el registro de asignación y control del direccionamiento IP de cada uno de los equipos conectados que forman parte de la red con acceso a internet de la gobernación del Quindío, el cual deberá contener la siguiente información:

1. Nombre del funcionario
2. Placa del equipo
3. Dependencia

Finalidad del uso de internet: los canales de acceso a internet de la entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos de cada funcionario. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la gobernación del Quindío o de las personas.

La entidad se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

Uso de la Intranet

- Las cuentas de acceso a Intranet serán administradas por la Secretaría TIC y serán creadas para el personal de planta de la entidad.

- El personal de contrato por prestación de servicios de apoyo a la Gestión y Profesional podrán ser usuarios de la Intranet con previa autorización del secretario TIC, con previo oficio escrito por el secretario de despacho de la dependencia donde se desempeña el funcionario.

- Para el uso de Intranet se deben observar las mismas normas de comportamiento definidas para el uso de internet.

7.7 Políticas de publicación en el portal web

Administración de los Contenidos Institucionales de las Páginas:

- La administración de los contenidos de las páginas institucionales estará a cargo de cada funcionario de cada dependencia, previamente designado por el secretario de despacho, 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 copiar y utilizar en otros sitios WEB.

Editores de los Contenidos Institucionales de las Páginas:

- 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 Secretaría TIC para el manejo de la estrategia de gobierno en línea, dentro de sus funciones deberá capacitar a los funcionarios para el cargue y administración de la información que se cargue a la página web institucional.

- Solo el funcionario designado por la Secretaría TIC tendrá contraseñas de administrador del portal web.

- La empresa encargada del dominio y hosting de la gobernación del Quindío tendrá contraseñas de superusuario, pero dentro de sus funciones estará supeditada a cláusulas de confidencialidad de la información.

7.8 Políticas de dispositivos móviles

Política

La gobernación 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 que se encuentran en cada piso de la gobernación del Quindío.

Controles

- Aunque se permite el acceso a la red wi-fi de la gobernación del Quindío 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.

- Solo los(as) secretarias(os) de cada dependencia tendrán las contraseñas de cada piso.

- La Secretaría TIC 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.

7.9 Políticas de adquisición y mantenimiento de software y hardware

Política

Toda adquisición de recurso tecnológico en la gobernación del Quindío deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte de la Secretaría TIC, el proceso deberá ser supervisado por el director de sistemas.

Política de software

La gobernación del Quindío en cabeza de la Dirección de TIC protegerá la propiedad intelectual propia y de terceros. El software registrado con derechos de autor, el cual no se podrá copiar sin previa autorización del propietario.
Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.

Controles

Adquisición de equipos tecnológicos

- La Dirección de TIC a través del liderazgo del director de sistemas, verificará las características y el estado de todos los equipos tecnológicos que ingresan a la Gobernación del Quindío, previo al ingreso a almacén.

- 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

- Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos.

- El Servidor Público que requiera soporte técnico debe dar aviso a la Secretaría TIC a través de la mesa de ayuda, para que allí el encargado envíe el personal especializado a diagnosticar el equipo; en caso de que se presente un daño mayor, el funcionario deberá autorizar el envió del equipo a la Secretaría TIC, autorizado al personal de dicha dirección para que realice lo necesario para el mantenimiento correctivo.

- Se deberá brindar el servicio de atención de emergencia ante un desperfecto presentado en cualquier equipo de la gobernación del Quindío, para este servicio se requerirá realizar una solicitud por la aplicación mesa de ayuda, y dependiendo de la gravedad del problema se le deberá dar prioridad a las solicitudes más urgentes y/o importantes.

- Cuando el equipo de cómputo necesite ser reseteado por alguna razón, el funcionario a cargo del equipo deberá firmar una autorización por escrito (formato de autorización formateo) y validar la copia de seguridad de los datos que realiza el funcionario de la Secretaría TIC, para que este luego pueda restaurar los archivos.

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 Secretaría TIC recomienda a los usuarios que no deben consumir alimentos en áreas cercanas al recurso tecnológico.

- La Secretaría TIC 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

Legalidad del Software

- Todo software instalado en equipos de la Entidad será autorizado o instalado por la Secretaría TIC, 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 gobernación del Quindío, Software no autorizado por la Secretaría TIC.

- El secretario de despacho responsable de su dependencia asumirá la responsabilidad por el software instalado en el computador que le sea

asignado o que esté utilizando. Toda aplicación que esté instalada debe estar debidamente licenciada.

- La Secretaría TIC será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

Sistemas operativos

- Aunque la gobernación del Quindío cuenta con diferentes tipos de sistemas operativos de Microsoft, estos tienen activados las actualizaciones automáticas para mantener los equipos seguros.

- Los equipos servidores o los que hagan sus veces, deben contar con el software para realizar el chequeo de integridad del sistema operativo y del hardware (OCS inventory). La periodicidad de su ejecución estará definida por la persona o grupo de informática designados para ello. Esto aplica para todos los equipos de cómputo de propiedad de la gobernación de Quindío. (ej.: equipos de escritorio y portátiles).

7.10 Política 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

- La gobernación del Quindío, a través del comité de seguridad de la información y el director de sistemas de la entidad remendará y vigilará a los funcionarios públicos que tengan equipos de la gobernación del Quindío, a que adopten buenas prácticas en el manejo y administración de la información física y electrónica a su cargo, conforme a su clasificación, con el fin de evitar el acceso a personas no autorizadas.

- 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.

- Una vez culmine el proceso de impresión o copiado, los documentos deberán ser retirados por el funcionario responsable de forma inmediato.

- 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.

- Los funcionarios, contratistas y terceros de la Gobernación del Quindío serán los responsables del buen uso de la información tanto física como lógica, y del cumplimiento de los lineamientos determinados en esta política.

- Los equipos de cómputo y lugares de trabajo podrán ser revisados y auditados por las áreas de control que determine la Gobernación del Quindío, a fin de validar el cumplimiento de la presente política.

- La Secretaría TIC, 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.

7.11 Política sobre el uso de servidores

Política

El director 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

Los servidores están ubicados en el data center de la gobernación del Quindío, la cual cumple con las siguientes características:

- 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.

Funcionalidad y mantenimiento de Servidores: Todo servidor que proporcione servicios a través de la red debe:

- Funcionar las 24 horas al día los 365 días del año.
- Tener mantenimiento preventivo mínimo dos veces al año.
- Ser objeto de Mantenimiento semestral donde se realizará la depuración de bitácoras.
- Hacerle revisión de su configuración anual.
- Ser Monitoreado diariamente por la persona encargada o director sistemas de la Secretaría TIC.

7.12 Política de baja sistemas de información y/o software

Política

El director 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 La gobernación del Quindío, cumplen con los criterios para ser dados de baja en la entidad.

Controles

- La dirección de sistemas de información e infraestructura tecnológica será la encargada de determinar que equipos de cómputo y/o software poder ser dados de baja, lo anterior cumpliendo con los siguientes criterios:
    - Vencimiento de las licencias adquiridas con anterioridad que obliguen al comprador (gobernación del Quindío) a dar de baja el software.
    - Cuando la versión del software se considera obsoleta, se procede a través de la dirección 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 dirección de

sistemas a dar el correspondiente concepto técnico antes de dar de baja.

- Cuando se identifica que el software instalado en algún sistema de información infringe los derechos de autor.

8. CONTROL DE ACCESO

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales la gobernación 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.

8.1 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 gobernación del Quindío, serán controladas por medio de la creación de cuentas de usuario en el dominio DQUINDIO.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 la Secretaría TIC.

Controles

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información:

1. Nombre completo del funcionario que utilizará el equipo y/o que pertenece el equipo en el inventario.
2. Correo electrónico para notificación de Contraseñas.
3. Tipo de Permiso (VIP, general)
4. Tipo de vinculación: (Personal de Planta o Prestación de Servicios).
5. En caso de solicitar acceso a aplicativos especiales se debe especificar por cada uno de ellos los permisos a los que va a tener derecho.
6. Los permisos deben ser solicitados por el Director o secretario responsable de cada uno de los módulos.

Cambio Forzoso de Todas las Contraseñas del Administrador

Siempre que se detecte un ingreso no autorizado al sistema de información, con la contraseña de administrador, la Secretaría TIC deberá cambiar inmediatamente cada una de sus contraseñas en el sistema, con el fin de que se viole la seguridad e integridad de los datos.

Cambios de Contraseñas Periódicas para el Administrador

El o el administrador (es) deben cambiar periódicamente la contraseña en el sistema (dominio de la gobernación del Quindío).

Control de Acceso al Sistema con contraseña Individual para cada Usuario

- Se precisa que el control de acceso al cualquier equipo de la gobernación del Quindío, se debe realizar por medio de usuario único, controlado por la Secretaría TIC a través del dominio, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

- La Dirección de Talento Humano reportará a la Secretaría TIC el traslado o retiro de los servidores públicos, a fin de ejercer control sobre el estado de los usuarios.

- La Secretaría TIC bloqueará desde el dominio el acceso a los equipos en los siguientes horarios:

    - Lunes a viernes de 9:00 pm a 7:00 am del siguiente día.
    - Sábados: de 4:00 pm en adelante.
    - Domingos: Todo el día.

- La dirección de recursos físicos informará a la Secretaría TIC del acceso a funcionarios a la entidad en horarios no permitidos, lo anterior con el fin de habilitar dicho usuario para trabajar en el horario.

- Los equipos que se encuentran en el dominio de la gobernación del Quindío se deberán bloquear cada cinco (5) minutos que pasen de tiempo de inactividad, lo anterior para evitar acceso no autorizado de alguna persona al equipo.

Entrega de Contraseñas a Usuarios

Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico o través de la mesa de ayuda.

Confidencialidad de las contraseñas

- Las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

- Los servidores públicos serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Visualización de mensaje a personal no autorizado

El dominio DQUINDIO deberá generar un mensaje en todos los equipos de la gobernación del Quindío, cuando este se bloquee por tiempo de inactividad, este mensaje debe advertir que solo los usuarios autorizados pueden acceder al equipo.

8.2 Política de seguridad de control de acceso físico

Política

El acceso a las instalaciones físicas de la gobernación del Quindío deberá ser supervisado por controles acceso físico y electrónico, que garanticen la integridad de la información que se maneja en las diferentes dependencias de la entidad.

Controles

Controles de acceso físico

- Para el ingreso a las instalaciones de la gobernación del Quindío se deberá inspeccionar por parte del personal autorizado a los visitantes de manera que se ejerzan controles físicos a todas las personas.

- Se deberá implementar controles de manera física y electrónica en los que se puedan registrar la fecha, el horario de ingreso o egreso de cualquier

visitante, dichos controles se realizaran mediante torniquetes los cuales funcionan con control de acceso biométrico.

- Para el acceso de funcionarios de la planta del personal y contratistas de la gobernación del Quindío, se deberá registrar la huella, junto con los datos personales, foto y dependencia donde labora.

- El control de acceso a los visitantes se realizará diariamente, registrando la huella de la persona, el tiempo de instancia de la persona en el edificio será controlado en los siguientes horario lunes a viernes de 8:00 a 12:30 pm y de 2:00 pm a 7:00 pm.

Controles de acceso físico a lugares protegidos

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, lo que debe ser determinado por el director de sistemas y el director de recursos físicos, a fin de permitir el acceso sólo al personal autorizado.

Estos controles de acceso físico deben tener, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso justificando propósitos específicos y autorizados e informando al visitante en el momento de ingreso, sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

- Deberá existir una bitácora de ingreso, en el cual se registre la fecha la hora de entrada y la hora de salida a los lugares restringidos (como data center).

- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

- Revisar y actualizar cada tiempo determinado (no mayor a 6 meses), los derechos de acceso a las áreas protegidas, los que debe ser documentados y firmados por el responsable del área organizacional de la que dependa y el comité de seguridad de la información.

- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Áreas protegidas

Para la selección y el diseño de un área protegida se tendrá en cuenta y 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 gobernación del Quindío:

- Datacenter Principal.
- Centros de cableado de cada piso.
- 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 gobernación del Quindío.
- 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.

9. PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene la descripción y los controles que la gobernación del Quindío realiza en el tratamiento de los datos personales. Dicha política está reglamentada conforme a la normatividad vigente.

9.1 Política de tratamiento de datos personales

Política

La gobernación del Quindío, 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 al cual serán sometidos los datos personales de los usuarios

En relación con la naturaleza y las funciones propias de la gobernación del Quindío:

- El tratamiento de los datos se realizará con la finalidad de las funciones propias del departamento, en las disposiciones contenidas en la ley 1581 de 2012[1] (Ministerio de tecnologías de la información y comunicaciones, 2013)y el decreto 1377 de 2013[2] (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 departamento 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 el proceso de gestión contractual de productos o servicios que la practicante requiere 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 gobernación del Quindío, 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 la gobernación del Quindío 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 departamento 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.

- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la superintendencia de industria y comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la ley 1581 de 2012 y a la constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

[1] "Por la cual se dictan disposiciones generales para la protección de datos personales"
[2] "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

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 fuere 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 o sus causahabientes que consideren que la información contenida en una base de datos del departamento 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 la gobernación 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 gobernación del Quindío 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 gobernación del Quindío 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.

- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo, y si no fuere posible responder en dicho término, la gobernación del Quindío informará al interesado los motivos de la demora y la fecha en que aquél se atenderá, sin llegar a superar, en ningún caso, los ocho (8) días hábiles siguientes al vencimiento del primer término.

Datos sensibles en el tratamiento de datos personales

- El Titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la gobernación del Quindío, 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.

Autorización del titular de los datos personales

- Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Casos en los que no se requiera autorización del titular de los datos personales

La autorización del titular no será necesaria cuando se trate de:

- Información requerida por la gobernación del Quindío en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el registro civil de las personas.

10. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Este ítem se evalúa el impacto potencial que provoca la interrupción parcial o total de los servicios electrónicos y procesamiento de la información, sobre el normal desarrollo de las actividades de la GOBERNACION DEL QUINDIO; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

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 gobernación del Quindío, ante el evento de un incidente de seguridad de la información, la entidad ha creado un plan de contingencias y continuidad del negocio el cual tiene como objetivo general plantear y dotar a la gobernación del Quindío de los procedimientos y elementos mínimos requeridos para afrontar alguna contingencia relacionada con el eventual cese de actividades, inoperatividad de equipos causada por razones de fuerza mayor y de diferente índole (Secretaria TIC, Gobernación del Quindío, 2016).

11. 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. (2013, Junio 23). *Decreto No 1377 de 2013.* Retrieved from https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

- Ministerio de tecnologías de la información y comunicaciones. (2015). Decreto 1078 de 2015. MinTic.
- Ministerio de Tecnologías de la información y comunicaciones. (2017). Decreto1413 del 2017. Bogotá D.C, Colombia.
- Ministerio de tecnologías de la información y comunicaciones. (2017). *estrategiade gobierno en línea*. Retrieved from http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html
- Secretaria TIC, Gobernación del Quindío. (2016). Plan de contingencias y continuidad del negocio. Armenia, Quindío, Colombia.
- Universidad del Cauca. (2017). *Conceptos básicos de sistemas de información*. Retrieved from http://fccea.unicauca.edu.co/old/siconceptosbasicos.html

ELABORACIÓN	REVISIÓN	APROBACIÓN
Elaborado por Equipo Gobierno Digital	Revisado por: Jairo Andres Silva	Aprobado por: Héctor Fabio hincapié
Cargo: Contratista	Cargo: Director Gobierno Digital	Cargo: Secretario TIC

CONTROL DE CAMBIOS			
VERSION	**FECHA**	**DESCRIPCION DE LA MODIFICACION**	**FUNCIONARIO**
VERSION 1	15/05/2018	Creación primera versión deldocumento	Ing. Andrés Felipe Barrera - Contratista
VERSION 2	21/05/2019	Creación de la Política de preservación de archivos electrónicos	Ing. Andrés Felipe Barrera - Contratista
VERSION 3	17/02/2021	Creación de la política de baja de sistemas de información y/o software. Cambio de logos	Ing. Andrés Felipe Barrera - Contratista
VERSION 4	31/01/2022	Revisión general del documento y normalización bajo el código POL-TIC-01	Ing. Bryan Johann Aranzazu Medina – Director de Gobierno digital
VERSION 5	12/06/2024	Revisión y actualización integral	Equipo gobierno digital