PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD, PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Gobernación del Quindío
2025

TABLA DE CONTENIDO

TABLA DE TABLAS

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

En un mundo cada vez más interconectado y dependiente de tecnologías digitales, garantizar la seguridad y privacidad de la información se ha convertido en una prioridad estratégica para las organizaciones públicas. En este contexto, el Gobierno del Quindío, como ente rector del desarrollo regional, reconoce la importancia de adoptar medidas efectivas para la protección de los datos, la mitigación de riesgos digitales y la construcción de una cultura de seguridad integral.

Este Plan de Gestión de Riesgos de Seguridad, Privacidad de la Información y Seguridad Digital está diseñado como una guía estructurada y dinámica que permite identificar, evaluar y gestionar los riesgos propios de la era digital. Su principal objetivo es fortalecer la confianza de los ciudadanos en los servicios y sistemas ofrecidos por la entidad, garantizando la confidencialidad, integridad y disponibilidad de la información.

A través de un enfoque basado en buenas prácticas internacionales, normativas nacionales como la Ley 1581 de 2012 (Protección de Datos Personales) y estándares reconocidos como ISO/IEC 27001, este plan busca integrar la seguridad digital en todos los niveles de gestión. Esto promueve un entorno tecnológico resiliente frente a amenazas emergentes y asegura que el Gobierno del Quindío sea un modelo de gobierno transparente, innovador y seguro, comprometido con la transformación digital y el bienestar de sus ciudadanos.

La gestión de riesgos en este contexto implica un enfoque estratégico y proactivo que abarca la identificación, evaluación, mitigación y monitoreo continuo de los riesgos asociados a los activos de información. Estos activos, fundamentales para la misión institucional, representan un patrimonio crítico cuyo resguardo es prioritario. Las estrategias incluyen tanto la prevención como la respuesta efectiva ante incidentes, mediante el uso de recursos tecnológicos avanzados, capacitación del personal y procesos claramente definidos para garantizar la continuidad de las operaciones.

El Gobierno del Quindío entiende que la información es uno de sus principales activos, esencial para la toma de decisiones, la prestación de servicios a los ciudadanos y la ejecución de sus funciones misionales. Por ello, se han diseñado protocolos de seguridad informática, planes de contingencia y estrategias de recuperación que buscan minimizar los impactos negativos de cualquier interrupción

en los sistemas. Además, se fomenta una cultura organizacional de sensibilización frente a los riesgos, donde cada funcionario comprende su rol en la protección de la información institucional.

Finalmente, este enfoque integral no solo busca proteger los recursos tecnológicos e informáticos, sino también garantizar la continuidad operativa y la sostenibilidad de los servicios esenciales para los ciudadanos. De esta manera, el Gobierno del Quindío reafirma su compromiso con la innovación, la transparencia y la gestión responsable del riesgo en todos los niveles de la organización.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Diseñar e implementar un sistema integral de gestión de riesgos en seguridad, privacidad de la información y seguridad digital que permita identificar, evaluar, prevenir y mitigar amenazas, garantizando la confidencialidad, integridad y disponibilidad de los datos, así como la continuidad de los servicios digitales de la entidad, en alineación con los principios de eficiencia, transparencia y desarrollo sostenible del territorio.

2.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico integral de los riesgos asociados a la seguridad de la información y el entorno digital, considerando aspectos técnicos, humanos, legales y de procesos, para establecer un mapa de riesgos que permita priorizar acciones estratégicas.

- Implementar y mantener tecnologías de protección avanzadas, sistemas de monitoreo y protocolos de respuesta ante incidentes, asegurando la resiliencia de la infraestructura digital frente a posibles amenazas cibernéticas.

- Promover la capacitación y sensibilización de los funcionarios y colaboradores de la entidad en temas de seguridad digital, privacidad y manejo ético de la información, fomentando una cultura de corresponsabilidad en la protección de los datos.

- Asegurar la adherencia a las normativas nacionales e internacionales en materia de protección de datos personales, ciberseguridad y seguridad de la información, integrando estándares como ISO/IEC 27001 y guías del Ministerio de Tecnologías de la Información y las Comunicaciones. de Colombia.

- Establecer mecanismos de monitoreo, auditoría y evaluación continua del sistema de gestión de riesgos para garantizar su eficacia, adaptabilidad y mejora constante frente a las dinámicas cambiantes del entorno digital y las necesidades del territorio.
- Integrar el Plan de Gestión de Riesgos con las estrategias de desarrollo territorial, impulsando un entorno digital seguro que facilite la sostenibilidad, la innovación y la cohesión social en el departamento del Quindío.

3. ALCANCE

Este plan abarca la definición, implementación y monitoreo de estrategias, políticas y procedimientos destinados a la protección de la información, la seguridad digital y la privacidad en todas las actividades y servicios liderados por la entidad. Su enfoque es integral, considerando tanto el ámbito institucional como la infraestructura tecnológica y los riesgos asociados a las amenazas digitales.

En el ámbito institucional, el plan se aplica a todas las dependencias, procesos y funcionarios de la Gobernación, así como a contratistas y terceros que tengan acceso a la infraestructura tecnológica o manejen información institucional. Este alcance asegura una cobertura total en la gestión y uso de los recursos digitales del departamento.

En cuanto a la infraestructura tecnológica, el plan abarca todos los sistemas de información, plataformas digitales, redes de comunicación, dispositivos de almacenamiento y tecnologías utilizadas para la gestión administrativa, operativa y de servicios al ciudadano. Esto incluye tanto los recursos físicos como los virtuales, garantizando la protección integral de los activos digitales.

Respecto a la gestión de la información, el plan se enfoca en la protección de datos personales, sensibles y confidenciales recopilados, almacenados o procesados en el marco de las actividades de la Gobernación. Esto se realiza conforme a la Ley 1581 de 2012 y otras normativas nacionales e internacionales aplicables,

asegurando el cumplimiento legal y ético.

Finalmente, el plan cubre la identificación y mitigación de riesgos asociados a amenazas digitales como ataques cibernéticos, brechas de seguridad, pérdida de datos y otros incidentes que pueden comprometer la integridad, confidencialidad y disponibilidad de la información. Así, se busca fortalecer la resiliencia digital del departamento y garantizar la confianza de los ciudadanos en los servicios ofrecidos por la Gobernación del Quindío.

4. GLOSARIO

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Backup: Una copia de seguridad o un duplicado de los datos que se hace para poder recuperarlos ante cualquier pérdida o incidente. Por lo tanto, las copias de seguridad forman una parte muy importante de la seguridad TIC de una entidad, ya que sin ellas una entidad podría quedarse sin sus datos.

Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI). REQUISITOS, 2006).

Firewall: También llamado cortafuegos, es un sistema cuya función es prevenir y proteger
a nuestra red privada, de intrusiones o ataques de otras redes, bloqueando el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red

GB: Un gigabyte es una unidad de almacenamiento de información.

Gestión de capacidad: Garantiza que todos los servicios de TIC estén respaldados por una capacidad de procesamiento y almacenamiento suficiente y correctamente dimensionada.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)., 2016).

Información: Se refiere a toda comunicación o representación de conocimiento como Documento controlado por el Sistema de Gestión su reproducción total o parcial versión es vigente si se consulta en la Intranet de la Gobernación del Quindío 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.

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Hardware: Representa los componentes físicos y tangibles de un sistema, es decir los componentes tangibles que pueden ser vistos y tocados.

Inventario de activos: [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

Lan: Una red local (también conocida habitualmente como red de área local o LAN) consiste en un grupo de ordenadores y otros dispositivos que se encuentran conectados entre sí a través de una red, encontrándose todos en una misma ubicación, ya sea dentro de una casa o una oficina.

Malware: el término malware se refiere a un software o código malicioso que causa daños a los sistemas de información, daña los dispositivos, roba datos y siembra el caos. Hay muchos tipos de malware entre los que se incluyen virus, troyanos, spyware, ransomware entre otros.

Mbps: significa Megabits por segundo y generalmente se usa para medir las velocidades de descarga de Internet.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)., 2016).

Procesador: también conocido como CPU por sus siglas (Central Processing Unit) es el componente más importante, esta unidad de procesamiento es la encargada de descifrar las instrucciones de un hardware, que todas las tareas se desarrollen en nuestro equipo y los códigos de los programas sean ejecutados sin problema.

Phishing: El phishing es un delito informático que tiene como objetivo robar información confidencial. Los estafadores se hacen pasar por grandes empresas u otras entidades de confianza para que les facilite voluntariamente sus datos de acceso a un sitio web o Información Personal.

RAM: La memoria de acceso aleatorio (RAM) es su almacenamiento de datos a corto plazo del sistema. Almacena la información que usa de forma activa su computadora para que pueda acceder a ella de manera rápida. Cuanto más programa ejecute su sistema, más memoria necesitará.

Redes: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables).

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Servidor: es un equipo diseñado para procesar solicitudes y entregar datos a otros ordenadores a los que podríamos llamar clientes. Esto se puede hacer a través de una red local o a través de Internet.

Software: permite administrar los recursos que necesita el sistema del computador para manejar los programas y aplicaciones. El software sirve como puente para que el usuario interactúe con el hardware a través de este. Documento controlado por el Sistema de Gestión su reproducción total o parcial versión es vigente si se consulta en la Intranet de la Gobernación del Quindío.

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 cumple con la colaboración en la arquitectura cliente-servidor.

Spyware: también denominado spybot, es un programa malicioso espía. Se trata de un malware, un tipo de software utilizado para recopilar información de un ordenador o dispositivo informático y transmitir la información a una entidad externa sin el permiso del dueño del ordenador.

TB: Un terabyte es una unidad de medida de la capacidad de memoria y de dispositivos de almacenamiento informático (disquete, disco duro CD ROM,etc).

TI: Tecnología Información.

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)., 2016).

Virtualización: tecnología que utiliza el software para imitar las características del hardware y crear un sistema informático virtual. Esto permite a las organizaciones de TI ejecutar más de un sistema virtual con multitareas, sistemas operativos y aplicaciones, en un solo servidor.

Web: La palabra web (del inglés: red, malla, telaraña, entramado) se refiere a: World Wide Web (WWW) sistema de documentos (o páginas web) interconectados por

enlaces de hipertexto, disponibles en Internet.

5. Normatividad

Este documento ha sido elaborado en cumplimiento de la normativa vigente emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y está sujeto a las disposiciones legales aplicables en materia.

- Ley 1341 de 2009: Ley de TIC
  Define los principios para el desarrollo del sector TIC en Colombia, incluyendo la promoción de la seguridad digital.

- Ley 1273 de 2009: Protección de la Información y los Datos
  Crea el bien jurídico de la protección de la información y los datos, tipificando delitos relacionados con el acceso indebido, daño informático y suplantación de sitios web para capturar datos personales (phishing).

- Ley 1581 de 2012: Ley de Protección de Datos Personales
  Regula el manejo de datos personales y establece los principios de legalidad, finalidad, libertad, veracidad, acceso y circulación restringida, seguridad y confidencialidad.
- Decreto 1377 de 2013 : Reglamenta parcialmente la Ley 1581 de 2012
  Especifica cómo las organizaciones deben proteger los datos personales y detalla los mecanismos para informar a los titulares.

- Política Nacional de Seguridad Digital (2016).

- Decreto 1008 de 2018 : Política de Seguridad Digital
  Presenta una hoja de ruta para la seguridad digital en Colombia, incluyendo la gestión de riesgos y la protección de infraestructuras críticas.

- Decreto 2106 de 2019 : Simplificación de Trámites en el Sector TIC
  Incorpora medidas de seguridad en los servicios digitales como parte del proceso de digitalización de trámites.

6. NIVELES DE TOLERANCIAS AL RIESGO

Entendiendo que el nivel de tolerancia al riesgo es la exposición al riesgo que una entidad, en este caso la gobernación del Quindío, está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su misión institucional, la secretaría TIC a definido los siguientes niveles de tolerancia al riesgo:

Tabla 1 Niveles de Tolerancia al Riesgo

	CARACTERÍSTICA	MITIGACIÓN
Insignificante	Estos riesgos son inherentes al desempeño rutinario de las funciones, tales como inconvenientes menores en procesos operativos diarios. Ejemplo: retrasos en la actualización de sistemas internos sin impacto significativo.	Dado su carácter rutinario, se gestionan en el nivel 1 de soporte técnico, que está preparado para resolver problemas de bajo impacto sin requerir escalamiento. Esto garantiza la continuidad operativa sin necesidad de asignar recursos adicionales o modificar procedimientos estándar.
Bajo	Aunque pueden representar interrupciones o desafíos menores, no generan impacto relevante en la funcionalidad de los servicios ni comprometen la seguridad de la entidad. Ejemplo: fallas puntuales en sistemas no críticos.	Este tipo de riesgos no justifica una inversión adicional más allá de los controles ya establecidos en la matriz de riesgos. En este nivel, se confía en que los procedimientos existentes sean suficientes para mantener la estabilidad operativa.
Medio	Estos riesgos tienen el	Aunque deben ejecutarse

	potencial de impactar los servicios ofrecidos por la entidad. Aunque las consecuencias pueden ser absorbidas dentro de las actividades normales, podrían generar interrupciones o demoras significativas. Ejemplo: fallas temporales en servicios digitales utilizados por los ciudadanos.	actividades para la mitigación del riesgo, estas pueden ser debido a su nivel y ejecutadas a mediano plazo.
Alto	Impacta sobre la funcionalidad del servicio de la Gobernación del Quindío, la mayoría de las veces estas consecuencias NO pueden ser absorbidas y subsanadas en el desarrollo normal de las actividades de la secretaría TIC.	Requiere que se ejecuten actividades para disminuir exposición al riesgo, como adquisición de equipos, coberturas de seguros o pólizas, personal especializado, etc. Todo lo anterior se debe hacer a corto plazo.
Catastrófico	Afecta gravemente el desempeño de las actividades propias de la Gobernación del Quindío. Generando riesgos que si no se priorizan, por lo general pueden desencadenar hasta en pérdida de información valiosa de la entidad.	Bajo ninguna circunstancia se deberá tener este riesgo y si se llegase a tener, este deberá tener una alta prioridad por el comité de gobierno en línea y se deberá comunicar a la alta dirección de la gobernación del Quindío.

7. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Definición: La matriz de riesgos es una confrontación analítica de los posibles riesgos a los que se encuentra sometida el área tecnológica, este análisis nos permitirá evaluar la probabilidad de ocurrencia de los distintos riesgos para diseñar los controles preventivos y correctivos, los que se considera más críticos y causan

más impacto para la gobernación del Quindío. En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Análisis de Riesgos: Los diferentes riesgos a los que puede encontrarse sometida el área tecnológica se pueden agrupar de la siguiente forma:

7.1. Riegos por incidencia externa

- **Desastre natural:** Hace referencia a los riesgos a los que está expuesta cualquier entidad pública, en caso de incendio, terremoto, tormenta eléctrica, etc.

- **Interrupción del fluido eléctrico:** Esto es la capacidad que tiene la gobernación del Quindío para reaccionar ante el corte parcial del fluido eléctrico, por daños inesperados por parte de la empresa prestadora del servicio.

- **Modificaciones a la constitución política**: Ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

7.2. Riesgos por incidencia interna

- **Pérdida de la información:** Hace referencia a la seguridad de la información que maneja la gobernación del Quindío, ya que debido a los procesos que la entidad maneja, esta debe conservarse de manera confidencial, y así evitar que sea entregada accidentalmente, o bien, que sea objeto de robo.

- **Falla de equipos electrónicos**: Como cualquier equipo electrónico los computadores son susceptibles a fallos en cualquier momento, pudiendo llegar a provocar pérdida de la información y retrasos en procesos administrativos.

- **Falla en servidores:** Los servidores que se encuentran en el Data center de la gobernación del Quindío, pueden llegar a presentar fallas de configuración, provocando que se paren los aplicativos esenciales con los que trabajan los funcionarios, como PCT, SEVENET, INTRANET Y DOMINIO.

- **Virus informáticos:** Los virus informáticos tienen por objeto alterar el funcionamiento normal de los equipos de cómputo, además tienen la facilidad de propagarse con facilidad con el uso de memorias USB, correo electrónico, etc.

- **Seguridad o Robo:** hace referencia al hurto de la información, de los mismos equipos de cómputo o equipos de red con los que cuenta la gobernación de Quindío.

- **Calentamiento de la Sala de Cómputo (Data center):** Este riesgo está asociado a la probabilidad de que se incremente la temperatura de la data center por encima de los mínimos permitidos por la dirección Tic, cabe aclarar que en el data center se encuentran los servidores de la gobernación del Quindío y switches principales de la red interna, los cuales generan que se incremente la temperatura dentro del cuarto.

- **Copias de seguridad sistemas de información:** Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, dichas copias se deben realizar diariamente y por la Secretaría TIC.

- **Falta de Actualización de la infraestructura tecnológica:** se refiere a la falta de adquisición y/o actualización de equipos que se van quedando obsoletos por su tiempo de uso.

- **Incumplimiento de los contratistas:** Este riesgo puede ocurrir a causa del posible retraso en la contratación, ejecución o trasgresión del de los contratos de actualización, modificación, mantenimiento, que se asumen durante la vigencia, contratos como licenciamiento de antivirus, mantenimiento correctivo de equipos, red de acceso a internet, sistemas de información como PCT, Sevenet, Ventanilla única virtual Quindío, Siscar, etc.

- **Retrasos en Procesos Administrativos:** La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos, los cuales se pueden llegar a retrasar por exigencias en el cumplimiento de requisitos.

- **Procesos de capacitación constante del personal TI:** Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información de la gobernación del Quindío.

- **Accesos no autorizados a los sistemas de información:** Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.

- **Equivocaciones humanas:** Riesgo permanente que se genera por el desconocimiento, descuido, o mal uso de un sistema de información o aplicativo de la entidad.

- **Activos de la información desactualizados:** La no actualización de los activos de la información por parte de la secretaria TIC, genera un riesgo inherente a la pérdida de la información y/o desconocimiento de lo que se encuentra instalado en cada equipo de la entidad.

- **Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso:** Riesgo asociado a equipos de red identificados en diferentes pisos de la entidad, los cuales tienen acceso cualquier funcionario o persona ajena a la entidad, pudiéndose conectar a internet.

7.3. Mitigación del riesgo

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Los cuales se resumen a continuación:

Desastres naturales

Aunque realmente un desastre natural no se puede evitar, la gobernación del Quindío puede llegar a prevenir algunas de las consecuencias que este tipo de siniestro pueda llegar a tener sobre la infraestructura tecnológica.

El edificio de la gobernación, cuenta con una estructura sismo resistente, que ayuda a que en caso de terremoto este pueda seguir en pie o, en consecuencia, con muchos menos daños que otros edificios.

Por otra parte, la red interna de la gobernación del Quindío, está respaldada con UPS, para
evitar que los Switches se dañen en casa de tormentas eléctricas, con este mismo respaldo
cuentan los servidores de la gobernación que se encuentran en el data center.

Interrupción del fluido eléctrico

Como se dijo anteriormente la red interna de la Gobernación del Quindío se encuentra respaldada con UPS, para que esta siga su funcionamiento normalmente durante más de
20 minutos de interrupción. Además de que los servidores se encuentran respaldados.

Modificaciones a la constitución política

Leyes, decretos, resoluciones, ordenanzas, etc. Que expida el gobierno nacional a cargo del ministerio de Tecnologías de la información y comunicaciones MinTic, sobre el trato, seguridad y manejo de la información que tienen los entes gubernamentales.

Pérdida de Información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Falla de equipos electrónicos

Para tratar de mitigar este riesgo, la gobernación del Quindío a través de la secretaría TIC y con el apoyo de la empresa contratista a cargo de los mantenimientos preventivos y correctivos, viene realizando y ejecutando un plan de mantenimiento preventivo, el cual incluye un cronograma de actividades y que es ejecutado durante todo el año.

Falla en servidores

Los servidores se actualizan constantemente con las últimas actualizaciones de seguridad, además estos cuentan con monitores de confiabilidad y rendimiento que envían alertas al administrador ante cualquier eventualidad.

Virus informáticos

Contra los virus informáticos, la gobernación del Quindío, cuenta con antivirus en todos los equipos de cómputo de la misma, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que a través del año, se está ejecutando el mantenimiento preventivo el cual incluye mantenimiento de software y sistema operativo (desinfección).

Seguridad o Robo

Para reducir el riesgo de robo la gobernación del Quindío cuenta con un plan de mantenimiento de las cámaras de seguridad para del edificio, así como un estudio de la
viabilidad para aumentar el número de las cámaras con el fin de reforzar la seguridad del
mismo. la gobernación cuenta con vigilancia las 24 horas del día.

Calentamiento de la Sala de Cómputo (Data center)

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la gobernación del
Quindío ha implementado procedimientos para su mitigación, tales como: La
implementación en el centro de cómputo principal (piso 1) de un Sistema de Temperatura
autorregulada, provisto de un sistema de aire acondicionado, con sensores ambientales
para el control y monitoreo de temperatura.

Copias de seguridad sistemas de información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos

duros externos que se encuentran en el data center.

Falta de actualización de la infraestructura tecnológica

La Gobernación del Quindío cuenta con un plan de compras, en el cual se tiene proyectado
siempre la adquisición de equipos y/o dispositivos que ayuden a actualizar la infraestructura
tecnológica de la misma.

Incumplimiento de los contratistas

Dentro de los procesos de contratación que tiene la gobernación del Quindío, con los proveedores de sistemas de información, se cuenta con pólizas de cumplimiento responsabilidad que ayudan a mitigar el riesgo inherente al incumplimiento.

Retrasos en Procesos Administrativos

La gobernación del Quindío tiene como prioridad el resguardo de la seguridad d la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para la Secretaria TIC

Procesos de capacitación constante del personal TI

La secretaria TIC, capacita en el manejo de los sistemas de información a todo el personal que ingresa a la dependencia, se realiza un proceso de aprendizaje en el cual el ingeniero, técnico o tecnólogo aprende a dominar las herramientas tecnológicas que se tienen en la gobernación.

Por otra parte, a través de la estrategia de gobierno en línea, la secretaría TIC capacita constantemente a su personal en implementación de la misma.

Accesos no autorizados a los sistemas de información

Como parte de las políticas de seguridad de la información aprobadas por la secretaría administrativa, la entidad cuenta con una política de bloqueo de cesión de los equipos cada 5 minutos de inactividad. Lo anterior con el fin de evitar accesos no autorizados a los sistemas cuando el funcionario responsable del equipo no se

encuentre en el sitio de trabajo.

Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte de personas tanto internas como externas a la gobernación del Quindío; La entidad cuenta con un firewall instalado y con un sistema de antivirus licenciado que brindan seguridad a la hora de bloquear intentos de ataques o accesos a sistemas de información de la entidad.

Equivocaciones humanas

Si bien es cierto que este riesgo es difícil de mitigar, por la cantidad de funcionarios que laboran en la entidad, cabe decir que la Secretaria TIC, brinda capacitaciones continuas a los funcionarios de la entidad, sobre el manejo de los aplicativos de la entidad, además de eso, desde el área se generan copias de seguridad diarias de las bases de datos de los aplicativos de la entidad, lo anterior con el fin restaurar la información, ante cualquier pérdida o daño que se haga en una base de datos.

Activos de la información desactualizados

Dentro de los planes y controles que la Secretaria Tic ejecuta, se tiene establecido el catálogo de servicios tecnológicos y la arquitectura de servicios TI, los cuales deben de tener actualizados los activos de la información para su correspondiente actualización anual. Igualmente, la secretaría TIC cuenta con un sistema de información, el cual hace un levantamiento de la información de los equipos de la entidad, su licenciamiento y sus características de hardware.

Equipos de red (switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso

Como parte del levantamiento de los diagramas de red y activos de la información de IPV6, se identificó diferentes puntos de red, los cuales están conectados switch no autorizados por la secretaria TIC, por tal motivo se ha venido trabajando en deshabilitar puertos de red que no están utilizando o que no han sido autorizados por la gobernación del Quindío

8. MATRIZ DE RIESGOS

A continuación, se relaciona la matriz de probabilidad e impacto de los riesgos relacionados con anterioridad

Identificación del riesgo		Análisis del riesgo inherente				
Referencia	Descripción del Riesgo	Probabilidad Inherente	%	Impacto Inherente	%	Zona de Riesgo Inherente
1	Posibilidad de afectación economica y reputacional por hurtos de sistemas de informacion en custiodia de la secretaria TIC, debido a la falta de controles de seguridad apoyados en la tecnología, que garanticen la seguridad de los bienes tecnologicos del edificio de la gobernación del Quindío	Media	60%	Leve	0.2	Moderado
2	Posibilidad de afectación económica por equipos susceptibles a fallos electrónicos que encuentran en el edificio de la gobernación del Quindío.	Baja	40%	Menor	0.4	Moderado
3	Posibilidad de afectación económica y reputacional asociado a la falta de copias de seguridad permanente a los sistemas de información y equipos de computo que se encuentran en la gobernación del Quindío, debido a la baja capacitación en el manejo y realización de copias de seguridad a los diferentes funcionario de la Secretaría TIC.	Media	60%	Leve	0.2	Moderado

Ilustración 1Matriz de probabilidad e impacto de riesgos de seguridad digital part. 1

4	Posibilidad de afectacion reputacional de la entidad asociado a la baja calificación en el Medición del Desempeño Institucional, a través del FURAG, por falta de planes y/o políticas correspondientes a la estrategia, para el Indice de la Politica de Gobierno Digiral como requisito legal bajo el decreto 2008 de 2018.	Muy Baja	20%	Moderado	0.6	Moderado
5	Posibilidad de afectación económica y reputacional por falta herramientas indispensables para brindar cubrimiento oportuno en la solución de soporte técnico en los servicios internos, debido a la inadecuada gestión administrativa en la asignacion de recursos insuficientes para cubrir las necesidad de las herramientas indispensables para la solución de novedades relacionadas con las fallas o incidencias técnicas en la	Media	60%	Mayor	0.8	Alto
6	Posibilidad de afectación economica y reputacional en el incumplimiento de las metas del Plan de Desarrollo, planes y polícias, por falta de capacitación adecuada en nuevas tecnologías y herramientas asociadas a la Administración Departamental, lo que podría limitar la eficiencia y la innovación dentro del entorno.	Media	60%	Leve	0.2	Moderado

Ilustración 2 Matriz de probabilidad e impacto de riesgos de seguridad digital part.2

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Ilustración 3 Criterios para definir el nivel de probabilidad

9. IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información MSPI con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información al interior de la entidad.

El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad digital, ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL (MGRSD), llevarán a cumplir dichas tareas de gestión de riesgo de seguridad digital requeridas en el MSPI (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, 2018).

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.

- Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de implementación del MSPI.

- Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de MEDICIÓN DEL DESEMPEÑO del MSPI.

- Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependen de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

- Teniendo en cuenta lo anterior la gobernación del Quindío, adoptará el modelo de identificación de riesgos de seguridad digital propuesto el departamento de la función pública en su guía para la administración del riesgo y el diseño de controles en entidades públicas:

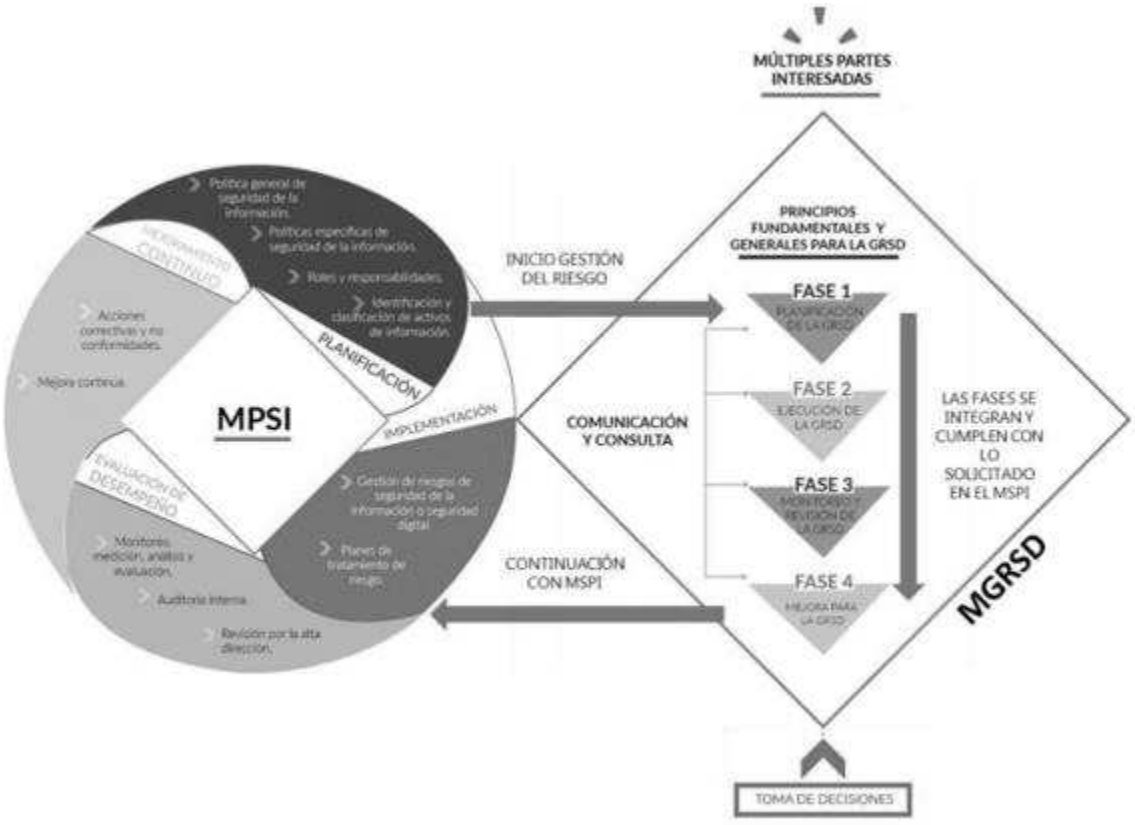


Ilustración 4 Modelo de identificación de riesgos de seguridad digital

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

10. ESTABLECIMIENTO DEL CONTEXTO

Según la guía del departamento administrativo de la función pública, la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9). Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso y sus activos de seguridad digital (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

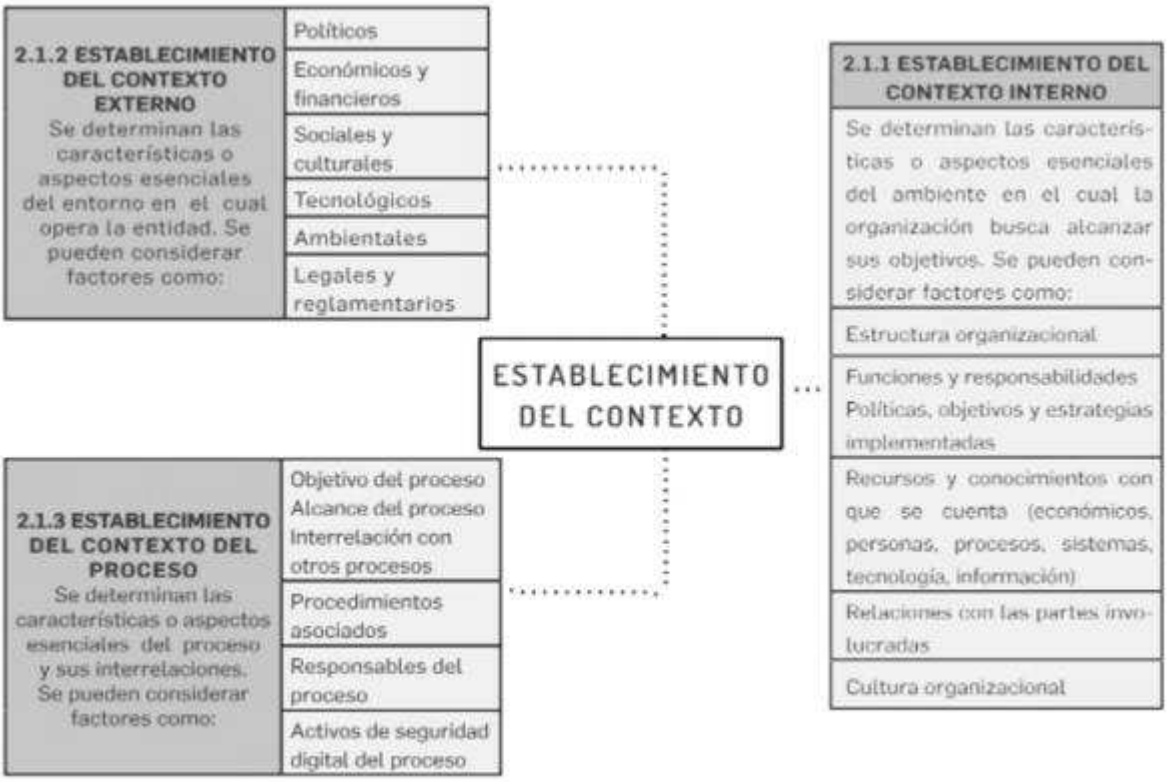


Ilustración 5 Contexto interno y externo de la entidad

Fuente: (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018)

10.1. CONTEXTO EXTERNO

A nivel nacional el decreto 1581 del año 2012 “Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales” y el cual 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.

Por lo que toda información de carácter personal que se encuentra en los distintos medios o dispositivos de almacenamiento de la gobernación del Quindío, debe contemplar medidas de protección de dicha información de modo que no se vea afectada la integridad y buen nombre de las personas.

Por otra parte, la ley 1712 del año 2014 “Ley de Transparencia y del Derecho de Acceso a la Información Pública” la cual 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”.

En razón a esto, la gobernación del Quindío está comprometida con la identificación clasificación de todo tipo de información que es creada, almacenada, administrada publicada, permitiendo así dar correcto cumplimiento a lo establecido en esta ley.

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC el 4 de junio de 2018 estableció el decreto 1008 *"Por el cual se establecen los lineamientos 1 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*" que por medio del uso de tecnologías de la información y las comunicaciones permita 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.

10.2. CONTEXTO INTERNO

La gobernación del Quindío dentro de su estructura organizacional recientemente modificada adhirió a la secretaría TIC, mediante el decreto 187 del 28 de marzo del 2019, como una más de sus secretarías y creando a su vez dos direcciones que ayudarán a cumplir los objetivos institucionales que la entidad trace a corto, mediano y largo plazo.

Dentro de las funciones de la secretaría TIC están Diseñar y formular los planes, programas y proyectos, así como fortalecer el uso, la innovación y la apropiación de las tecnologías de la información y las comunicaciones y la gestión de la información, con el fin de propiciar la implementación de la TI en el Departamento del Quindío.

Teniendo en cuenta lo anterior y como parte de las funciones propias de la secretaría se debe encaminar esfuerzos para ejecutar las acciones orientadas a la gestión de riesgos de seguridad digital, hacia la protección de la disponibilidad, integridad y confidencialidad de los datos e información que se almacena en la gobernación del Quindío, que se procesa, que se almacenada y se transmite, previniendo la materialización de amenazas que puedan impactar de forma considerable la información concerniente a los ciudadanos y funcionarios
propios de la administración departamental.

Por otra parte, y con la adopción del modelo de seguridad y privacidad de la información MSPI y con la definición del plan estratégico de tecnologías de la información PETI, la gobernación del Quindío da un paso adelante en la consecución de la estrategia de gobierno digital con todos sus componentes, logrando así beneficiar a los funcionarios y a la comunidad en general.

10.3. CONTEXTO DEL PROCESO

El plan de gestión de riesgos y la matriz de identificación de riesgos, hacen parte del modelo de seguridad y privacidad de la información adoptado por la gobernación del Quindío, en cumplimiento con la estrategia de gobierno digital y apuntan básicamente a la protección de los activos de información de la entidad, garantizando así el funcionamiento interno de los procesos que van de cara a los ciudadanos.

11. IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018).

Teniendo en cuenta lo anterior se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Para la fase de identificación de activos de información, se tomará como base de referencia el catálogo de servicios tecnológicos y sus fichas de servicio con los que cuenta la secretaría TI:

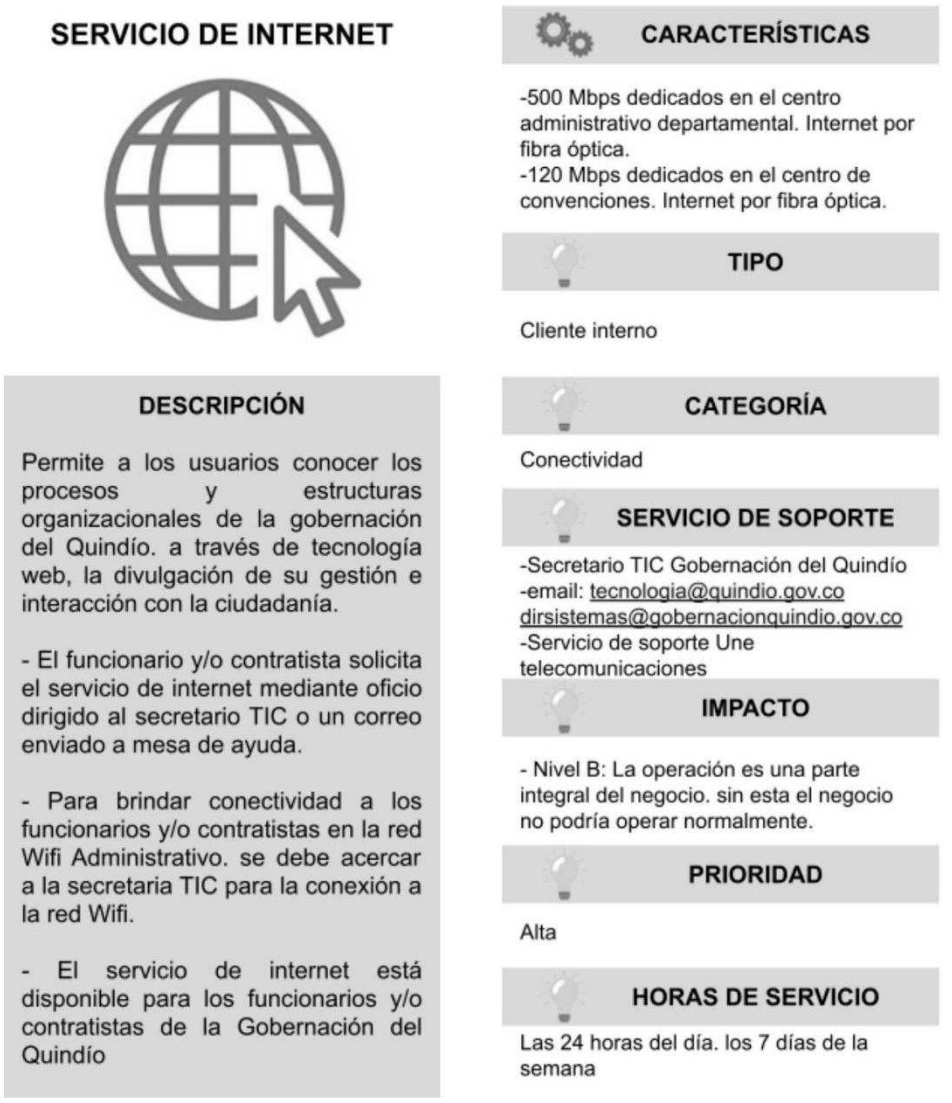
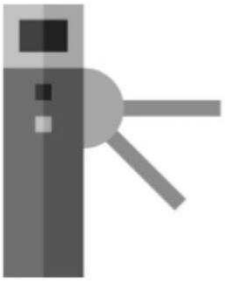


Ilustración 6 Fichas de servicio con los que cuenta la secretaría TI

TORNIQUETES



DESCRIPCIÓN

Sistema de seguridad física dedicado al control de acceso a las instalaciones del centro administrativo departamental, Cuyo fin es el de tener un registro completo de todas las personas que ingresan al lugar para así poder aplicar los controles de seguridad pertinentes.

El sistema de torniquetes funciona bajo un servidor y aplicación de software.

CARACTERÍSTICAS

- Torniquete trípode de acceso doble brazo.
-Incluye: lectora biométrica y RFID.
-Implementación en interior /exterior
-Acceso usuarios:30 por minuto.
-Botón de emergencia • Brazos caídos.
-Puerta acceso personas discapacitadas (Doble Puerta)
-Software de control visitantes
-Registro huella

TIPO

Cliente Interno
Cliente Externo

CATEGORÍA

Seguridad

SERVICIO DE SOPORTE

Secretario TIC Gobernación del Quindío

IMPACTO

- Nivel C: La operación no es una parte integral del negocio

PRIORIDAD

Baja

HORAS DE SERVICIO

Lunes a Viernes 7:00 a.m a 12:00 m. 2:00 p.m. a 5:00 p. m

Ilustración 7 Torniquetes

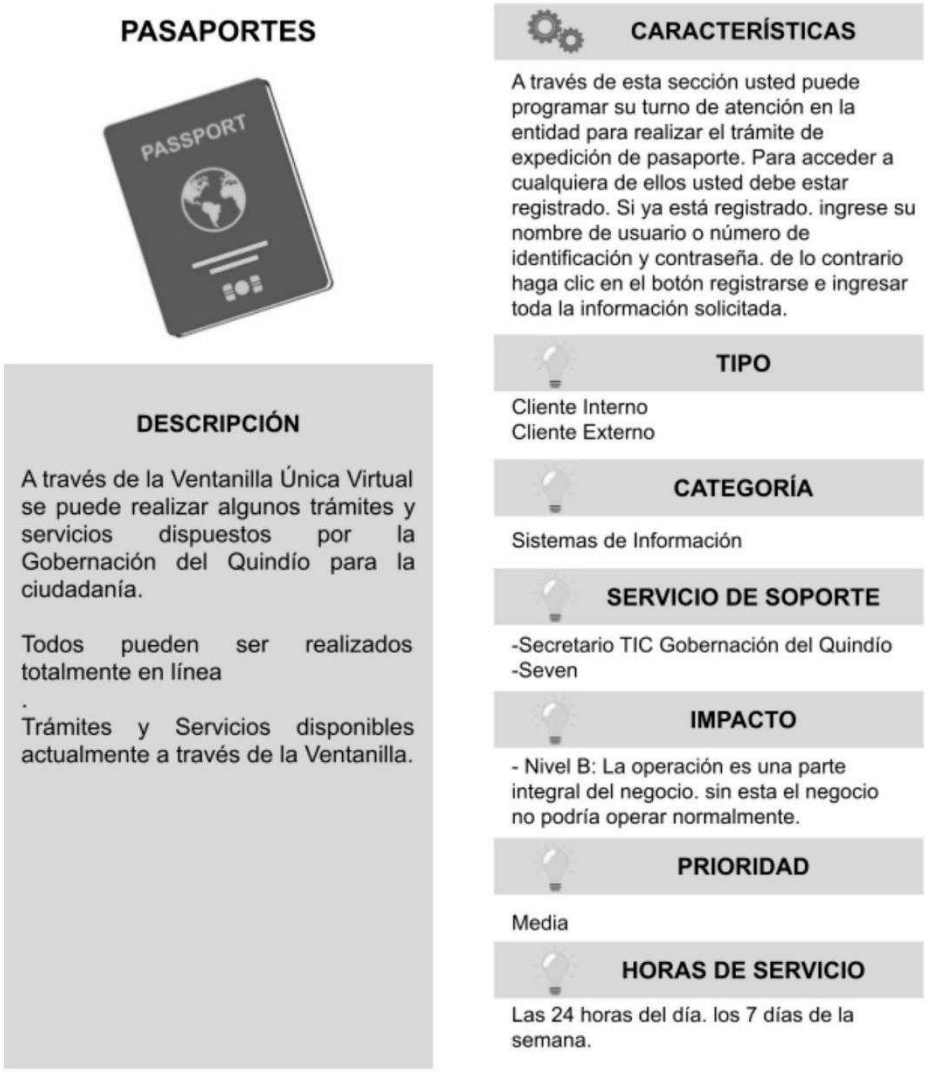


Ilustración 8 Pasaportes

CORRESPONDENCIA SEVENET

DESCRIPCIÓN

Permite la incorporación de la Quindío gestión de documentos a los procesos de la Gobernación del Quindío automatizando procedimientos, con importantes ahorros en tiempo, costos y recursos tales como tóner de impresora, papel, fotocopias, entre otros, así como el control sobre los documentos.

CARACTERÍSTICAS

El aplicativo Sevenet le apunta a la estrategia cero papel liderada por el ministerio de tecnologías de la información y comunicaciones MinTic.

TIPO

Cliente interno

CATEGORÍA

Comunicaciones

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Lexco

IMPACTO

- Nivel C: La operación no es una parte del negocio.

PRIORIDAD

Media

HORAS DE SERVICIO

Lunes a Viernes 7:00 a. m. a 12:00 m.
2:00 p. m. a 5:00 p. m.

Ilustración 9 Correspondencia SEVENET

PCT

DESCRIPCIÓN

PCT Enterprise es un Sistema de Información Administrativo y Financiero exclusivo para el Sector Público.

PCT Enterprise está presente en entidades del Sector Público que operan en 15 Departamentos y la ciudad de Bogotá. Actualmente productivo en 14 Gobernaciones de Colombia, 18 alcaldías Municipales, 14 corporaciones Autónomas Regionales (y otras entidades públicas de Nivel Central Territorial y Empresas del Estado 12.

CARACTERÍSTICAS

33 módulos ejecutables. entre los cuales se encuentran (contratación. consultas. egresos. ingresos. almacén. entre otros)

TIPO

Cliente interno

CATEGORÍA

Sistemas de información

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- soporte@pctltda com
- soporte2@pctltda.com
- soporte3@pctltda.com

IMPACTO

- Nivel A: La operación es crítica para el negocio. Una operación es crítica cuando al no contar con esta. la función del negocio no puede realizarse.

PRIORIDAD

Crítica

HORAS DE SERVICIO

Lunes a Viernes 7:00 a. m. a 12:00 m.
2:00 p. m. a 5:00 p. m.

Ilustración 10 PCT

Ilustración 11 Backup

DIRECTORIO ACTIVO

DESCRIPCIÓN

Active Directory o también llamado AD o Directorio Activo. Es una herramienta perteneciente a la empresa de Microsoft que proporcione servicios de directorio normalmente en una red LAN. Lo que es capaz de hacer este directorio activo es proporcionar un servicio ubicado en uno o varios servidores capaz de crear objetos como usuarios. equipos o grupos para administrar las credenciales durante el Inicio de sesión de los equipos que se conectan a una red. Pero no solamente sirve para esto. ya que también podremos administrar las políticas de absolutamente. Toda la red en la que se encuentre este servidor Esto implica, por ejemplo. la gestión de permisos de acceso de usuarios, bandejas de correo personalizadas. etc.

CARACTERÍSTICAS

-Active directory montado en Windows server 2016.
-grupos de trabajo, VIP (permisos especiales). general (para la mayoría de usuarios). Bancos (Usuarios que hacen transacciones bancarias.
- Políticas de seguridad aplicadas desde active directory

TIPO

Cliente interno

CATEGORÍA

Sistemas de información

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente

PRIORIDAD

Alta

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 12 Directorio Activo

MESA DE AYUDA

DESCRIPCIÓN

Proporciona a los usuarios un medio para generar solicitudes ya sean preventivas, correctivas o explicativas del canal e infraestructura tecnológica. A través de la plataforma el usuario puede ver la trazabilidad de la solicitud.

CARACTERÍSTICAS

- Sistemas de logue para funcionarios y personal de soporte de la secretaria Tic.
-Encuesta de satisfacción de los servicios prestados.
- Clasificación de categoría de servicios.
- Tiempos de soporte para cada servicio.

TIPO

Cliente interno

CATEGORÍA

Soporte

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Seven

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente

PRIORIDAD

Media

HORAS DE SERVICIO

Lunes a Viernes 7:00 a. m. a 12:00 m.
2:00 p. m. a 5:00 p. m.

Ilustración 13 Mesa de Ayuda

INVENTARIO

DESCRIPCIÓN

El inventario de equipos de cómputo de la gobernación del Quindío se realiza a través de la aplicación llamada Ocs inventory.

"Open Computer and Software Inventory Next Ceneration (OCS) es un software libre que permite a los Administradores de TI (Tecnología de Información) gestionar el inventario de sus activos de TI.

OCS-NC recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS (""agente OCS de" "inventario"")."

CARACTERÍSTICAS

- Software Libre.
-Sistema de transmisión avanzado para implementar instalaciones de software o ejecutar scripts y comandos en computadoras sin sobrecargar la red. Soporte para muchos sistemas operativos. incluidos: Microsoft Windows. Linux. BSD. Sun Solaris. IBM A IX. HP UX. Macos X. Android.
- Detección de redes

TIPO

Cliente Interno

CATEGORÍA

Sistemas de información

SERVICIO DE SOPORTE

-Secretario TIC Gobernación del Quindío

IMPACTO

- Nivel C: La operación no es una parte integral del negocio.

PRIORIDAD

Media

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 14 Inventario

SEGURIDAD PERIMETRAL

DESCRIPCIÓN

Sistemas destinados a proteger de intrusos el perímetro del centro administrativo departamental. La única diferencia es que, en lugar de un espacio físico, se protegen las redes privadas de tu sistema informático.

Se trata de una primera línea de defensa. igual que las alarmas de una oficina. La seguridad total no existe ni en el mundo físico ni en el informático, pero se puede reducir el riesgo a que nos roben nuestros datos o incluso que estos puedan desaparecer.

CARACTERÍSTICAS

Los servicios de ciberseguridad. corresponden al servicio de internet dedicado e incluyen:
·Full UTM (Unified Threat Management)
- VPN client to site.
- Vpn site to site.
-IDS/IPS.
- Application control.
- Antivirus Gateway.
- Email Protection

TIPO

Cliente Interno

CATEGORÍA

Seguridad

SERVICIO DE SOPORTE

-Secretario TIC Gobernación del Quindío
- Une epm telecomunicaciones

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente.

PRIORIDAD

Alta

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 15 Seguridad Perimetral

IMPUESTO VEHICULAR

DESCRIPCIÓN

El impuesto vehicular se puede recaudar de manera presencial o a través de la página web de la gobernación del Quindío. Este impuesto se realiza con la ayuda de la aplicación SISCAR.

SISCAR ayuda a administrar totalmente las rentas con esta plataforma tecnológica 100% web desde su determinación, fiscalización, liquidación. cobro y devolución de una manera integral, automatizando, su operatividad y optimizando en el recaudo de los impuestos. especies venales. Comparendos y estampillas.

CARACTERÍSTICAS

Módulos y componentes:
- Administración de usuarios y perfiles.
- Auditoría.
- Contabilidad.
- Fiscalización y liquidación del impuesto
- Recaudos vía web serviceS.
- Cobro Coactivo.
- Cobro persuasivo

TIPO

Cliente Interno
Cliente externo

CATEGORÍA

Sistemas de información

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Datasoft

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente.

PRIORIDAD

Alta

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 16 Impuesto Vehicular

Ilustración 17 Antivirus

SERVICIO DE WIFI

DESCRIPCIÓN

Brinda servicio conectividad a los contratistas e invitados en la red Wifi de cada piso de la Gobernación del Quindío.

Se debe acercar a la secretaria TIC Para el ingreso a esta red por parte de un funcionario.

CARACTERÍSTICAS

-500 Mbps dedicados. Internet por fibra óptica.

TIPO

Cliente interno

CATEGORÍA

Conectividad

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Email: tecnologia@quindio.gov.co
- Servicio de soporte Une telecomunicaciones

IMPACTO

- Nivel C: La operación no es una parte integral del negocio.

PRIORIDAD

Media

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 18 Servicio Wifi

INTRANET

DESCRIPCIÓN

Establece un sistema de gestión y comunicación interna para todas las áreas y usuarios de la Gobernación del Quindío de una forma ágil y segura.

CARACTERÍSTICAS

• Mi cuenta Opciones personales del usuario (información personal. Agenda. archivos.
• Para Todos: Información publicada por el administrador de la Intranet (clasificados, cumpleaños, foros de discusión, encuestas)
• Bandeja de Correo electrónico: Correo de la intranet del usuario.
• Grupos a los que pertenece cada usuario. Por defecto es el grupo de la secretaría donde labora y el grupo gobernación para comunicarse con el resto de funcionarios de la Intranet.

TIPO

Cliente Interno

CATEGORÍA

Conectividad

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Seven

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente.

PRIORIDAD

Media

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 19 Intranet

EMAIL

DESCRIPCIÓN

Permitir a los usuarios de la Gobernación del Quindío el intercambio de mensajes a través de una cuenta de electrónico institucional. Correo que facilite el desarrollo de sus funciones.

Aplica a todos los usuarios que tengan un vínculo con la Gobernación del Quindío. usuarios tales como funcionarios en todos los niveles (Carrera administrativa, provisionales y libre nombramiento y remoción)

CARACTERÍSTICAS

El tamaño del buzón tiene una capacidad de 25GB.
·La capacidad de envío y recepción de archivos adjuntos es de 25MB
·La cuenta de correo electrónico es creada como: oficina@gobernacion.gov.co

TIPO

Cliente interno

CATEGORÍA

Comunicaciones

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Seven

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente.

PRIORIDAD

Alta

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 20 Email

PÁGINA WEB

DESCRIPCIÓN

Permite a los usuarios conocer los procesos y estructura organizacional de la Gobernación del Quindío. A través de tecnología web, la divulgación de su gestión e interacción con la ciudadanía.

CARACTERÍSTICAS

• Página web cumple con el certificado de seguridad https.
• Página web cumple con los requisitos de accesibilidad AA

TIPO

Cliente interno
Cliente externo

CATEGORÍA

Comunicaciones

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Seven

IMPACTO

- Nivel C: La operación no es una parte integral del negocio.

PRIORIDAD

Media

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 21 Página Web

VENTANILLA ÚNICA VIRTUAL

DESCRIPCIÓN

A través de la Ventanilla Única Virtual se puede realizar algunos trámites y servicios dispuestos por la Gobernación del Quindío para la ciudadanía.

Todos pueden ser realizados totalmente en línea.

CARACTERÍSTICAS

PQRDS: En este sistema el usuario puede ingresar nuevos requerimientos tales como Derechos de Petición. Quejas. Reclamos. Sugerencias. Denuncias. entre otros. puede realizar seguimiento a sus requerimientos y recibirá. si así lo desea. notificación del estado de sus requerimientos vía correo electrónico.

TIPO

Cliente Interno
Cliente externo

CATEGORÍA

Comunicaciones

SERVICIO DE SOPORTE

- Secretario TIC Gobernación del Quindío
- Seven

IMPACTO

- Nivel B: La operación es una parte integral del negocio. sin esta el negocio no podría operar normalmente.

PRIORIDAD

Alta

HORAS DE SERVICIO

Las 24 horas del día. los 7 días de la semana.

Ilustración 22 Ventanilla Única Virtual

12.MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

A continuación, se presenta el mapa de calor del resultado del análisis de riesgos de los activos de información con los que cuenta la gobernación del Quindío.

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy Alta 100%					
	Alta 80%					
	Media 60%	R1 R3 R6			R5	
	Baja 40%		R2			
	Muy Baja 20%			R4		
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

Ilustración 23 Matriz de Calor Inherente

La anterior matriz se pone a disposición y se encuentra anexa a este plan de tratamiento de riesgos de seguridad digital.

12.1. FASE DE IMPLEMENTACIÓN

Actualmente desde la secretaría TIC de la gobernación del Quindío ya se está haciendo un control sobre los riesgos identificados en las dos matrices de riesgos, reduciendo así la posibilidad de que los riesgos anteriormente mencionadas puedan materializarse

Ahora bien, en esta fase se seguirá la ruta definida para la aplicación de controles, los cuales estarán a cargo de su implementación en los tiempos definidos, los responsables o líderes de proceso con el apoyo de la Secretaría TIC, en lo concerniente a controles tecnológicos e informáticos, también será necesario contar con el apoyo y compromiso del responsable de la seguridad digital (director de sistemas e infraestructura tecnológica) que brinde conocimiento, apoyo y experticia en la aplicación de los controles.

12.2. FASE DE SEGUIMIENTO Y CONTROL

De acuerdo al modelo integrado de planeación y gestión MIPG, la entidad debe asegurar el
logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad.

Dado que el origen y tipos de riesgos son variables, el monitoreo constante será necesario
para detectar cambios respecto a nuevos activos de información, nuevos procesos o procedimientos, nuevos factores o amenazas que afecten los activos de información, nuevas vulnerabilidades, incremento del impacto e incluso la materialización de incidentes de seguridad.

12.2.1. REPORTE Y SOCIALIZACIÓN DE RIESGOS DE SEGURIDAD

A la fecha, la secretaría TIC ha gestionado eventos e incidentes que han afectado la seguridad en la entidad con un impacto bajo, tratando de mitigar y trasladar los riesgos, por lo que no ha sido necesario aún realizar reporte al Centro Cibernético Policial y al Equipo de Respuesta a Incidentes de Seguridad Informática CSIRT.

Por otra parte, desde la secretaría TIC se trabajará de manera eficaz con los

funciona funcionarios, gestores de proceso y la dirección de sistemas e infraestructura tecnológica para la restauración de los activos de información afectados por el incidente y como acciones de mejora para prevenir futuras recurrencias del incidente, se trabajará en la
identificación de causa raíz e implementación de mejoras y controles que ayuden a la protección de los distintos activos de información.

Se realizará la comunicación respectiva, de la mano con el plan de sensibilización y comunicación de las políticas de seguridad de la información, para capacitar a los funcionarios y que ellos sepan reportar de manera correcta un evento o riesgo de seguridad el cual pueda comprometer la integridad de los sistemas de información de la gobernación del Quindío.

12.2.2. AUDITORÍAS INTERNAS Y EXTERNAS

Se espera que desde la Oficina Asesora de Control Interno se les dé seguimiento a las acciones de mejora necesarias para lograr una efectiva gestión de riesgos de seguridad digital y permita esto salvaguardar los activos de información de la entidad.

12.3. FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL.

La secretaría TIC, trabajará en la mejora continua de la gestión de riesgos de seguridad digital, como parte del modelo de seguridad y privacidad de la información MSPI, velando por la mitigación de vulnerabilidades, amenazas, riesgos, eventos e incidentes que atenten contra la disponibilidad, integridad y confidencialidad de los datos e información asociada a los distintos activos de información como parte de los procesos de la entidad y se llevaran a cabo las acciones necesarias para atender los hallazgos o no conformidades producto de
auditorías internas y externas.

13.CONTROL DE CAMBIOS

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**	**FUNCIONARIO**
1.0	15/05/2020	Creación primera versión del Documento.	Ing. Andrés Felipe Barrera Pérez
2.0	21/05/2021	Implementación de riesgos de seguridad digital	Ing. Andrés Felipe Barrera Pérez
3.0	13/11/2022	Actualización fichas de servicios tecnológicos	Ing. Andrés Felipe Barrera Pérez
4.0	31/01/2023	Actualización fichas de servicios tecnológicos y ampliación glosario	Equipo de Ingenieros Contratistas Gobierno Digital
5.0	04/07/2024	Revisión Integral y actualización de diseño	Equipo Gobierno Digital
6.0	20/01/2025	Revisión Integral, actualización de diseño y contenido.	Equipo Gobierno Digital e Infraestructura Tecnológica