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

Instituto Departamental De Tránsito Del Quindío

Circasia, Quindío

2023

Control de Versiones

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0	21/06/2023	Creación del Documento

Índice de Contenido

INTRODUCCIÓN 5
OBJETIVOS 7
Objetivo general 7
Objetivos específicos 7
ALCANCE 8
GLOSARIO 9
NIVELES DE TOLERANCIAS AL RIESGO 14
VALORACIÓN DE LOS RIESGOS 15
IDENTIFICACIÓN DE CONTROLES / RIESGO RESIDUAL 17
IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO 17
IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS 19
Riegos por incidencia externa 19
Riesgos por incidencia interna 20
MITIGACIÓN DEL RIESGO 23
MATRIZ DE RIESGOS 27
IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL 32
ESTABLECIMIENTO DEL CONTEXTO 34
CONTEXTO EXTERNO 35
CONTEXTO INTERNO 37
CONTEXTO DEL PROCESO 38
IDENTIFICACIÓN DE ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN 38
FASE DE IMPLEMENTACIÓN 40
FASE DE SEGUIMIENTO Y CONTROL 40
REPORTE Y SOCIALIZACIÓN DE RIESGOS DE SEGURIDAD 43
AUDITORÍAS INTERNAS Y EXTERNAS 43
FASE DE MEJORAMIENTO CONTINUO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL. 44

Índice de Tablas

Tabla 1. Niveles de tolerancia al riesgo 14
Tabla 2. Análisis por probabilidad 15
Tabla 3. Impacto del Riesgo 15
Tabla 4. Mapa de Calor de Riesgo 16
Tabla 5. Factores de Riesgo 18
Tabla 6. Clasificación de la zona de riesgo 28
Tabla 7. Probabilidad de Ocurrencia del riesgo 30
Tabla 8. Niveles de Impacto del riesgo 30
Tabla 9. Zona de riesgo 31
Tabla 10. Distribución de Riesgos de la entidad en el mapa de calor 31
Tabla 11. Controles para riesgos de seguridad digital 42

Índice de Figuras

Figura 1. Tratamiento de riesgos 16
Figura 2. Matriz de Probabilidad e Impacto de riesgos de seguridad digital 27
Figura 3. Ilustración entre el MSPI y el MGRSD 33
Figura 4. Contexto interno y externo de la entidad 34
Figura 5. Pasos para la identificación y valoración de activos 39

INTRODUCCIÓN

Desde los inicios de los sistemas de información se sabe que las contingencias forman parte de los mismos, ya que como es sabido las amenazas a la información pueden venir de diferentes fuentes, tanto de origen natural (terremotos, tormentas eléctricas, etc.), origen humano (huelgas, competencia entre compañeros, problemas laborales, etc.) y de origen técnico (fallas de hardware, software, suministro de energía, etc.) casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización. Conscientes de ello, se pretende definir en este documento, las políticas más asertivas aplicables al Instituto Departamental de Transito del Quindío, en materia de recuperación de la normalidad para aquellas eventualidades no previstas en las que algún recurso informático se vea amenazado o afectado.

El documento denominado **Modelo de Seguridad y Privacidad de la Información** (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022. De igual manera es importante resaltar que es a través del Decreto Presidencial 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan

de Acción por parte de las entidades del Estado", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad.

La gestión de riesgos establece procesos, procedimientos y actividades encaminados a lograr un equilibrio entre la prestación de servicios y los riesgos asociados a los activos de información que dan apoyo y soporte en el desarrollo de la misionalidad de la entidad. En tal sentido, se debe considerar e implementar medidas que implican tiempo, esfuerzos y recursos necesarios para dar un adecuado tratamiento a los riesgos, generando una estrategia de seguridad efectiva que controle y administre la materialización de eventos o incidentes, mitigando los impactos adversos o considerables al interior de la entidad.

Teniendo en cuenta lo anterior la entidad. Considera que la información es el patrimonio principal de toda la Institución, por lo que planifica y toma medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

OBJETIVOS

OBJETIVO GENERAL

Plantear y establecer un marco de gestión de riesgos a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información que soportan el cumplimiento de los objetivos organizacionales del Instituto Departamental de Transito del Quindío, con el fin de lograr reducir su probabilidad e impacto en la entidad.

OBJETIVOS ESPECÍFICOS

- Proteger y conservar los activos informáticos del Instituto Departamental de Transito del Quindío contra riesgos, desastres naturales o actos malintencionados.
- Garantizar la operatividad de la red interna del Instituto Departamental de Transito del Quindío, cuando se presente alguna eventualidad.
- Evaluar los riesgos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la entidad.
- Gestionar los riesgos identificados con una matriz que ayude a reducir su probabilidad e impacto si se este se llegará a materializar.

ALCANCE

La necesidad de desarrollar un plan de tratamiento de riesgos, está relacionada con el impacto potencial que provoca la interrupción parcial o total de los sistemas de información, sobre el normal desarrollo de las actividades del Instituto Departamental de Transito del Quindío; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos.

Los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al hardware, software, equipos electrónicos y redes involucrados en los procesos críticos definidos en el Plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales de los equipos de cómputo y la red interna, las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los usuarios y dependen de la diligencia y colaboración de las dependencias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

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, bloqueándole 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 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 danos 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 Mega bits 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), ésta se da por medio

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.

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 referirse a: World Wide Web (WWW) sistema de documentos (o páginas web) interconectados por enlaces de hipertexto, disponibles en Internet.

NIVELES DE TOLERANCIAS AL RIESGO

Entendiendo que el nivel de tolerancia al riesgo es la exposición al riesgo que se encuentra asociado a una entidad, en este caso el Instituto Departamental de Transito 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 entidad a definido los siguientes niveles de tolerancia al riesgo:

	CARACTERÍSTICA	MITIGACIÓN
Insignificante	Estos tipos de riesgos, son riesgos rutinarios, propios del desempeño de las funciones	De acuerdo a los niveles de soporte establecidos en el diagrama de servicios, estos pertenecen a soporte nivel 1 y la mayoría se solucionan en este nivel de servicio
Bajo	No tiene impacto potencial sobre la funcionalidad del servicio ni compromete la seguridad de la entidad.	El riesgo que tiene gravedad baja, por lo general no justifica inversión de recursos y controles a los ya establecidos en la matriz de riesgos.
Medio	Impacta sobre la funcionalidad de los servicios que ofrece la entidad, cuyas consecuencias pueden ser absorbidas y subsanadas en el desarrollo normal de las actividades de la entidad.	Aunque deben ejecutarse actividades para la mitigación del riesgo, estas debido a su nivel pueden ser ejecutadas a mediano plazo
Alto	Impacta sobre la funcionalidad del servicio de la entidad, la mayoría de las veces estas consecuencias NO pueden ser absorbidas y subsanadas en el desarrollo normal de las actividades de la entidad.	Requiere que se ejecuten actividades para disminuir la 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 entidad. Generando riesgos que, si no se priorizan, por lo general pueden desencadenar hasta en perdida de información valiosa.	Bajo ninguna circunstancia se deberá tener este riesgo y si ocurre, deberá tener una alta prioridad por el comité de gobierno digital y se deberá comunicar a la alta dirección de la entidad.

Tabla 1. Niveles de tolerancia al riesgo

VALORACIÓN DE LOS RIESGOS

ANÁLISIS POR PROBABILIDAD		
Rara Vez	**1**	No se ha presentado en los últimos cinco años
Poco Probable	**2**	Al menos una vez en los últimos cinco años
Posible	**3**	Al menos una vez en los últimos dos años
Probable	**4**	Al menos una vez en el último año
Casi Cierto	**5**	Más de una vez al año

Tabla 2. Análisis por probabilidad

IMPACTO DEL RIESGO		
Insignificante	**1**	No se genera afectación hacia los objetivos del proceso
Menor	**2**	Afectación leve de los objetivos, las medidas requeridas no son significativas, no hay pérdidas económicas, ni sanciones legales.
Moderado	**3**	Requiere toma de medidas para lograr el cumplimiento del objetivo. Aunque no hay sanciones legales si se evidencia incumplimiento del marco legal. Hay una afectación parcial de la imagen de la entidad.
Mayor	**4**	Impacto sobre la funcionalidad del servicio o sobre la imagen de la entidad, cuyas consecuencias NO pueden ser absorbidas y subsanadas en el desarrollo normal del proyecto.
Catastrófico	**5**	Afecta gravemente la imagen de la entidad. Generando riesgo reputacional.

Tabla 3. Impacto del Riesgo

A continuación, se describen los niveles de aceptación del riesgo en la *tabla 4*, mapa de calor donde la zona de riesgo es igual a la multiplicación entre la probabilidad y el impacto del riesgo los cuales definen en la *tabla 2* y *tabla 3* sucesivamente.

Probabilidad x Impacto = Zona de Riesgo

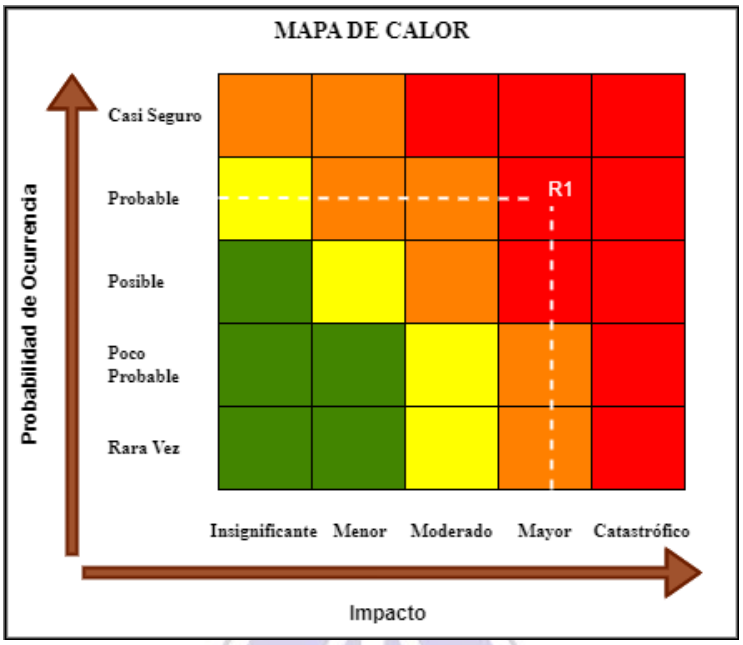

Tabla 4. Mapa de Calor de Riesgo

La *figura 1* muestra como se debe realizar el tratamiento del riesgo relacionado al mapa de calor de la *tabla 4*.

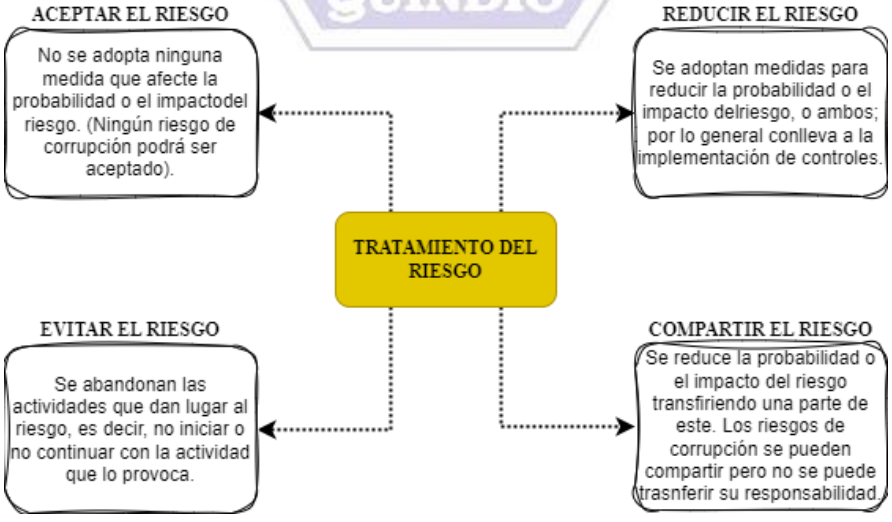

Figura 1. Tratamiento de riesgos

IDENTIFICACIÓN DE CONTROLES / RIESGO RESIDUAL

Control: Es una medida que modifica el riesgo. (ISO/IEC 27000:2018). Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Riesgo Residual: Probabilidad x Impacto = zona de riesgo

Esta evaluación del riesgo residual define el tratamiento del riesgo

NIVEL DE RIESGO	NRA	TRATAMIENTO A SEGUIR
Bajo	Aceptable	Asumir
Moderado	Acepatable	Asumir
Alto	No Aceptable	Reducir-Evitar-Compartir
Extremo	No Aceptable	Reducir-Evitar-Compartir

NRA: Nivel de Riesgo acepatable

IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Son las fuentes generadoras de riesgos. En la *Tabla 1* encontrará un listado con ejemplos de factores de riesgo que puede tener una entidad.

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos

			Falta de capacitación, temas relacionados con el personal.
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible intención frente a la corrupción.		Hurtos activos
			Posibles comportamientos no éticos de los empleados.
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de Equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Tabla 5. Factores de Riesgo

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 el Instituto Departamental de Transito 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:

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 entidad 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.

Riesgos por incidencia interna

- **Perdida de la información:** Hace referencia a la seguridad de la información que maneja el Instituto Departamental de Transito 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 perdida de la información y retrasos en procesos administrativos.
- **Falla en servidores:** Los servidores que se encuentran en el área de la oficina de sistemas de la entidad, pueden llegar a presentar fallas de configuración, provocando la no funcionalidad de los aplicativos esenciales con los que trabajan los funcionarios, como el software financiero Publifinanzas, Intraweb (Ventanilla Única Virtual), Dominio y los aplicativos del SIOT (Sistema de información de organismos de tránsito).
- **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 entidad.
- **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 y switchs 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 oficina de sistemas.
- **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 atraso en la contratación, ejecución o trasgresión 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 Publifinanzas, SIOT, Ventanilla única virtual, 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 puede 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 entidad.

- **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 entidad genera un riesgo inherente a la perdida 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 áreas de la entidad, los cuales tienen acceso cualquier funcionario o persona ajena a la entidad, pudiéndose conectar a internet.

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.

- **Desastres naturales**

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

Las instalaciones del Instituto Departamental de tránsito del Quindío, 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 otras edificaciones.

La red interna de la entidad, está respaldada con una UPS, para evitar que los Switchs se dañen a causa de tormentas eléctricas, con este mismo respaldo cuentan los servidores de la que se encuentran en el data center.

- **Interrupción del fluido eléctrico**

Como se dijo anteriormente la red interna se encuentra respaldada con UPS, para que esta siga su funcionamiento normalmente durante más de 15 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 entidad, cuenta con un manual de política de respaldo de la información de los servidores, este respaldo se realiza todos los días en discos duros externos que se encuentran en la oficina de sistemas.

- **Falla de equipos electrónicos**

Para tratar de mitigar este riesgo, la entidad a través de la oficina de sistemas 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 entidad, cuenta con antivirus en todos los equipos de cómputo, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que, a en cada vigencia anual, 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 entidad cuenta con sistema de seguridad y video vigilancia, así como un estudio de la viabilidad para aumentar el número de las cámaras con el fin de reforzar la seguridad del mismo. A demás cuenta con vigilantes 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 entidad ha implementado procedimientos para su mitigación, tales como: La implementación 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 entidad, cuenta con una política de respaldo de la información de los servidores, este respaldo se realiza todos los días en discos duros externos que se encuentran en la oficina de sistemas.

- **Falta de actualización de la infraestructura tecnológica**

La entidad 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 entidad, con los proveedores de sistemas de información, se cuenta con pólizas de cumplimiento y responsabilidad que ayudan a mitigar el riesgo inherente al incumplimiento.

- **Retrasos en Procesos Administrativos**

El Instituto Departamental de tránsito del Quindío, tiene como prioridad el resguardo de la seguridad de la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para la entidad.

- **Accesos no autorizados a los sistemas de información**

Como parte de las políticas de seguridad de la información aprobadas por la dirección general, la entidad cuenta con una política de bloqueo de cesión de los equipos cada 5 minutos de inactivad. 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.

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.

MATRIZ DE RIESGOS

En la *figura 2*, se relaciona la matriz de probabilidad e impacto de los riesgos de seguridad digital de la entidad.

Probabilidad \ Impacto	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
5	0	0	0	0	0
Casi cierto	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
4	0	0	0	0	0
Probable	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
3	0	3	0	0	0
Posible	BAJO	MODERADO	ALTO	EXTREMO	EXTREMO
2	0	4	7	0	0
Poco Probable	BAJO	BAJO	MODERADO	ALTO	EXTREMO
1	2	2	0	0	0
Raro	BAJO	BAJO	MODERADO	ALTO	ALTO
TOTAL	BAJO	MODERADO	ALTO	EXTREMO	
	8	10	0	0	

DISTRIBUCIÓN DE RIESGOS - Inherente	
ZONA DE RIESGO	TOTAL
EXTREMO	0
ALTO	0
MODERADO	10
BAJO	8
TOTAL	18

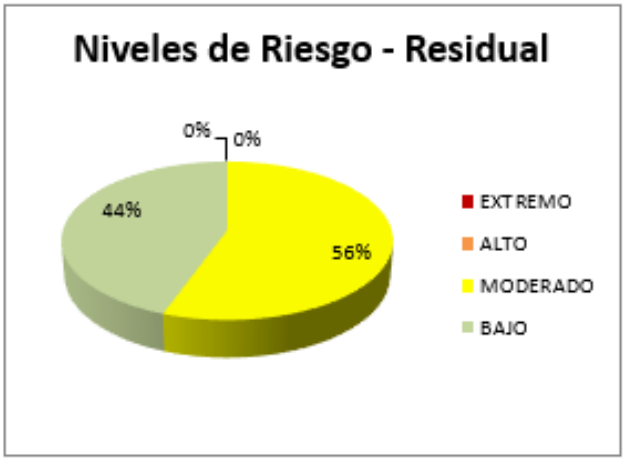

Figura 2. Matriz de Probabilidad e Impacto de riesgos de seguridad digital

La anterior distribución de riesgos de seguridad digital según la probabilidad y el impacto, se calculan los valores a partir del mapa de riesgo de seguridad digital de la entidad con código documental **ES-MR-006** del 23/06/2023 *(Ver Anexo).*

IDENTIFICADOR RIESGO	PROBABILIDAD	VALOR	IMPACTO	VALOR	VALORACIÓN	ZONA RIESGO
R1	Poco probable	2	Moderado	3	6	MODERADO
R2	Raro	1	Insignificante	1	1	BAJO
R3	Raro	1	Menor	2	2	BAJO
R4	Poco probable	2	Moderado	3	6	MODERADO
R5	Posible	3	Menor	2	6	MODERADO
R6	Raro	1	Insignificante	1	1	BAJO
R7	Poco probable	2	Moderado	3	6	MODERADO
R8	Raro	1	Menor	2	2	BAJO
R9	Poco probable	2	Menor	2	4	BAJO
R10	Posible	3	Menor	2	6	MODERADO
R11	Poco probable	2	Menor	2	4	BAJO
R12	Poco probable	2	Moderado	3	6	MODERADO
R13	Poco probable	2	Menor	2	4	BAJO
R14	Poco probable	2	Menor	2	4	BAJO
R15	Poco probable	2	Moderado	3	6	MODERADO
R16	Poco probable	2	Moderado	3	6	MODERADO
R17	Posible	3	Menor	2	6	MODERADO
R18	Poco probable	2	Moderado	3	6	MODERADO

Tabla 6. Clasificación de la zona de riesgo

En la *tabla 6* se muestra la clasificación de la zona del riesgo, de los activos de servicios TI de la entidad, donde se encuentran 18 Riesgos, de los cuales, a través de la matriz de riegos y el mapa de calor, obtenemos el impacto y la probabilidad, siguiendo la siguiente criticidad del riesgo.

CRITICIDAD DEL RIESGO

Extremo: Compromete la viabilidad de la entidad, la cristalización del riesgo podría llevarla a su desaparición. Las pérdidas son tan extremas que la destrucción de valor puede ser total. Existe muy baja o nula capacidad de respuesta frente al riesgo.

Alto: Compromete seriamente a la organización, la cristalización del riesgo puede llevarla a una intervención del estado como garante, frente a los terceros afectados. Las pérdidas son muy significativas, al punto de poner en duda la viabilidad futura de la institución, puede decirse que la destrucción de valor es muy significativa. Existe baja o moderada capacidad de respuesta frente al riesgo, pero requiere de un plan de acción inmediato avalado por la alta gerencia.

Moderado: Compromete a la entidad, aunque no tan significativamente, la cristalización del riesgo puede llevarla al reconocimiento de pérdidas, puede convertirse en un impacto mayor. Las pérdidas pueden corregirse, sin comprometer la viabilidad futura de la entidad. Existe capacidad de respuesta, puede decirse que la destrucción de valor podría ser significativa si no son efectivas las estrategias de mitigación del riesgo.

Bajo: Podría llegar a comprometer a la entidad de alguna manera, la cristalización del riesgo puede llevarla al reconocimiento de algunas pérdidas, que deben controlarse tácticamente. Existe plena capacidad de reacción para la mitigación del riesgo. La entidad podría convivir con el riesgo, sin embargo, cuando sea prudente la implementación de medidas correctivas, deben adoptarse para prevenir una eventual destrucción de valor de la institución.

La *tabla 7* muestra la descripción de la probabilidad de ocurrencia del riesgo según el mapa de calor de la matriz de riesgos de seguridad digital de la entidad.

CLASIFICACIÓN	FACTOR RELATIVO	CARACTERÍSTICA
Casi Cierto	5	La expectativa de ocurrencia se da en todas las circunstancias
Probable	4	Probabilidad de ocurrencia en la mayoría de las circunstancias
Posible	3	Puede ocurrir
Poco probable	2	Podría ocurrir algunas veces
Raro	1	Puede ocurrir bajo ciertas circunstancias excepcionales

Tabla 7. Probabilidad de Ocurrencia del riesgo

La *tabla 8* describe el nivel de impacto del riesgo dentro del mapa de calor, definido por la matriz de seguridad digital de la entidad.

CLASIFICACIÓN	RELATIVO	CARACTERÍSTICA
Insignificante	1	Pérdidas de reputación e imagen mínimas, pérdidas económicas mínimas
Menor	2	No tiene impacto potencial sobre la funcionalidad del servicio ni compromete la imagen de Entidad.
Moderado	3	Impacto sobre la funcionalidad del servicio o sobre la imagen de la entidad, cuyas consecuencias pueden ser absorbidas y subsanadas en el desarrollo normal del proyecto.
Mayor	4	Impacto sobre la funcionalidad del servicio o sobre la imagen de la entidad, cuyas consecuencias NO pueden ser absorbidas y subsanadas en el desarrollo normal del proyecto.
Catastrófico	5	Afecta gravemente la imagen de la entidad. Generando riesgo reputacional.

Tabla 8. Niveles de Impacto del riesgo

ZONA DE RIESGO	CANTIDAD
Extremo	0
Alto	0
Moderado	10
Bajo	8
TOTAL	18

Tabla 9. Zona de riesgo

La *tabla 9* muestra la cantidad de riesgos de la matriz de seguridad digital según la zona riesgo residual, donde 10 riesgos están en nivel moderado y 8 riesgos en nivel bajo.

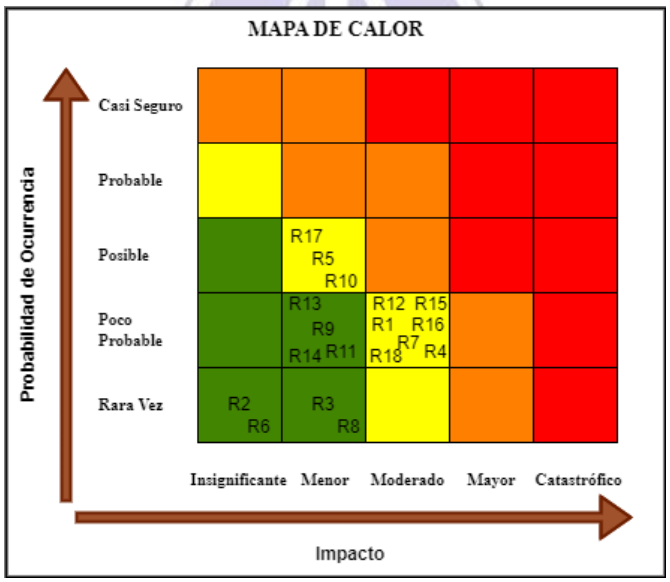

Tabla 10. Distribución de Riesgos de la entidad en el mapa de calor

En la *tabla 10* se muestra la distribución de los 18 riesgos de la entidad identificados en la matriz de riesgos de seguridad digital, donde se clasifican según su probabilidad de ocurrencia e impacto de cada riesgo, siguiendo sus niveles característicos.

IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DIGITAL

Conforme lo indica el 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. (Mintic, 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 de desempeño del MSPI.
- Las actividades de mejoramiento continuo en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

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

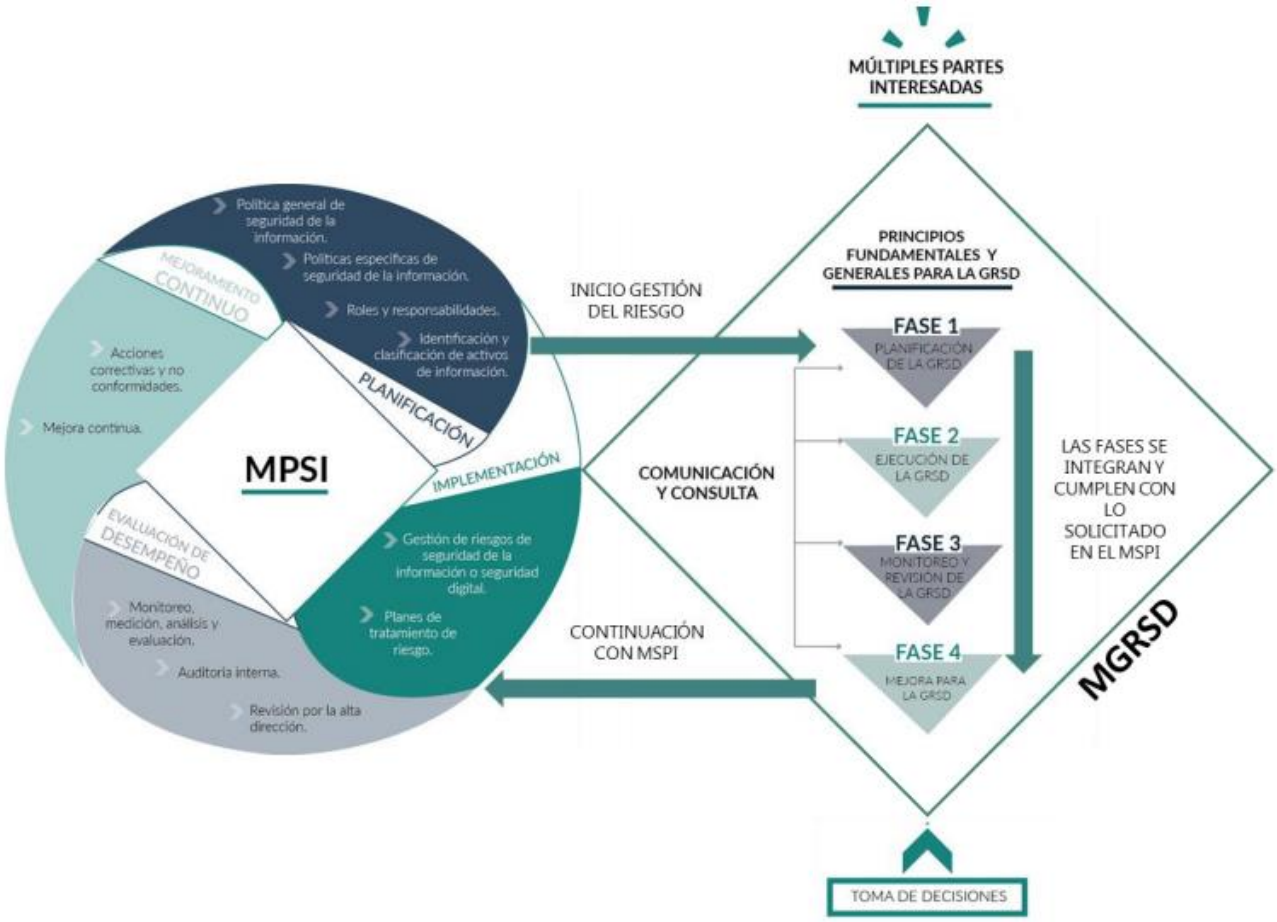

Figura 3. Ilustración entre el MSPI y el MGRSD
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

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).

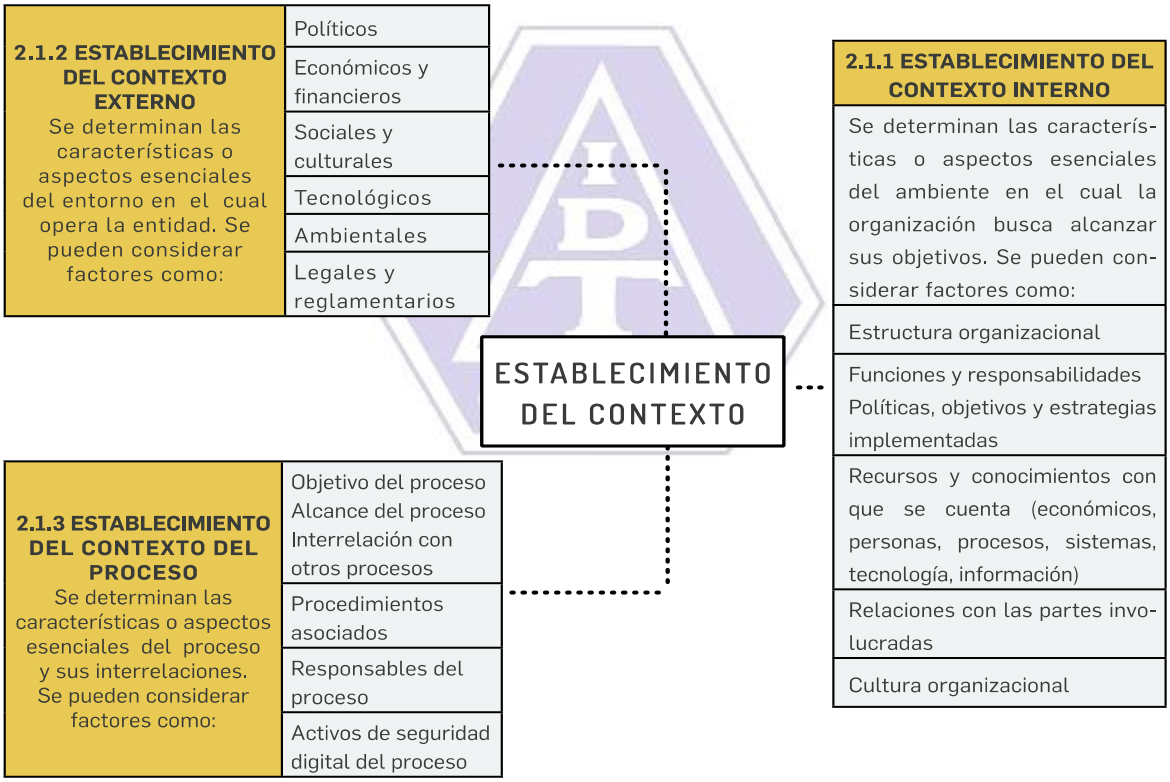

Figura 4. Contexto interno y externo de la entidad
Fuente: (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018)

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 entidad, debe contemplar medidas de protección de dicha información de modo que no se vea afectada la integridad y buen nombre de las personas.

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".

Por esta razón a esto, la entidad está comprometida con la identificación y clasificación de todo tipo de información que es creada, almacenada, administrada y 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 14 de Junio de 2018 estableció el decreto 1008 *"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"* 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 entidad 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.

CONTEXTO INTERNO

Dentro de las funciones de la oficina de sistemas están 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 la entidad, para el uso de sus aplicativos misionales que fortalecen la entidad y atención a la ciudadanía.

Teniendo en cuenta lo anterior 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 el Instituto Departamental de Tránsito del Quindío, que se procesa, que es almacenada y se trasmite, previniendo la materialización de amenazas que puedan impactar de forma considerable la información concerniente a los ciudadanos y funcionarios propios de la entidad.

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 entidad 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.

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 entidad con código según el archivo documental **AF-MP-003**, 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.

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 referencia el plan de capacidades TI, el catálogo de servicios tecnológicos y sus fichas de servicio TI, que cuenta la entidad, en la *figura 5* muestra los pasos para la identificación, construcción y valoración de los activos de información de la entidad.

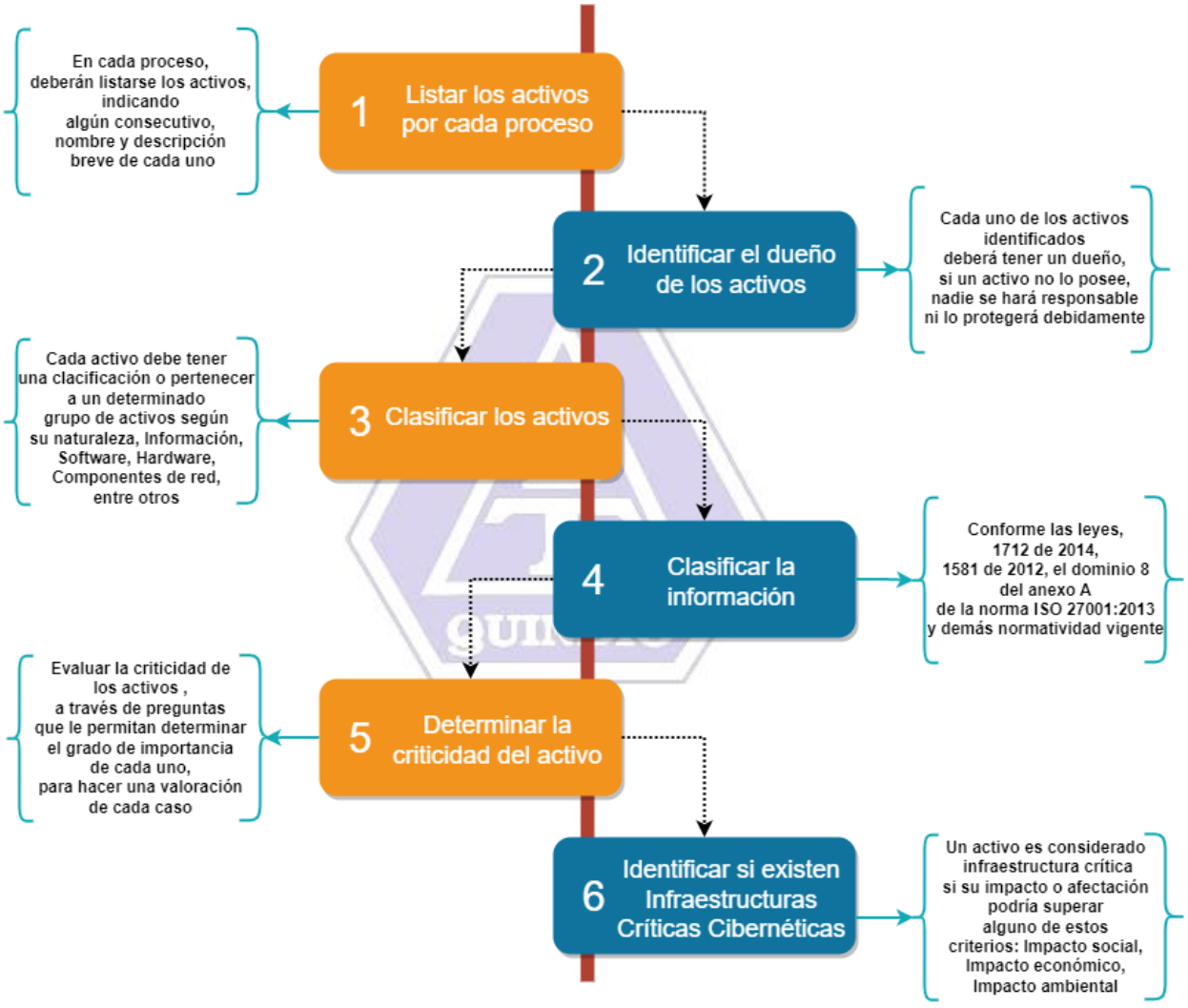

Figura 5. Pasos para la identificación y valoración de activos

FASE DE IMPLEMENTACIÓN

Actualmente desde el Instituto Departamental de Tránsito del Quindío, se realiza un control sobre los riesgos identificados en la *tabla 10 (*distribución de riesgos de la entidad en el mapa de calor), reduciendo así la posibilidad de que los riesgos puedan materializarse.

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 entidad, en lo concerniente a controles tecnológicos e informáticos, también será necesario contar con el apoyo y compromiso del responsable de la seguridad digital (Oficina de sistemas) que brinde conocimiento, apoyo y experticia en la aplicación de los controles.

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.

En cuanto a los controles asociados con la seguridad de la información, las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la **ISO/IEC 27001:2013**, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

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.

A continuación, se incluyen algunos ejemplos de controles para el riesgo de seguridad digital y los dominios a los que pertenecen.

Procedimientos operacionales y responsabilidades	**Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información**
Procedimientos de operación documentados	**Control:** los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	**Control:** se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	**Control:** para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	**Control:** se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

Protección contra códigos maliciosos	**Objetivo:** asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	**Control:** se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	**Objetivo:** proteger la información contra la perdida de datos.
Respaldo de información	**Control:** se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Tabla 11. Controles para riesgos de seguridad digital
Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018

Acorde con el control seleccionado como se muestra en la *tabla 11*, será necesario considerar las características de diseño y ejecución definidas para su valoración.

REPORTE Y SOCIALIZACIÓN DE RIESGOS DE SEGURIDAD

La entidad 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.

El Instituto Departamental de Tránsito del Quindío, trabajará de manera eficaz con los funcionarios, jefes de proceso y el área de sistemas 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, para que controles ayuden a la protección de los distintos activos de información.

Se realizará la comunicación respectiva, con el plan de sensibilización y comunicación de las políticas de seguridad y privacidad 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 del instituto.

AUDITORÍAS INTERNAS Y EXTERNAS

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

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

El Instituto Departamental de Tránsito del Quindío, 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.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Bryan Johann Aranzazu Medina Cargo: Ingeniero Contratista Fecha: 06-07-2023	Nombre: Jorge Mauricio Pardo Ruiz Cargo: PU Oficina Sistemas Fecha: 06-07-2023	Nombre: Jorge Mauricio Pardo Ruiz Cargo: PU Oficina Sistemas Fecha: 06-07-2023