SECRETARÍA
TIC Y CTEI

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC) Y DE CIENCIA, TECNOLOGÍA E INNOVACIÓN (CTEI)

ALCALDÍA MUNICIPAL DE CAJICÁ

CAJICÁ 2024

TABLA DE CONTENIDO

.

.

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

GLOSARIO

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Análisis del Riesgo: Proceso cuyo objetivo es comprender la naturaleza del riesgo y determinar el nivel de riesgo. NOTA 1: El análisis de riesgo proporciona la base para la valoración del riesgo y las dimensiones con respecto al tratamiento del riesgo. NOTA 2: El análisis del riesgo incluye la estimación del riesgo. (ISO/IEC Guía 73:2009, IDT)

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

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: Da el resultado en donde se ubica el riesgo por cada activo de información.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Aceptación de riesgo: Decisión de asumir un riesgo Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Control: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.
Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Efecto de la incertidumbre sobre el cumplimiento de los objetivos.

Tratamiento del riesgo: Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

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.

Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

Riesgo residual: Nivel restante de riesgo después del tratamiento del riesgo.

Valoración del riesgo: Proceso de análisis y evaluación del riesgo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Ingeniería Social: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social

Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

1. OBJETIVO

Definir los lineamientos mediante los cuales se realizará la gestión de riesgos de seguridad digital en la Alcaldía de Cajicá, la cual debe incluir amenazas, vulnerabilidades, riesgos, controles, niveles aceptables de riesgo y el tratamiento de riesgos.

2. ALCANCE

Establecer la hoja de ruta para la implementación del plan de tratamiento de riesgos de seguridad digital, siendo aplicable a todos los procesos, funcionarios y contratistas de la Entidad, basado en la guía para la administración del riesgo en el diseño de controles del Departamento Administrativo de Función Pública-DAFP V5 y en la norma ISO/IEC 27001-2017.

3. METODOLOGÍA DE GESTIÓN DE RIESGO

La metodología para la administración y gestión de riesgos está basada en las directrices definidas por el Departamento Administrativo de la Función Pública - DAFP el cual plantea las directivas de gestión, definición, aplicación, desarrollo e implantación de los sistemas de calidad y gestión a partir del enfoque de riesgos.

De esta manera, la etapa inicial propuesta por el DAFP, comienza con un análisis relacionado con el estado actual de los riesgos y su gestión dentro de la Entidad, haciendo especial énfasis en el conocimiento de ésta, desde un punto de vista estratégico, pero teniendo en mente todo el modelo de riesgos que busque la disminución del impacto en el caso de materialización de alguno de ellos y propendiendo por la continuidad del negocio.

La gestión de riesgos ofrece para la Alcaldía de Cajicá un método sistemático para analizar los riesgos derivados de los procesos que la componen con un especial énfasis en las tecnologías de la información y comunicaciones usadas en la Entidad, con el objetivo de descubrir, valorar, planificar y adelantar el tratamiento oportuno que busque mantener los riesgos en niveles óptimos de control y así preparar a la entidad para una posible materialización de alguno de los riesgos y dentro de la misma línea, poder adelantar procesos de evaluación, auditoría, certificación o acreditación, según corresponda.

3.1 Identificación y Valoración de los Activos de Información

3.1.1 Identificación de Activos de Información

Un “activo de información” se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido. Por consiguiente, la primera actividad en la Gestión de Riesgos es identificar los activos de información bajo las consideraciones que la Entidad defina, actividad que debe realizarse sin perder de vista el alcance definido y aprobado por la alta dirección para el Sistema de Gestión de Seguridad de la Información (SGSI) o en el caso de la Alcaldía municipal de Cajicá el Modelo de Seguridad y Privacidad de Información - MSPI.

En este sentido, las actividades necesarias para la identificación de los activos de información y su formalización dentro de la entidad son:

1. Definir el instrumento de captura de información identificando las variables que se deben capturar.
2. Identificar los procesos y agendar las entrevistas con sus responsables.
3. Recolectar la información necesaria bajo las consideraciones definidas por la Entidad.
4. Realizar los cruces necesarios con otras fuentes de información como inventarios, Tablas de Retención Documental, entre otros, para completar información.
5. Consolidar la información.

Para adelantar esta primera etapa se debe tener en cuenta la definición de la siguiente información, con el fin de poder tener parámetros precisos frente a la captura y consolidación de la herramienta de trabajo.

3.1.2 Identificación de Propietario, custodio, responsable y ubicación

Los activos de información previamente identificados en el paso anterior deben tener su respectivo propietario, definido como la dependencia o proceso donde se crea o custodia dicho activo. Así mismo, definir el custodio de la información el cual, puede ser el mismo propietario o en su defecto el proceso o la persona que la Entidad haya definido para adelantar dicha tarea.

El responsable es el jefe y/o subdirector de cada dependencia o proceso de uno o un grupo de activos de información y es quien debe velar porque los controles de seguridad sean implementados de manera satisfactoria.

En esta medida la tipología de activos de información está definida en la siguiente tabla:

Tabla 1 Tipología del activo

Tipo de activo	Propiedad del activo	Descripción
Activos de Información Puros	Información digital	Bases de datos y archivos, documentos de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, entre otros
	Información física	
	Activos de Información intangibles	
Activos de Tecnologías de Información	Servicios de información	Equipamiento informático, servicios informáticos y de comunicaciones, utilitarios generales (aire acondicionado, iluminación, energía eléctrica, entre otros), software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, entre otros.
	Software	
	Hardware de TI	
	Controles ambientales	
Activos de Información Recurso Humano	Funcionarios y servidores públicos	recursos humanos, funcionarios de la entidad, contratistas.
	Terceros	

3.1.3 Categorización de la Información

La Entidad cuenta con una categorización para el etiquetado de la información, la cual se ha establecido al interior de la entidad con los siguientes criterios:

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de Entidad y debe estar a disposición de cualquier persona natural o jurídica del estado colombiano.

Información pública clasificada: "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014."

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 18 de la ley 1712 del 2014.

Datos Personales: Cualquier información vinculada o que pueda asociarse con los datos públicos y no públicos de una o varias personas naturales o jurídicas, de acuerdo con la ley estatutaria 1581 de 2012.

3.1.4 Valoración de los Activos de Información

Los activos de información deben ser valorados de acuerdo a su impacto en términos de la pérdida de las tres (3) propiedades básicas de la seguridad de la información que son la confidencialidad, integridad y disponibilidad, definidos a partir de la norma ISO/IEC 27001:2013.

Confidencialidad: Es la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Integridad: Es la propiedad de salvaguardar la exactitud y estado completo de los activos de información.

Disponibilidad: Es la propiedad de que la información sea accesible y utilizable por solicitud de un individuo o entidad autorizada cuando se requiera.

Dada las anteriores definiciones, se establecen las escalas para la confidencialidad, integridad y disponibilidad respectivamente.

Tabla 2. Valoración de la confidencialidad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBILCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Tabla 3. Valoración de la integridad

Alta	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
Media	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad
Baja	Información cuya pérdida de exactitud y completitud conlleva un impacto no

	significativo para la entidad o entes externos
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA

Tabla 4. Valoración de la disponibilidad

Alta	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos
Media	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad
Baja	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen
No clasificada	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

4. ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

4.1 Identificación de las amenazas

De acuerdo con la ISO 27005, las amenazas pueden ser de origen natural o humana y pueden ser accidentales o deliberadas y ambas deben ser identificadas. Las amenazas pueden surgir desde dentro o fuera de la organización y algunas pueden afectar a más de un activo. En este caso, pueden causar diferentes impactos dependiendo de los activos afectados.

Las amenazas deben identificarse de manera genérica y por tipo: luego, cuando sea apropiado, se identificarán las amenazas individuales dentro de la clase genérica. Esto significa que no se pasa por alto ninguna amenaza.

Las siguientes son tablas de ejemplo y pueden usarse durante la identificación y evaluación de amenazas.

Donde las siglas del origen hacen referencia a:

- A: Accidental (Accidental), se usa para todas las acciones humanas que pueden accidentalmente dañar activos de información.

- D: Deliberado (Deliberate), se utiliza para todas las acciones deliberadas dirigidas a los activos de información.

- E: Ambiental (Environmental), se usa para todos los incidentes que no son basados en acciones humanas.

Tabla 5. Amenazas comunes por tipo

TIPO	AMENAZAS	ORIGEN
Daño Físico	Fuego	A, D, E
	Daño por Agua	A, D, E
	Polución	A, D, E
	Destrucción de equipos o dispositivos	A, D, E
	Accidentes mayores	A, D, E
	Polvo, Corrosión, Congelamiento	A, D, E
Eventos Naturales	Fenómenos climáticos	E
	Fenómenos Sísmicos	E
	Fenómenos Meteorológicos	E
	Inundaciones	E
Perdida de servicios esenciales	Falla de aire acondicionado	A, D
	Falla en el suministro de energía	A, D, E
	Falla de equipo de telecomunicaciones	A, D
Información comprometida	Interceptación de señales de interferencia	D
	Espionaje remoto	D
	Robo de documentación o medios de información	D
	Robo de equipos	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos de fuentes no confiables	A, D
	Manipulación de hardware	D
	Manipulación de software	A, D
Fallas técnicas	Falla de equipos	A
	Equipos defectuosos	A
	Saturación del sistema de información	A, D
	Funcionamiento erróneo del software	A

	Brechas en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado de equipos	D
	Copia fraudulenta de software	D
	Uso de software falsificados	A, D
	Datos corruptos	D
	Procesamiento ilegal de datos	D
Compromiso de funciones	Error en uso	A
	Abuso de derechos o permisos	A, D
	Falsificación de derechos o permisos	D
	Negación de acciones	D
	Violación de la disponibilidad de personal	A, D, E

Fuente: Adoptado de ISO 27005:2018

Aparte de las amenazas por tipo, se debe prestar especial atención a las fuentes de amenaza humana, como se listan en la tabla 6.

Tabla 6. Tabla de amenazas dirigida por el hombre

ORIGEN DE LA AMENAZA	MOTIVACIÓN	POSIBLES CONSECUENCIAS
Hacker	Reto o desafío Ego Rebelión Estatus Dinero	Hackeo Sistema de intrusión (Robo) Sistema de acceso no autorizado Ingeniería Social
Delincuencia informática	Destrucción de información Divulgación ilegal de información Ganancia económica (Dinero) Alteración de datos no autorizada	Acecho cibernético Actos de fraudulencia Soborno informativo Suplantación de identidad Sistema de intrusión
Terrorismo	Chantaje Destrucción Explotación Venganza Beneficio político Cobertura mediática	Terrorismo Guerra informática Ataques al sistema Penetración del sistema Manipulación del sistema

Ventaja competitiva	Interceptación de señales de interferencia Espionaje económico Robo de documentación o medios de información Robo de equipos Recuperación de medios reciclados o desechados Divulgación Datos de fuentes no confiables Manipulación de hardware Manipulación de software	Ventaja política Explotación económica Robo de información Intrusión en la privacidad personal Penetración del sistema Acceso no autorizado al sistema (acceso a información clasificada, patentada y/o relacionada con la tecnología)
Motivos de nivel interno (empleados mal entrenados, descontentos, maliciosos, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia económica (dinero) Venganza Errores no intencionados u omisión	Chantaje Información patentada comprometida Fraude y el robo Entrada de datos falsificados y corruptos Intercepción Código malicioso Venta de información personal Errores de sistema Intrusión en el sistema Sabotaje del sistema acceso no autorizado al sistema

Fuente: ISO/IEC 27005:2018

4.2 Identificación de la Vulnerabilidades

Las vulnerabilidades de los activos de información son debilidades que son aprovechadas por amenazas y generan un riesgo. Una vulnerabilidad que no tiene una amenaza asociada puede no requerir de la implementación de un control; sin embargo, es necesario identificarla y monitorearla. Es importante tener en cuenta que un control mal diseñado e implementado puede constituir una vulnerabilidad.

La identificación de las vulnerabilidades se basa en los resultados de las pruebas de hacking ético, entrevistas con los responsables de los activos de información y serán registradas en la matriz de riesgos.

Tabla 7 Vulnerabilidades Comunes

TIPO	VULNERABILIDADES
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de remplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoria
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envió o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Trafico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo de limpieza
Lugar	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/ retiro de usuarios
	Ausencia de proceso para supervisión de

	derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas de seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantallas limpias entre otros)

Fuente: ISO/IEC 27005:2009

4.3 Identificación de Riesgos

Los riesgos en seguridad de la información se identifican mediante las pruebas de seguridad, identificación por parte de los funcionarios quienes tienen claridad y han experimentado la materialización de algunos riesgos en sus procesos y finalmente por la experiencia del personal que gestiona los riesgos o el sistema.

Los riesgos se relacionan con las vulnerabilidades y amenazas de cada activo de información los cuales se encuentran listados en la matriz de riesgos, bajo la tipología definida a continuación:

Tabla 8. Tipología de riesgos

Riesgos estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización publica y por tanto impactan toda la entidad.
Riesgos gerenciales	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos operativos	posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos financieros	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería,

	contabilidad, cartera, central de cuentas, costos, etc.
Riesgos tecnológicos	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgo de imagen o reputaciones	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
Riesgos de corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos de Seguridad Digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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

4.4 Análisis de la Probabilidad

Se realiza el análisis de la posibilidad de ocurrencia de un riesgo y se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos ocurridos en un período determinado, tratando los hechos que se han materializado o que se cuente con un historial de situaciones o eventos asociados al riesgo (información histórica); factibilidad por su lado, implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, tratándose en este caso, de un hecho que no se han presentado pero es posible que suceda.

Para poder adelantar la valoración de la probabilidad en los casos que no haya información dentro de la entidad, se puede entrar a definir a partir de datos de referencias externas (otras entidades o mercado) o finalmente por el criterio de una persona experta en riesgos o en seguridad de información. Cabe resaltar que dicha probabilidad debe ser determinada por el

responsable del proceso de acuerdo a su experiencia y asociado a la vulnerabilidad detectada sobre un activo de información específico y de acuerdo a la amenaza definida.

Los criterios para calificar la probabilidad se describen a continuación:

Ilustración 1.Criterios para definir el nivel de la probabilidad

	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%

Fuente Guía DAFP V5

4.5 Determinar el Impacto

El impacto está determinado por el valor máximo de la calificación registrada en términos de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) de los activos de información.

Ilustración 2.Matriz Guía Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente Guía DAFP V5

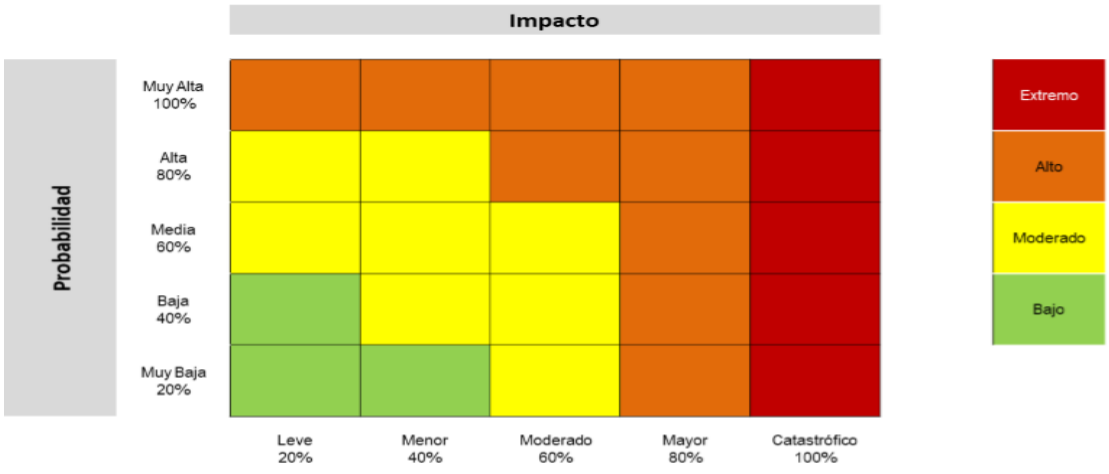
5. EVALUACIÓN DE RIESGOS

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

5.1. Análisis preliminar (riesgo inherente)

se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Ilustración 3. Medición Riesgos Inherentes



Fuente Guía DAFP V5

Una vez determinado los niveles de probabilidad e impacto estos deben ser cruzados en la matriz de calor, para determinar el nivel de severidad del riesgo como se indica en la ilustración.

5.2. Controles

La guía del DAFP define un control como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos, funcionarios o contratistas basado en su experiencia y conocimiento.

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

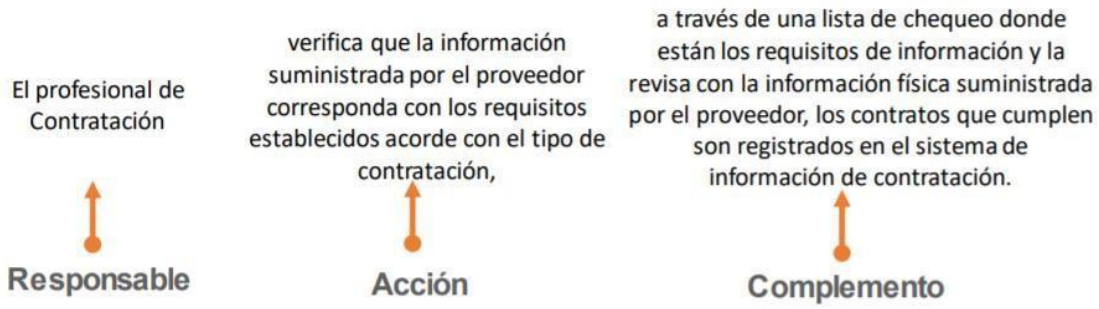
La guía del DAFP propone una estructura para la descripción de controles sé que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Responsable de ejecutar el control: identifica el responsable que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ilustración 4. Ejemplo redacción de un control



Fuente Guía DAFP V5

Los controles se clasifican de la siguiente manera:
Control preventivo: para evitar que la amenaza entre en contacto con la debilidad
Control detective: para identificar que la amenaza ha aterrizado en nuestros sistemas.
Control correctivo: para mitigar o disminuir los efectos de la amenaza que se manifiesta.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

Control manual: controles que son ejecutados por personas.
Control automático: son ejecutados por un sistema.

Tabla 9.Ejemplo clasificación de controles

PREVENTIVOS	DETECTIVOS	CORRECTIVOS
Concientización en la seguridad	Sistemas de monitoreo de red	Actualización de Sistema Operativo
Firewalls	IDS	Restaurar copias de respaldo en caliente
Antivirus	Antivirus	Aislamiento del servidor
Controles de acceso	Detectores de humo/ presencia	Mitigación de la vulnerabilidad

6. DECLARACIÓN DE APLICABILIDAD

De acuerdo con la guía 8 del Min tic - Controles de Seguridad de la Información, La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

- La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

- La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

Dentro de las actividades a seguir, después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, esto con la finalidad de definir las actividades necesarias para la aplicación de los controles de seguridad.

A continuación, se presenta un ejemplo de formato de Declaración de aplicabilidad:

Ilustración 5. Formato ejemplo declaración de aplicabilidad

		Objetivo de control o control seleccionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta dirección Firma director de la entidad
Dominio	A.5 Políticas de seguridad de la información						
Objetivo de control	A. 5.1 Directrices establecidas por la dirección para la seguridad de la información						
Control	A. 5.1.1 Políticas para la seguridad de la información						
Control	A. 5.1.2 Revisión de las políticas para seguridad de la información						

Fuente Guía 8 del Mintic- Controles de Seguridad y Privacidad de la Información

7. TRATAMIENTO DE RIESGO

7.1. Opciones de Tratamiento de Riesgo

Es la respuesta establecida por la primera línea defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad impacto de este y la relación costo-beneficio de las medidas de tratamiento.

Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la Secretaria, se deberá volver analizar y revisar dicho riesgo.

Con base en los resultados del análisis de riesgos se puede asumir una de las siguientes acciones:

Tabla 10 Clasificación del riesgo

BAJA	Aceptar el riesgo
MODERADA	Reducir el riesgo
ALTA	
EXTREMA	Evitar el riesgo

Aceptar el riesgo: no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

Reducir el riesgo: se adoptan medidas para reducir la probabilidad o el impacto del riesgo o ambos; por lo general conlleva a la implementación de controles.

Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

7.2. Herramientas para la Gestión del Riesgo

Producto de la aplicación de la metodología se contará con la matriz de riesgo. Además de esta herramienta, se tienen las siguientes:

Gestión de eventos: Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- Mesa de Servicio
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica

7.3. Riesgo Residual

Es aquel riesgo que subsiste, después de haber implementado controles. Es importante advertir que el nivel de riesgo al que está sometida la entidad nunca puede erradicarse. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es

preciso dedicar para minimizar o mitigar estos riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable). El riesgo residual puede verse como aquello que separa a la entidad de la seguridad absoluta.

El riesgo residual es aquél que permanece después de que la Secretaria desarrolle sus respuestas a los riesgos. El riesgo residual refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas por la Secretaria para mitigar el riesgo inherente.

8. MONITOREO Y REVISIÓN

La valoración de los riesgos de seguridad digital (Matriz de Riesgos de seguridad digital) será revisada continuamente y/o teniendo en cuenta los cambios en:

- La entidad

- La tecnología
- Los procesos de la Entidad
- Aplicación de controles.

Todo control aplicado con el fin de reducir el valor de riesgo calculado debe ser medible a través de su eficacia. La aplicación de un control no necesariamente implica la reducción total del valor de riesgo esperado sino la reducción a los niveles de riesgo aceptables establecidos por la entidad.

La funcionalidad de los controles debe ser constantemente evaluada; en caso de no obtener los resultados esperados se debe aplicar mejoras de acuerdo a la aplicación de la metodología PHVA (Planear, Hacer, Verificar, Actuar).

9. PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de guía para la administración del riesgo en el diseño en controles del Departamento Administrativo de Función Pública-DAFP V5 y en la norma ISO27001-2013.

Tabla 11 Plan Actividades Gestión de Riesgo

ACTIVIDADES	TAREAS	RESPONSABLE DE LA TAREA	FECHAS LÍMITE PROGRAMACIÓN TAREAS
Actualización de lineamientos de riesgos	Implementación y seguimiento a la Política y metodología de Gestión de Riesgos.	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional servidores y seguridad perimetral	junio de 2024
Sensibilización	Socializar la Política Gestión de riesgos de seguridad y privacidad de la información, seguridad digital	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional	julio de 2024

		servidores y seguridad perimetral	
Identificación de riesgos de seguridad y privacidad de la información, seguridad digital	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional servidores y seguridad perimetral	Julio de 2024
	Realimentación, revisión y verificación de los riesgos identificados (ajuste)	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional servidores y seguridad perimetral	Agosto de 2024
Aceptación, riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional servidores y seguridad perimetral	Julio de 2024
Declaración Aplicabilidad	Actualizar la declaración de aplicabilidad	Profesional Gobierno Digital Secretaria de TIC – CteI- profesional servidores y seguridad perimetral	Julio de 2024

Publicación	Publicación interna matriz de riesgos	Profesional Gobierno Digital Secretaria de TIC - CTeI	Agosto de 2024
Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Profesional Gobierno Digital – Ing de Servidores Secretaria de TIC - CTeI	Octubre de 2024
Evaluación riesgos residuales	Evaluación e identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Profesional Gobierno Digital – Ing de Servidores Secretaria de TIC - CTeI	Octubre de 2024
Mejoramiento	Actualización del Plan de tratamiento de riesgos de Seguridad de la Información	Profesional Gobierno Digital Secretaria de TIC - CTeI	Noviembre de 2024
Publicación	Publicación y Sensibilizar el Plan de tratamiento de Riesgos de Seguridad de la Información	Secretaria de TIC – CteI, Prensa y Comunicaciones	Noviembre de 2024

Seguimiento al plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

SEGUIMIENTO AL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN					
ACTIVIDADES	**TAREAS**	**RESPONSABLE DE LA TAREA**	**FECHAS LÍMITE PROGRAMACIÓN TAREAS**	**SEGUIMIENTO AL PLAN**	
				Actividad realizada	**Fecha**
Actualización de lineamientos de riesgos	Implementación y seguimiento a la Política y metodología de Gestión de Riesgos.	Profesional Gobierno Digital Secretaria de TIC y CTeI	Junio de 2024		
Sensibilización	Socializar de la Política Gestión de riesgos de seguridad y privacidad de la información, seguridad digital	Profesional Gobierno Digital Secretaria de TIC CTeI	julio de 2024		
Identificación de riesgos de seguridad y privacidad de la información, seguridad digital	Identificación de riesgos de seguridad y privacidad de la información, seguridad digital	Profesional Gobierno Digital Secretaria de TIC y CTeI	julio de 2024		

	Realimentación, revisión y verificación de los riesgos identificados (ajuste)	Profesional Gobierno Digital Secretaria de TIC y CTeI	Agosto de 2024		
Aceptación, riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Profesional Gobierno Digital Secretaria de TIC y CTeI	Julio de 2024		
Declaración Aplicabilidad	Actualizar la declaración de aplicabilidad	Profesional Gobierno Digital Secretaria de TIC y CTeI	Julio de 2024		
Publicación	Publicación matriz de riesgos interna	Profesional Gobierno Digital Secretaria de TIC y CTeI	Agosto de 2024		
Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y	Profesional Gobierno Digital – Ing. de Servidores Secretaria de TIC y CteL	Octubre de 2024		
Evaluación riesgos residuales	Evaluación e Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Profesional Gobierno Digital – Ing de Servidores Secretaria de TIC - CTeI	Octubre de 2024		

Mejoramiento	Actualización del Plan de tratamiento de riesgos de Seguridad de la Información	Profesional Gobierno Digital Secretaria de TIC - CTeI	Noviembre de 2024		
Publicación	Publicación y Sensibilizar el Plan de tratamiento de Riesgos de Seguridad de la Información	Secretaria de TIC – CteI, Prensa y Comunicaciones	Noviembre de 2024		