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

	INSTITUTO DISTRITAL DE LA PARTICIPACION Y ACCION COMUNAL		
SISTEMA INTEGRADO DE GESTIÓN			
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
CÓDIGO	IDPAC-GTI-PL-01	VERSIÓN	01
ELABORÓ	REVISÓ	APROBÓ	
Maribel Ardila Flórez Contratista José Antonio Chaparro Gómez Profesional Especializado 222 – 04	Paula Lorena Castañeda Vásquez Jefe Oficina Asesora Jurídica Claudia Milena Salcedo Acero Jefe Oficina Asesora de Planeación	Comité Institucional de Gestión y Desempeño	
FECHA	FECHA	FECHA	
16/12/2020	17/03/2021	26/03/2021	

REGISTRO DE MODIFICACIONES		
VERSIÓN	**FECHA**	**ÍTEM MODIFICADO – DESCRIPCIÓN**
01	26/03/2021	Versión Inicial

ALCALDÍA MAYOR DE BOGOTÁ D.C.

IDPAC

BOGOTÁ

TABLA DE CONTENIDO

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

1 INTRODUCCIÓN

De acuerdo con lo contenido en el Modelo de Seguridad y Privacidad de la información - MSPI del IDPAC, un tema decisivo para la toma de decisiones es la Gestión de Riesgos. En concordancia con la IDPAC-PE-GU-01 "*Guía para la Administración del Riesgo del IDPAC*", la administración de riesgos es un método lógico y sistemático que le permite al Instituto minimizar pérdidas y maximizar oportunidades. Es así como todos los servidores públicos del IDPAC, en cumplimiento de sus funciones, y teniendo acceso a los elementos de Tecnologías de la Información – TI, están sometidos a riesgos que pueden hacer fracasar la gestión; por consiguiente, es indispensable tomar las medidas necesarias para identificar las causas y consecuencias de la materialización de estos.

Este documento también toma apartes y recomendaciones de la guía para la administración del riesgo y el diseño de controles en entidades públicas publicado por el Departamento Administrativo de la Función Pública.

2 OBJETIVO

Identificar y prevenir el riesgo buscando proteger los recursos de TI, mejorando la prestación de servicios a los usuarios internos y externos y la creación de las estrategias necesarias para ejecutar las actividades de prevención y correctivas, apoyados en:

- Una política de administración del riesgo, en cabeza de la alta dirección, teniendo aprobación de esta en cada etapa necesaria.
- Una identificación del riesgo de conformidad con la metodología para la evaluación del riesgo, precisando sus factores y su relación con las tipologías, en un trabajo articulado con planeación.
- Valoración del riesgo, buscando establecer los criterios para el análisis de probabilidad e impacto de este previamente identificado y su respectivo nivel de severidad, en este apartado se propone la tabla para el análisis de probabilidad con un enfoque en la exposición al riesgo.
- Capacitación en la metodología y prevención.

Todas las referencias a las políticas, definiciones o contenido relacionado se encuentran publicadas en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

3 METODOLOGIA PARA LA EVALUACIÓN DEL RIESGO

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información. Una buena práctica consiste en realizar gestión de riesgos a estos activos que se consideren con nivel de clasificación ALTA dependiendo de la calificación que se realice, según los criterios de clasificación (confidencialidad, Integridad y Disponibilidad) como se verá a continuación:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADAD	**ALTA (A)**	**ALTA (1)**
INFORMACIÓN PÚBLICA CLASIFICADA	**MEDIA(M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**BAJA(B)**	**BAJA (3)**
INFORMACIÓN NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento.

- Proceso para la administración del riesgo en seguridad de la información

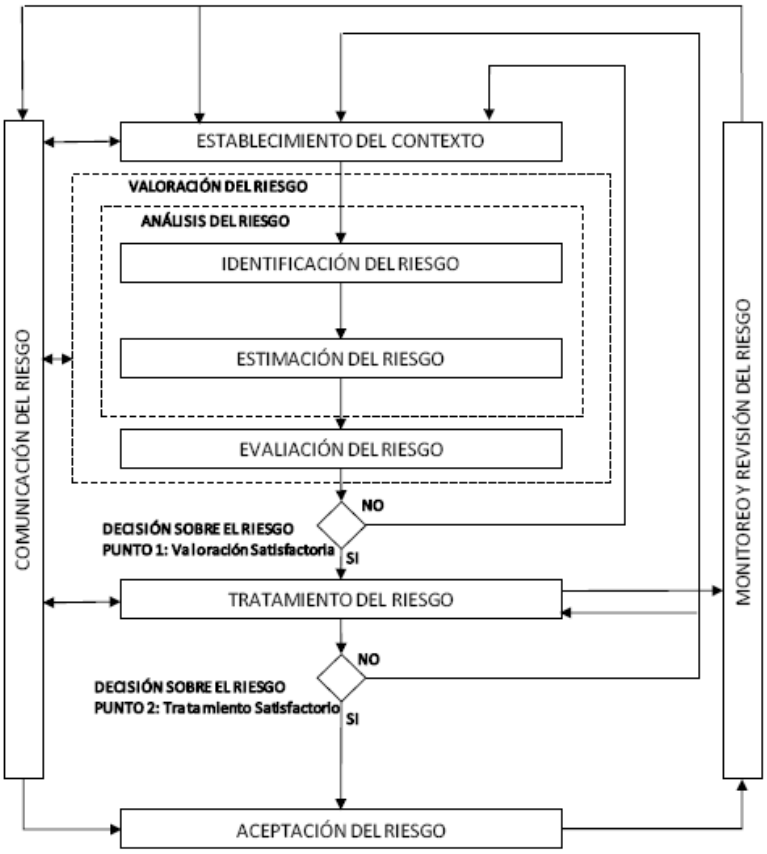

Ilustración 1 Tomado de la NTC-ISO/IEC 27005.

Así como se muestra en la Ilustración 1, el proceso de gestión del riesgo en la seguridad de la información puede ser reiterativo para las actividades de valoración y/o el tratamiento del riesgo.

Como primera medida es necesario establecer el contexto, esto es, la identificación del riesgo en el área de Tecnologías de la información. Luego de ello, se procede con la valoración del riesgo y si del resultado de este análisis se concluye que la información suministrada fue suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable, entonces la labor está terminada y se puede continuar con el tratamiento del riesgo. Pero, si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riesgo con un contexto revisado.

La eficacia del tratamiento del riesgo depende de los resultados de la valoración de este. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, por lo que, de considerarse necesaria, se puede requerir otra iteración de la etapa de valoración con cambios en los parámetros del contexto.

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por la alta o media dirección. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN
PLANEAR	ESTABLECER CONTEXTO
	VALORACIÓN DEL RIESGO
	PLANIFICACIÓN DEL TRATAMIENTO DEL RIESGO
	ACEPTACIÓN DEL RIESGO
IMPLEMENTAR	IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGO
GESTIONAR	MONITOREO Y REVISIÓN CONTINUO DE LOS RIESGOS
MEJORA CONTINUA	MANTENER Y MEJORAR EL PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFROMACIÓN

El Plan de Tratamiento de Riesgos del IDPAC contempla las actividades a desarrollar en pro de la mitigación de los riesgos de TI.

4 DEFINICIONES

Activo de información: Conocimiento o información que tiene valor para el individuo u organización.

Amenaza: Situación externa que no controla la entidad y que puede afectar su operación.
Riesgo: Efecto que se causa sobre los objetivos de las entidades debido a eventos potenciales.

Eventos Potenciales: Hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, procesos, tecnología, infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos de los procesos o sobre su operación.

Riesgo institucional: Son los riesgos que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen alguna de las siguientes características:

- Son clasificados como riesgos estratégicos
- Los riesgos que después de la evaluación residual se ubican en zona alta o extrema.
- Los riesgos que tengan incidencia directa en el usuario o destinatario final externo.
- Los riesgos de corrupción.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de los 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.

Control: Medida que permite reducir o mitigar un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Factores de Riesgo: Son las fuentes generadoras de riesgos

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

Integridad: Propiedad de exactitud y completitud.

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

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron.

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.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

5 MARCO NORMATIVO:

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

CONPES 3854 de 2016: Política Nacional de Seguridad Digital.

Manual para la Implementación de la Política de Gobierno Digital: Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019.

Modelo de Seguridad y privacidad de la información – MSPI: Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

NTC / ISO 27001:2013: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009: Gestión del Riesgo. Principios y directrices.

Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5 Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública diciembre 2020.

Guía para la Gestión y Clasificación de Activos de Información de MinTIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital.

6 GESTIÓN DE RIESGOS.

Corresponde a un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance de los objetivos del IDPAC.

6.1 IDENTIFICACIÓN DEL RIESGO

El IDPAC realizó la identificación de los principales riesgos asociados a TI:

- **Pérdida o modificación de información en medios digitales:** asociados a documentos producidos por las áreas, oficinas asesoras, dirección y subdirecciones y secretaria General del IDPAC, de acuerdo con el inventario de activos; Sistemas de Información, aplicativos, bases de datos, portal y páginas web, intranet, Servidores de datos, equipos de cómputo,

discos duros externos, sistemas de *backup* y recuperación, nube, almacenamiento interno y externo.

- **No disponibilidad de los servicios ofrecidos de tecnología de la información:** asociado fallas en canales de comunicación, caídas de servicios como nube, telefonía IP, canales de *backup*, acceso a las bases de datos, carpetas compartidas, almacenamiento, fallas en equipos de red activos y pasivos.

- **Fallas en las telecomunicaciones:** asociado a las comunicaciones ofrecidas por proveedores externos que contemplan los canales de datos que unen las diferentes sedes del IDPAC, las canales de navegación de Internet, servicios en la nube, telefonía IP, canales de backup, que pueden ocasionar fallas en los servicios de atención al ciudadanos, acceso a las bases de datos, interrupción de todos los procesos relacionados, pagos, nomina, correspondencia y tesorería, así como atrasos en contratación y demás actividades que se desarrollen en las diferentes dependencias del Instituto.

6.2 CLASIFICACIÓN

Al respecto, se debe tener en cuenta que la criticidad de los activos de información fue valorada de acuerdo con la Guía para la Gestión y Clasificación de Activos de Información de MinTIC, referenciada en el Anexo 4 para Riesgos de Seguridad Digital, midiéndose por los tres pilares de la seguridad de la información "CONFIDENCIALIDAD", "INTEGRIDAD", "DISPONIBILIDAD" según la clasificación que determina el numeral 7 de dicha Guía, de la siguiente manera:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

6.3 ACTIVIDADES:

Las actividades que se relacionan a continuación se realizarán conforme a los manuales y procedimientos para el tratamiento de los riesgos adoptados por del sistema de gestión del IDPAC en el marco de los lineamientos del Modelo Integrado de Planeación y Gestión - MIPG.

6.3.1 Identificación de amenazas

Eventos que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos, pueden desencadenar o explotar una vulnerabilidad para comprometer algún aspecto del activo.

Listado de amenazas y vulnerabilidades en ISO 27001

- Acceso a la red o al sistema de información por personas no autorizadas.
- Amenaza o ataque con bomba.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Comprometer información confidencial.
- Ocultar la identidad de un usuario.
- Daño causado por un tercero.
- Daños resultantes de las pruebas de penetración.
- Destrucción de registros.
- Desastre generado por causas humanas.
- Desastre natural, incendio, inundación, rayo.
- Revelación de información.
- Divulgación de contraseñas.
- Malversación y fraude.
- Errores en mantenimiento.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Espionaje industrial.
- Fuga de información.
- Interrupción de procesos de negocio.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.
- Mal funcionamiento del equipo.
- Código malicioso.
- Uso indebido de los sistemas de información.
- Uso indebido de las herramientas de auditoría.
- Contaminación.
- Errores de software.
- Huelgas o paros.
- Ataques terroristas.
- Hurtos o vandalismo.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Instalación no autorizada de software.
- Acceso físico no autorizado.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.

- Error de usuario.

6.3.2 Identificación de vulnerabilidades

Las vulnerabilidades se refieren a los defectos o debilidades en un activo.

Listado de vulnerabilidades en ISO 27001

- Interfaz de usuario complicada.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.
- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.
- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.
- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.

- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.

Las amenazas y vulnerabilidades contempladas en ISO 27001 deben ser correctamente identificadas y constituyen un aspecto clave del sistema de seguridad y privacidad de la información del IDPAC. Las amenazas y vulnerabilidades en ISO 27001 van de la mano y, por esa razón, se deben considerar en su conjunto.

6.3.3 Evaluar los controles establecidos para la mitigación de los riesgos en el IDPAC.

La evaluación de los controles se debe realizar cuando se ha establecido el riesgo inherente para los procesos, junto con el impacto y probabilidad de ocurrencia de cada uno de los riesgos establecidos. La evaluación de controles en el IDPAC se debe llevar a cabo identificando los criterios relacionados a cada uno de los riesgos establecidos ya descritos. Para ello se establecen las características que permiten establecer un seguimiento y verificación de los controles establecidos:

- Naturaleza del control: se debe definir cómo se va a llevar a cabo el control, si este control se hace manual, automático o ambos.
- Documentación: es necesario que todo el control se documente y se lleva un seguimiento de las actualizaciones y nuevos eventos.
- Evidencias: Revisión de la documentación, periodicidad, divulgación y demás actividades registradas que requieran para llevar a cabo la retroalimentación, las acciones de mejora y el control.
- Tipo de control: el IDPAC debe tener como prioridad el control investigativo, luego el preventivo y por último el correctivo y dejar documentación de los mismos en caso de que se presenten o puedan ser detectados a tiempo y cuál fue el proceso de mitigación.

6.3.4 Tratamiento

Tomando como base el resultado del análisis de riesgo y con el fin de tratar el riesgo residual se debe establecer los niveles de riesgo y se adelantan acciones de mejora que propenden por conservar las características de confidencialidad, integridad y disponibilidad de la información.

NIVELES DE RIESGO			
TIPO DE RIESGO	**VALOR ASIGNADO**	**GESTIÓN**	**ACTIVIDADES O TAREAS**

NIVELES DE RIESGO			
TIPO DE RIESGO	**VALOR ASIGNADO**	**GESTIÓN**	**ACTIVIDADES O TAREAS**
Riesgo Catastrófico	Si su ocurrencia es mayor a doce (12) veces en un año o se presenta varias veces en un (1) mes	MITIGAR	Requiere acciones inmediatas para evitar la pérdida de la confidencialidad, integridad y disponibilidad de la información Documentar.
Riesgo Alto	Si su ocurrencia es mayor a ocho (8) veces en un año, pero menor a diez (10) o se presenta al menos una vez en dos meses consecutivos.	MITIGAR	Se requiere de acciones rápidas que contempla la toma de decisiones conjuntas entre la alta dirección y tecnología del IDPAC. Documentar.
Riesgo Moderado	Si su ocurrencia es mayor a cinco (5) veces en un año, pero menor a ocho (8) o se presenta al menos una vez en dos meses no consecutivos para ese periodo.	MITIGAR	Se requiere revisar y ejecutar los controles establecidos para el riesgo y revisar eficacia de estos. Documentar.
Riesgo Bajo	Si su ocurrencia es mayor a dos (2) veces en un año, pero menor a cinco (5) o se presenta al menos una vez en un mes para ese periodo.	ACEPTAR	El riesgo se mitiga con actividades propias, controles establecidos y por medio de acciones de investigación y preventivas.
Riesgo insignificante	Si ocurre una (1) vez en el año	ACEPTAR	El riesgo no representa impacto significativo para el IDPAC.

Las opciones de tratamiento de riesgos según ISO 31000:2018 no son excluyentes entre sí y tampoco resultan eficaces en todas las circunstancias, éstas pueden incluir una o varias de las siguientes acciones:

- Eliminar el riesgo prescindiendo del proceso, la actividad o las circunstancias que lo generan.
- Asumir el riesgo, aun aumentándolo, con el fin de incrementar una posible oportunidad.
- Tomar acciones para disminuir la probabilidad del riesgo.
- Implementar acciones que disminuyan el impacto negativo del riesgo.
- Compartir el riesgo (cláusulas en contratos o comprar pólizas de seguros)
- Retener el riesgo con base en información confiable.