GOBIERNO ABIERTO DE BOGOTÁ

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

INSTITUTO DISTRITAL DE PROTECCIÓN Y BIENESTAR ANIMAL

ALCALDÍA MAYOR DE BOGOTÁ D.C. | BOGOTÁ

CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO	FECHA	VERSIÓN	DESCRIPCIÓN
Acta No. 1	30 de enero de 2025	1.0	Adopción

GOBIERNO ABIERTO DE BOGOTÁ

TABLA DE CONTENIDO

GOBIERNO ABIERTO DE BOGOTÁ

TABLA DE ILUSTRACIONES

GOBIERNO ABIERTO DE BOGOTÁ

TABLA DE TABLAS

1. INTRODUCCIÓN.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, comprendiendo el concepto de riesgo, así como el contexto de su tratamiento. De esta forma se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos estratégicos del IDPYBA en el entono TIC.

Gestionar de manera eficaz la seguridad de la información y riesgos de seguridad digital de los sistemas de información del IDPYBA, así como en los activos de información que participan en sus procesos y que se encuentran expuestos, los cuales permiten garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del modelo de Seguridad y privacidad de la Información y en concordancia a la normativa aplicable.

De igual forma este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos identificados dentro de la valoración de riesgos de todas las áreas del Instituto, realizado durante el cuarto trimestre de 2024, hallazgos de auditorías internas y el cumplimiento del procedimiento de planeación estratégica PE01-PR05 de la entidad.

Por otro lado, este plan se ajusta a lo que establece la política PE01-PL01 – “Política para la Administración de Riesgos” del IDPYBA y se integra con los riesgos de seguridad digital y de la información que se determinen en la evolución de los diferentes procesos tecnológicos que se vayan generando en la entidad.

2. OBJETIVO.

Consolidar los riesgos de seguridad y privacidad de la información de la entidad y realizar seguimiento de los mismos, para medir la efectividad en la aplicación de los controles establecidos, para realizar la evaluación y posteriores acciones de mejora pertinente a que haya lugar, para salvaguardar los activos de información, que contribuyan a prevenir y/o mitigar la posible materialización de los riesgos de seguridad de la información.

2.1. OBJETIVOS ESPECÍFICOS.

- Consolidar los
- Consolidar los riesgos de seguridad y privacidad de la información, para identificar el riesgo inherente y controles establecidos
- Definir el tratamiento de los riesgos de seguridad y privacidad de la información que sean consolidados, para implementar los controles necesarios para proteger los activos de información que apoyen en la mitigación y/o prevención del riesgo.
- Realizar el seguimiento del tratamiento de los riesgos de seguridad y privacidad de la información de la entidad.
- Evaluar la efectividad de los controles establecidos para el tratamiento de los riesgos de seguridad y privacidad de la información de la entidad.
- Realizar las acciones de mejora a que haya lugar a partir de la evaluación de los riesgos de seguridad y privacidad de la información de la entidad.

3. NORMATIVIDAD Y LINEAMIENTOS CONCEPTUALES Y METODOLÓGICOS.

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI, en lo relacionado con la identificación y gestión de los riesgos de seguridad de la información en la entidad:

Marco Normativo	Descripción
Constitución Política de Colombia. Artículo 15	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar
Ley 1952 de 2019	Por medio de la cual se expide el código general Disciplinario
Ley 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
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
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1221 de 2008	Se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones

Decreto 680 de 2001	
	Modifica la Comisión Distrital de Sistemas y es establece el carácter de obligatoriedad en la adopción de las políticas que la CDS determine.
Decreto 053 de 15 de febrero de 2002	Por el cual se crea el Comité para la implementación del Número Único de Emergencias y Seguridad del Distrito Capital, del cual forma parte el secretario técnico de la CDS.
Decreto 397 de 17 de septiembre de 2002	Delegar en el secretario general de la Alcaldía Mayor de Bogotá las atribuciones conferidas al alcalde Mayor en el Acuerdo 57 de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución
Decreto 767 de 2022	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'
Decreto 619 del 28 de diciembre de 2007	Que el Decreto Distrital 619 de 2007 establece la estrategia de Gobierno Electrónico en el Distrito y define la necesidad de reglamentar gradualmente por parte de la Secretaría General de la Alcaldía Mayor de Bogotá la utilización de medios Electrónicos en diversos trámites, procedimientos y actuaciones de las entidades distritales.
Decreto 2106 de 2019	, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones
Decreto 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.

Decreto 460 del 1995	Registro Nacional del Derecho de Autor
Decreto 1421 de 1993	Por medio del cual se dicta el régimen especial para el Distrito Capital de Santa Fe de Bogotá, ciudad con autonomía para la
	gestión de sus intereses, dentro de los límites de la Constitución y la ley.
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.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Se establecen las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

Decreto 1081 de 2015	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
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 1074 de 2015.	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
Decreto 103 de 2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.
Decreto 1083 de 2015	Decreto Único Reglamentario de Función Pública 1083 de 2015
Decreto 1078 de 2015	Manual para la Implementación de la Política de Gobierno Digital Decreto 1078 de 2015 libro 2, parte 2, título 9. Cap. 1.
Decreto 1080 de 2015	Se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Decreto 415 de 2016	Se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".
Directiva 005 -junio de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.

Directiva 22 de 2011	Política de estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos/as: que capturan las entidades del Distrito capital.
Directiva 005 del 12 de junio de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.
Resolución 305 de 2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
CONPES 3995 de 2011	Política Nacional de confianza y seguridad digital.

4. AUTODIAGNÓSTICO.

Para la vigencia 2024 se realizaron mesas de trabajo con las áreas para diligenciamiento del formato PE01-PR03-F01. Actualmente se están validando observaciones y cambios realizados por las áreas, después de aprobada la matriz de inventario de activos de información para la vigencia 2024; para la vigencia 2025 se debe dar continuidad para que sean aprobados por comité de gestión y desempeño.

Teniendo en cuenta lo anterior se hace necesario, efectuar actividades para realizar la mejora continua del plan de tratamientos de riesgos de seguridad y privacidad de la información del IDPYBA.

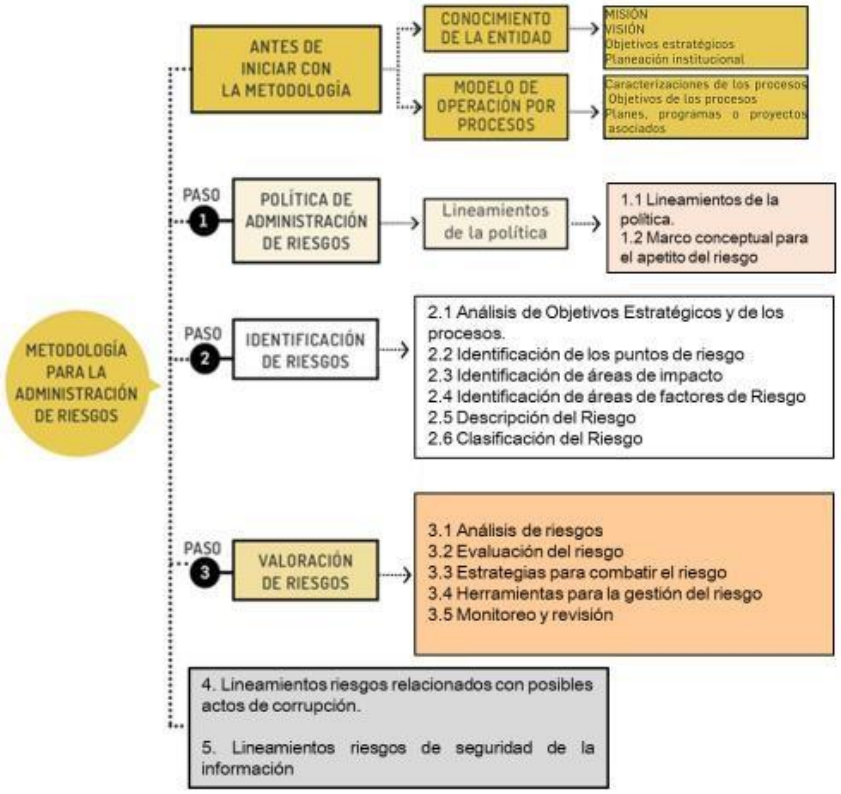
1. realizar la aprobación de los riesgos para Seguridad Digital identificados con las áreas, para monitorear y efectuar las acciones que correspondan en pro de prevenir materialización de incidentes de seguridad de la información
2. Continuar con el monitoreo y evaluación acciones de mejora de los controles de seguridad de la información, establecidos con las actividades documentadas en los riesgos de seguridad para evaluar y validar la efectividad de estos.

3. Realizar las acciones de mejora de los controles de seguridad de la información, para corregir desviaciones que se puedan presentar y evitar la posibilidad de materialización de los riesgos.

5. DESARROLLO DEL PLAN.

Los componentes metodológicos de la Administración del riesgo, se encuentran contenidos en el documento de política para la administración del riesgo (PE01-PL01)

Ilustración 1
Metodología para la administración de riesgos adoptada IDPYBA



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6 *"Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020"*

Como componente adicional el IDPYBA, establece que la gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y su tratamiento de manera progresiva.

Teniendo en cuenta los anterior se hace necesario, efectuar actividades para aumentar el nivel de implementación del Modelo de Seguridad y Privacidad de la Información dentro del IDPYBA, para ello se hace necesario incrementar el componente de planificación e implementación.

Para fortalecer la fase de planificación se requiere realizar las siguientes actividades:

1. Consolidar y aprobar los riesgos de seguridad y privacidad de la información tratados y gestionados.
2. Realizar seguimiento de los controles y acciones establecidas para los Riesgos de Seguridad de la Información.
3. Realizar evaluación de la efectividad de los controles de los Riesgos de Seguridad de la Información.

Estas actividades están asociadas con el componente de planificación y comprende que el plan de tratamiento de riesgos y la declaración de aplicabilidad cuenten con:

a. Se seleccionaron opciones apropiadas para tratar los riesgos, teniendo en cuenta los resultados de la evaluación de riesgos.
b. Se determinaron todos los controles necesarios para implementar las opciones escogidas para el tratamiento de riesgos.
c. Compare los controles determinados en el plan de tratamiento con los del Anexo A y verifique que no se han omitidos controles, si estos han sido omitidos se debe reflejar en la declaración de aplicabilidad.
d. Revise la Declaración de Aplicabilidad que tenga los controles necesarios y la justificación de las exclusiones, ya sea que se implementen o no y la justificación para las exclusiones de los controles del Anexo A, y que haya sido revisado y aprobado por la alta Dirección.
e. Revise que el plan de tratamiento de riesgos haya sido revisado y aprobado por la alta Dirección.
f. Revise que exista una aceptación de los riesgos residuales por parte de los dueños de los riesgos.
g. Contribuyen a medir la efectividad de la implementación del tratamiento de los riesgos de seguridad y privacidad de la información y controles de línea base de seguridad.

5.1. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

Parte importante del éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección: aprueban las directrices para la administración del riesgo en la entidad, siendo la responsable del fortalecimiento de la política de administración, generación y actualización de la metodología para la administración del riesgo de la entidad, coordinando, liderando y designando la capacitación y asesoría en la aplicación dentro del Instituto. Dentro del Instituto el Comité de gestión y desempeño asegurara la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

- Responsables o líderes de los procesos: identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos misionales, estratégicos, y de apoyo) al menos una vez al año. Esto no implica que el proceso de administración de riesgos este solo bajo su responsabilidad sino precisamente de garantizar que en el proceso a su cargo o dentro de sus obligaciones contractuales, se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada servidor público que trabaja en dicho proceso, en el entendido de que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

- Servidores públicos y contratistas: son los responsables de ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- Asesores Control Interno: debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos

5.2. CONTEXTO GENERAL DEL PROCESO DE GESTIÓN DEL RIESGO EN EL IDPYBA

La gestión de riesgos de seguridad de la información define los criterios básicos que son necesarios para enfocar el ejercicio por parte del IDPYBA y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos misionales, operativos y administrativos del IDPYBA, en el análisis de las debilidades y amenazas asociadas, orientadas a la planeación estratégica estipulada para la entidad, en la valoración de los riesgos en términos de sus consecuencias y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

Criterios de evaluación del riesgo de seguridad de la información: La evaluación pertinente se enfocará especialmente y como parte central de la gestión de riesgos en los siguientes aspectos:

- El valor estratégico del proceso de información en el IDPYBA como elemento medular en la gestión del riesgo.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad de las operaciones asociadas a información generada por el IDPYBA
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la entidad

Criterios de Impacto: se determinan en términos del grado, daño o costos para el IDPYBA, causados por un evento de seguridad de la información, en estos aspectos:

- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida de utilidad por desactualización o ingreso irregular de la información
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales

Los niveles de clasificación de los impactos establecidos por el IDPYBA se podrán tomar del documento – Política para la administración de riesgos - PE01-PL01

Criterios de aceptación: Los criterios de aceptación dependen de las políticas, metas, objetivos de la entidad y de las partes interesadas.

5.3. IDENTIFICACIÓN Y VALORACIÓN DE LOS RIESGOS

Determinando de manera preliminar la relevancia se deberán identificar, describir cuantitativa o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para el instituto teniendo en cuenta las siguientes actividades:

5.3.1. En cuanto a análisis del riesgo

Identificación de los riesgos, teniendo como base la identificación de los activos de información, que se clasifican de acuerdo con la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 diciembre 2020.

En términos específicos se clasifican en:

Primarios:

a) Procesos o subprocesos y actividades de la entidad: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la entidad; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b) Información: información vital para la ejecución de la misión de la entidad; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad y habeas data; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c) Actividades y procesos misionales: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

De soporte y/o mantenimiento:

a) Hardware: todos los elementos físicos que dan soporte a los procesos: PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.

b) Software: todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos como los sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.

c) Redes: todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información, entre ellos los conmutadores, cableado, puntos de acceso, etc.

d) Personal: consiste en todos los grupos de personas involucradas en el sistema de información, es decir los usuarios, desarrolladores, responsables, etc.

e) Lugares: todos los espacios físicos o virtuales en los cuales se pueden aplicar los medios de seguridad de la organización, es decir los edificios, salas, y sus servicios.

f) Estructura organizacional: funcionarios responsables, áreas, contratistas, proveedores, etc.

Una vez relacionados todos los activos se han de definir las amenazas que pueden causar daños en la información, los procesos y los soportes con los encargados de los procesos en las áreas.

Posteriormente se analizan las vulnerabilidades que podrán dar provecho de esas amenazas y causar daños a los activos de información del IDPYBA.

Este análisis de amenazas puede darse a través de:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Finalmente se identifican las consecuencias, que son el resultado y analizar como las amenazas y vulnerabilidades podrían afectar la integridad, disponibilidad y confidencialidad de los activos de información de la entidad.

Estimación del riesgo: con esta se pretende establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias (valorar y priorizar de los riesgos).

Se deben tener en cuenta estos aspectos:

- Probabilidad: la posibilidad de ocurrencia del riesgo representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- Impacto: hace referencia a las consecuencias que puede ocasionarle a la agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

Los criterios y establecimiento de probabilidad e impacto de los riesgos (incluidos los riesgos de seguridad digital) se podrán tomar de igual forma, del documento – Política y guía metodológica para la administración de riesgos PE01-PR03-P01.

5.3.2. En cuanto a evaluación del riesgo

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto en la entidad o en los casos a que haya lugar, a los ciudadanos.

5.4. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

Tabla 1

Paralelo costo beneficio y opción de tratamiento de riesgos de acuerdo con el nivel

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	Evitar el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto

La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

Fuente: Elaboración propia gestión tecnológica

PLANES DESARROLLADOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL IDPYBA

Para la vigencia 2024 se realizó seguimiento del plan y como acción de mejora se adoptó la Guía para la gestión de Riesgos de Seguridad de la Información con Código: PE01-G03 y actualizó el formato PE01-PR03-F01, matriz en la cual se consolidaron los riesgos por cada dependencia y se está haciendo una última revisión para validar que sean acordes los cambios y requerimientos de la entidad, para posterior aprobación en comité de gestión y desempeño.

6. CRONOGRAMA

Para hacer realizables las estrategias, estas son materializadas en actividades de acuerdo con su complejidad; el IDPYBA tiene previsto realizar las siguientes actividades para el desarrollo y cumplimiento del Plan de Seguridad y Privacidad de la Información, el cual se encuentra en la matriz adjunta al presente documento.

7. EVALUACIÓN Y SEGUIMIENTO

Tabla 2

Indicadores para seguimiento del plan de tratamiento de riesgos

N°	ACTIVIDAD	PRODUCTO O ENTREGABLE	MES DE EJECUCIÓN		RESPONSABLE
			FECHA INICIO	**FECHA FINAL**	
1	Consolidar y aprobar los riesgos de seguridad y privacidad de la información tratados y gestionados.	Documento riesgos de seguridad y privacidad de la información aprobado	Febrero	Abril	Líder del Proceso Gestión TIC/ profesional del proceso
2	Realizar seguimiento de los controles y acciones establecidas para los Riesgos de Seguridad de la Información.	Documento seguimiento del Tratamiento de riesgos de seguridad y privacidad de la información	Mayo	Noviembre	
3	Realizar evaluación de la efectividad de los controles de los Riesgos de Seguridad de la Información.	Documento de evaluación del tratamiento de los riesgos de seguridad y privacidad de la información	Diciembre	Diciembre	

Fuente: Elaboración propia gestión Tecnológica

La estrategia de control de riesgos para la vigencia 2025 contempla la atención de los riesgos identificados y consolidados con las áreas, siendo estos la línea base de seguridad y su actualización para la presente vigencia.

En la siguiente tabla se observan los riesgos inherentes de la línea base de seguridad del Instituto con los controles pretendidos.

Tabla actividades proyectadas para tratamiento y control de riesgos de seguridad de la información.

Tabla 3

Actividades proyectadas para tratamiento y control de riesgos de seguridad de la información

Riesgos básicos de seguridad de la información a contemplar	Acciones de tratamiento y control a realizar para atender cada riesgo
Riesgo de posibilidad de falta de contrato de mantenimiento y/o obsolescencia tecnológica, acorde a los niveles de soporte requeridos o fallas encontradas.	CONTROL: establecer roles y responsabilidades, para el área de Tecnología, de manera tal que se tengan asignados a los custodios o responsable técnicos de cada uno de los activos de seguridad del Instituto y de revisión de contratos de mantenimiento
	CONTROL: realizar seguimiento periódico al proveedor ETB, con respecto a las plataformas de Data Center contratadas. CONTROL: revisar con el proveedor opciones de recuperación ante fallas en el Data Center principal de la Etb.
	CONTROL: se debe hacer un inventario de equipos, donde se indique si tienen o no contrato de mantenimiento y de tener contrato de mantenimiento, indicar fecha de terminación del contrato de mantenimiento. Además, el inventario de equipos debe indicar si hay equipos que deban ser cambiados por obsolescencia tecnológica.
	CONTROL: realizar un inventario de activos digitales indicando versionamiento de frameworks, CMS, lenguajes y librerías utilizadas

	CONTROL: formalizar y documentar un proceso para seguimiento de contratos de mantenimientos vigentes y vencidos
Riesgo de exposición a vulnerabilidades técnicas posibilidad de software desactualizado por fallas de día cero, generando vulnerabilidades técnicas	CONTROL: Realizar pruebas de vulnerabilidad periódico de software. CONTROL: implementar un mecanismo de gestión alarmas de las diferentes plataformas del Instituto, y establecer un procedimiento para su revisión y monitoreo permanente. Establecer roles y responsabilidades, para el área de Tecnología y soporte a cada plataforma
	CONTROL: documentar las acciones que se van a tomar para realizar para identificar las plataformas de software desactualizadas.
	CONTROL: documentar los niveles de servicios contratados por los terceros periódicamente y evidenciar el cumplimiento de estos. CONTROL: documentar los protocolos de acceso a las plataformas de cloud contratadas por el Instituto.
Riego de posibilidad de fallas de seguridad en la actualización de software y/o aplicaciones existentes	CONTROL: realizar y documentar periódicamente el inventario de activos de la información del Instituto. Así como documentar los procesos de actualización de software a traces de un documento de control de cambios
Riesgo de posibilidad de ingreso a las B.D. de usuarios sin privilegios establecidos o asignados.	CONTROL: establecer mecanismos de seguridad fuerte de base de datos e incluso implementación de mecanismos criptográficos para la información reservada, confidencial y datos personales
	CONTROL: documentar y hacer seguimiento periódico, a las copias de respaldo de los servidores del Instituto. Revisar acuerdos de niveles de servicio con ETB

	CONTROL: documentar por cada aplicación, quienes tienen acceso a la información y con que privilegios. Además, identificar los responsables de dar o revocar dichos privilegios.
	CONTROLES: establecer procedimiento para revisión de usuarios activos o fuera de instituto, para desactivar y cortar sus privilegios de acceso
	CONTROL: hacer inventario regular de usuarios aprobados y sus niveles de privilegio para acceder a los Sistemas del Instituto, en las plataformas contratadas con terceros.
Riesgo de posibilidad de contraseñas hackeables por fuerza bruta, exposición por vulnerabilidades en el software, control de acceso débil	CONTROL: documentar y establecer un procedimiento de integración al directorio activo del Instituto, y poder así sincronizar el manejo de claves del Instituto. Realizar capacitación con usuarios, con respecto al manejo de claves de acceso
	CONTROL: implementar los controles de contraseñas fuertes en las plataformas del Instituto y establecer un procedimiento de verificación de su implementación.
	CONTROL: implementar mecanismos de claves fuertes de acceso y hacer que los terceros los implementen en las plataformas contratadas.
Riesgo de posibilidad de pérdida de información por falta de copias de respaldo ante una falla del sistema de almacenamiento	CONTROL: documentar y hacer seguimiento periódico, a las copias de respaldo de los servidores del Instituto. Revisar acuerdos de niveles de servicio con ETB
	CONTROL: documentar y establecer un procedimiento de copias y pruebas de copias de respaldo. Realizar proceso de prueba de las copias de respaldo.

	CONTROL: documentar y probar los procedimientos de copias de respaldo y pruebas de las copias de respaldo. CONTROL: revisar la capacidad de almacenamiento contratada con la ETB para copias de respaldo e información del Instituto. CONTROL: comprobación de copias de imágenes de las máquinas virtuales. CONTROL: tener mecanismos alternos de respaldo de información de ETB
Riesgo de vulnerabilidades en el proceso de desarrollo de software y software inmaduro	CONTROL: establecer con claridad los roles y actividades del operador externo, el administrador de infraestructura de la entidad y los desarrolladores. Orientar el proceso al Ciclo de DevOps: PLAN: planificar y diseñar lo que vamos a realizar. CREAR: programar el software. VERIFICAR: probar los requerimientos y que si cumpla las reglas establecidas. EMPAQUETAR: empaquetar el software para ser revisado REVISAR: realizar pruebas al código. CONFIGURAR: Organizar entornos y configuración requeridos. DISTRIBUIR: tras cumplir el ciclo, distribuir el Software. MONITOR: Revisar que en los dispositivos todo siga funcionando. REPETIR: plan de mejora continua
	CONTROL: establecer política de desarrollo de software y hacer una revisión periódica de su cumplimiento. Documentar el proceso de DevOps a seguir en el Instituto

Fuente: Elaboración propia Gestión Tecnológica

8. REFERENCIAS Y BIBLIOGRAFÍA.

Habilitador de Seguridad y Privacidad de la Información
https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221https://gobiernodigital.mintic.gov.co/692/w3-multipropertyvalues-533221-533236.html?__noredirect=1533236.html?__noredirect=1

listado maestro del Modelo de Seguridad y privacidad de la Información -MSPI https://gobiernodigital.mintic.gov.co/692/articles-237872_maestro_mspi.pdf

marco normativo y metodológico para implementación del Modelo de Seguridad y privacidad de la Información -MSPI

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/