PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
1	31/01/2022	1.0	Adopción mediante Acta Comité de Gestión y Desempeño

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	**OFICINA ASESORA DE PLANEACIÓN**	**LIDER DEL PROCESO**
Nombre: Germán González Rozo José Alfonso Pérez Contreras	**Nombre:** Loren Guisell Díaz Jimenez J Sebastián Moreno S	**Nombre:** Gotardo Antonio Yáñez Álvarez
Firma: Germán González Rozo	**Firma:** LorenDiaz	**Firma:**
Cargo: Profesionales Contratistas Tecnología	**Cargo:** Contratistas Profesionales Oficina Asesora de Planeación.	**Cargo:** Subdirector Gestión Corporativa.

TABLA DE CONTENIDO

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 que participan en sus procesos y que se encuentran expuestos, permite 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 Sistema de Gestión de Seguridad 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 2021, del Instituto, 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.

1. OBJETIVO GENERAL.

Establecer el plan de tratamiento de riesgos de seguridad y privacidad de la información e iniciar la implementación del MSPI (Modelo de Seguridad y Privacidad de la Información) del Instituto Distrital de Protección y Bienestar Animal; con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios, de tal forma que se definen y aplican los controles con los cuales se buscan mitigar la materialización de los riesgos de seguridad de la información. De esta manera lograr mediante el tratamiento de los riesgos y el mejoramiento continuo de la Seguridad y Privacidad de la Información.

2. OBJETIVOS ESPECÍFICOS.

Los objetivos específicos para el Instituto son los siguientes:

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir y proteger los activos de información mediante el control de la implementación de acciones de mitigación frente al riesgo.
- Generar una cultura y apropiación del trabajo enfocada en la identificación de los riesgos de seguridad de la información y su mitigación sobre los activos de información.
- Buscar reducir al mínimo cualquier posibilidad de que un evento produzca determinado impacto sobre los activos de información, a través de la gestión adecuada de los riesgos de la seguridad de la información.

3. GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **Activo de Información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.
- **Amenaza:** es la causa potencial de una situación de incidente y no deseada por la organización
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** resultado de un evento que afecta los objetivos.
- **Criterios del riesgo:** términos de referencia frente a los cuales la importancia de un riesgo se evaluada.
- **Control:** medida que modifica el riesgo.
- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos:** proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Evento:** un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

- **Factores de Riesgo:** situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

- **Identificación del riesgo:** proceso para encontrar, enumerar y caracterizar los elementos de riesgo. Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- **Integridad:** propiedad de la información relativa a su exactitud y completitud.

- **Impacto:** cambio adverso en el nivel de los objetivos del negocio logrados.

- **Nivel de riesgo:** magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

- **Matriz de riesgos:** instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

- **Monitoreo:** mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

- **Riesgo Inherente:** es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

- **Riesgo Residual:** el riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

- **Riesgo:** efecto de la incertidumbre sobre los objetivos.

- **Riesgo en la seguridad de la información:** potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

- **Reducción del riesgo:** acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

- **Seguimiento:** mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

- **Tratamiento del Riesgo:** proceso para modificar el riesgo

- **Valoración del Riesgo:** proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

- **Vulnerabilidad:** es aquella debilidad de un activo o grupo de activos de información.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

4. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
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
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 - diciembre de 2020	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública, diciembre 20 de 2020

Tabla 1 –base normativa para definición plan de tratamiento de riesgos de seguridad y privacidad de la información

5. ALCANCE

El Plan de Tratamiento de Riesgo del Instituto esta alineada con la guía de tratamiento de riesgos del DAFP y su correspondiente mapa de calor para los riesgos considerando Probabilidad e impacto.

.

PROBABILIDAD	IMPACTO				
	1-Leve	2-Menor	3-Moderado	4-Mayor	5-Catastrófico
1-Muy_Baja	BAJA	BAJA	MODERADA	ALTA	EXTREMA
2-Baja	BAJA	MODERADA	MODERADA	ALTA	EXTREMA
3-Media	MODERADA	MODERADA	MODERADA	ALTA	EXTREMA
4-Alta	MODERADA	MODERADA	ALTA	ALTA	EXTREMA
5-Muy_Alta	ALTA	ALTA	ALTA	ALTA	EXTREMA

Conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020

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 de la Entidad en el marco de los lineamientos del MIPG.

El presente documento aplica para los activos de información (Dimensionados en el PETI) y los riesgos asociados al tratamiento de riesgos de seguridad y privacidad de la información que se aplica a los procesos del Instituto Distrital de Protección y Bienestar Animal.

6. VISIÓN GENERAL DE LA GESTIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

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

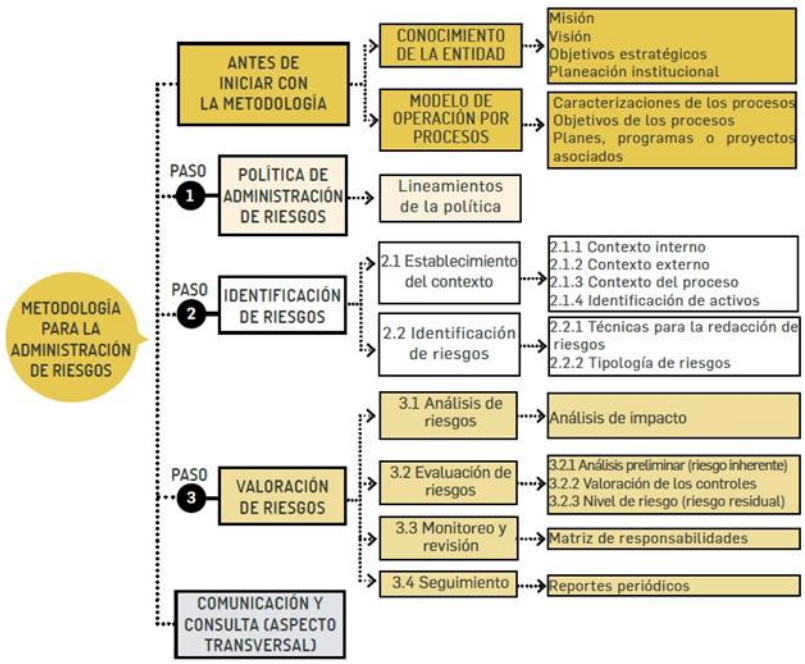

Gráfico 1 – Metodología para la administración de riesgos adoptada IDPYBA

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.

7. 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

8. 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 IDPYB 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.

9. 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:

9.1 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 V1.0

9.2 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.

10. 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.

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

Tabla 3 – Paralelo costo beneficio y opción de tratamiento de riesgos de acuerdo con el nivel

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

Desde la vigencia 2021 como primera tarea se adelantó el autodiagnóstico del componente de seguridad de la información y se definieron varias actividades dentro de las que se incluyeron la formulación del Plan de seguridad de la información y posteriormente se delimita el plan de tratamiento de riesgos.

Adicionalmente, se realizó la revisión y documentación de la Matriz de riesgos de seguridad de la información versus los controles que se deben atender desde el instituto; de tal forma que se definen nuevos riesgos de seguridad de la información y se asocian a los existentes, la relación de los controles aplicados versus los controles de la Norma ISO 27001:2013, se aplica a cada uno de ellos para evitar la materialización de estos.

11. ACTIVIDADES PARA DESARROLLAR SOBRE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Para adelantar las actividades es necesario mencionar que hay tres fases claves en el tratamiento de riesgos y fueron definidos con cada una de sus fases:

Fase de Planificación: Dentro de esta fase se describe las actividades propias del relacionamiento de las actividades de implementación del Plan de seguridad de Información y los riesgos posiblemente se presenten.

Fase de Tratamiento de los riesgos de seguridad de la información: En esta fase el Instituto una vez identificados los riesgos en la implementación del plan de seguridad de la información aplicado a los procesos del Instituto, revisando primordialmente los procesos responsables como son el proceso de Gestión tecnológica, y los procesos que tengan relacionamiento con los sistemas de información misionales del instituto.

Fase de socialización: en la cual se presenta conjuntamente a los grupos de interés del Instituto y se define una propuesta de seguridad de la información para incluir en el manejo y tratamiento de los riesgos.

Estas actividades, se han organizado de manera trimestral para ser implementadas durante la vigencia de 2022 como se muestra a continuación. Los riesgos de seguridad de la información para el 2022 debe aprobarse por comité de gestión y desempeño y publicarse antes en la página web y hacer seguimiento a los controles (definir periodicidad)

	ACTIVIDAD	DESCRIPCIÓN	ENTREGABLE	FECHA
1.	Revisión de estado de tratamiento y controles de línea base de seguridad	Esta actividad se realizará teniendo en cuenta la **línea base de seguridad** definida para el Instituto, de la valoración de riesgos de seguridad de la información de noviembre de 2021, con fin de identificar el estado actual del tratamiento de los estos, el nivel de impacto, roles y responsabilidades.	Documento de informe de estado de tratamiento y controles de línea base de seguridad	1 TRIMESTRE 2022 (marzo 31 de 2022)
2.	Identificación y evaluación de riesgos de seguridad y privacidad de la información	Esta actividad se realizará luego de la actualización de activos de información, con fin de hacer una valoración de riesgos de seguridad de la información de cada uno de los procesos de la entidad.	Documento de valoración de riesgos 2022	2 TRIMESTRE 2022 (junio 30 de 2022)

3.	Tratamiento y control de riesgos de seguridad y privacidad de la información	Verificación, aceptación, aprobación y plan de mejora de los controles a los riesgos de seguridad y privacidad de la información para mitigación de materialización de estos.	Documento de tratamiento y control de riesgos 2022	3 TRIMESTRE 2022 Septiembre 30 de 2022)
4.	Monitoreo, planes de mejoramiento	Seguimiento periódico de materialización de riesgo y de la efectividad de los controles implementados. Monitoreo del riesgo residual.	Actualización trimestral del documento de Tratamiento y controles de riesgos de seguridad de la información	4 TRIMESTRE 2022 (marzo 30, junio 30, Septiembre30 y diciembre 15 de 2022)

La estrategia de control de riesgos para la vigencia 2022, contempla la atención de los riesgos identificados del ejercicio de valoración de riesgos de seguridad de la información de noviembre de 2021, definidos estos como línea base de seguridad y su actualización para la vigencia 2022.

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

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: documentar los requerimientos de las plataformas, con respecto a las copias de respaldo
	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: establecer un mecanismo de seguimiento al contrato de ETB de las plataformas del Data Center, para que estas plataformas sean actualizadas periódicamente ante fallas de seguridad encontradas. Solicitar evidencia de actualización de plataforma de servidores con ETB
	CONTROL: documentar y hacer seguimiento periódico, donde se evidencie la actualización del software contratado y los ajustes al contrato con ETB
	CONTROL: realizar y documentar periódicamente el inventario de activos de la información del Instituto. 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.

Riego de posibilidad de fallas de seguridad en la actualización de software y/o aplicaciones existentes	CONTROL: documentar los protocolos de acceso a las plataformas de cloud contratadas por el Instituto.
	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 mecanismo para asegurar el uso restringido de la herramienta phpadmin
	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: evidencia de cambio de claves trimestralmente. Revisar con ETB que los sistemas de información del Instituto tengan implementados los controles de calidad de claves de seguridad del Instituto.
	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

Tabla 5 –Tabla actividades proyectadas para tratamiento y control de riesgos de la **línea base de seguridad**

12. ELEMENTOS ESTRUCTURALES

12.1 Metas

- Realizar el 100% del plan de trabajo propuesto para la vigencia 2022
- Tener un (1) plan de tratamiento de riesgos de seguridad y privacidad de la información

12.2 Indicadores de medición al cumplimiento del Plan

Tipo Indicador	Nombre Indicador	Objetivo	Fórmula	Periodicidad
Eficiencia	Cumplimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Cumplir con el 90% de ejecución del plan	$\frac{Total\ de\ actividades\ ejecutadas}{Total\ de\ actividades\ del\ plan}$	Trimestral
Efectividad	Impacto del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Cumplir con los porcentajes de Eficiencia y Eficacia	$\frac{Total\ de\ riesgos\ materializados}{Total\ de\ riesgos}$	Trimestral
Eficacia	Cobertura del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Alcanzar al 80% del personal del Instituto	(Personal del Instituto beneficiado a través de los planes) / (Total de personal del Instituto)	Trimestral

13. REFERENCIAS

Plan de tratamiento para los riesgos y seguridad de la información MINTIC 2020 https://www.mintic.gov.co/portal/604/articles-100251_plan_tratamiento_seguridad_2020_u20200902.pdf

Plan de tratamiento de riesgos de seguridad y privacidad de la información ANI https://www.ani.gov.co/sites/default/files/u410/plan_de_tratamiento_de_riesgos_de_seguridad_de_la_informacion_ani.pdf

Plan de tratamiento de riesgos de seguridad de la información ESAP https://www.esap.edu.co/portal/wp-content/uploads/2019/03/Plan-de-Tratamiento-deRiesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf