TABLA DE CONTENIDO

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 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 del proceso de gestión tecnológica, hallazgos de auditorias 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-PR03-PL01 – “Política y guía Metodológica 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. OBJETIVOS

Describir las actividades que detallan el plan de tratamiento de riesgos de seguridad y privacidad de la información que hace parte del Sistema de Gestión de Seguridad de la Información – SGSI del Instituto Distrital de Protección y Bienestar Animal; 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, las aportantes tengan mayor confianza en el tratamiento de la información que se gestiona y almacena en el Instituto.

Se debe mencionar que los objetivos específicos para el Instituto son:

- Brindar lineamientos y principios que busquen unificar los criterios para la administración de riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos del Instituto incorporando controles y medidas de seguridad de la información acordes con el entorno de gestión del Instituto.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas.
- Generar una cultura y apropiación del trabajo enfocada en la identificación de los riesgos de seguridad de la información y su mitigación.
- Promover una gestión adecuada de los riesgos de la seguridad de la información mediante la reducción al mínimo de cualquier posibilidad de que un evento produzca determinado impacto en la información existente.
- Mantener el nivel de probabilidad e impacto residual de los riesgos en un nivel aceptable, que define la Alta Dirección del Instituto

3. GLOSARIO DE TERMINOS 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

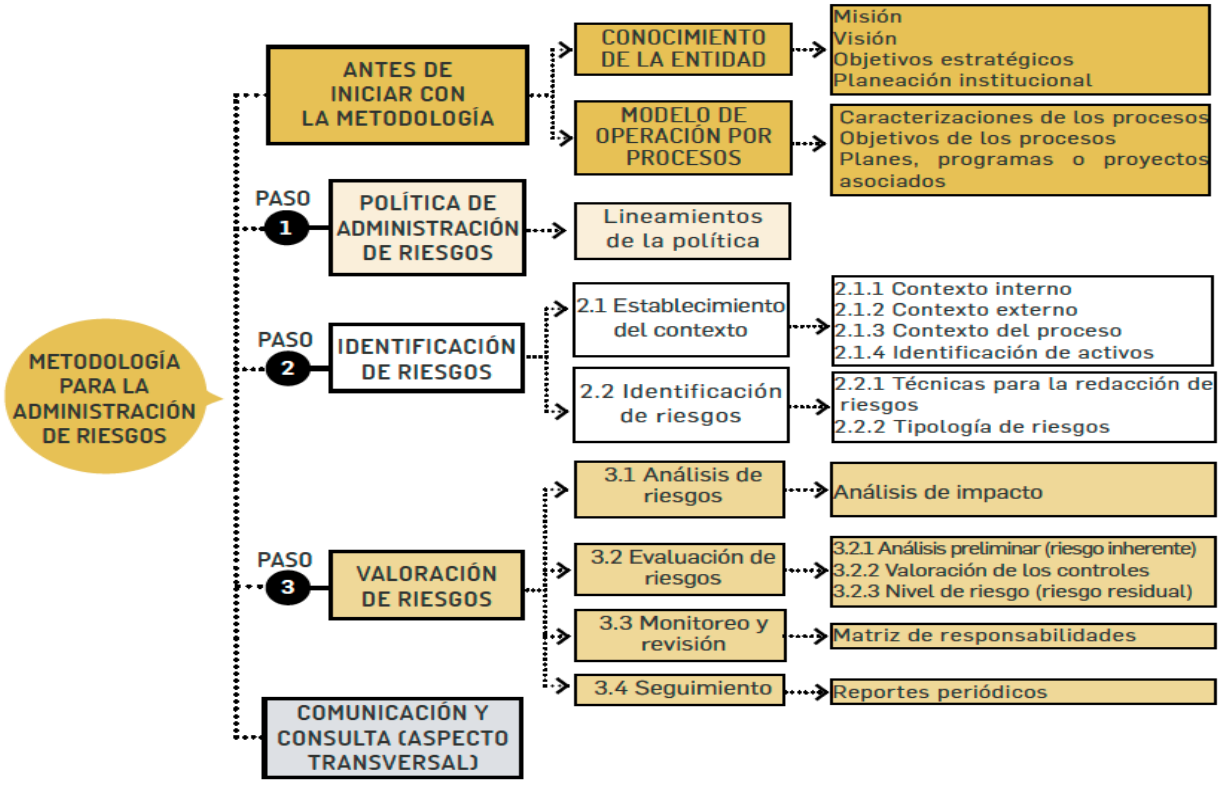
NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 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 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

5. ALCANCE

El alcance del plan de plan de tratamiento de riesgos de seguridad y privacidad de la información se aplica a los procesos del Instituto Distrital de Protección y Bienestar Animal, a cualquier sistema de información o aspecto de control del Instituto a través de los principios básicos y metodológicos para la administración del riesgo de acuerdo con el alcance del Sistema de Gestión de Seguridad de la Información.

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 y guía metodológica para la administración del riesgo (PE01-PR03-P01)** que adopta la metodología establecida por el DAFP en la guía para la administración del riesgo y el diseño de controles en entidades públicas:



Como componente adicional en el IDPYBA, como entidad que se encuentra en etapa de evolución, 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.

- **Responsables o líderes de los procesos:** Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos misionales, administrativos u operativos) 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.

- **La Oficina Asesora de 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, (matrices DOFA) 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 particularmente en los siguientes aspectos:

    - El valor estratégico del proceso de información en el IDPYBA
    - 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 y guía metodológica para la administración de riesgos - PE01-PR03-P01 V1.0**

- **Criterios de aceptación:** Los criterios de aceptación dependen de las políticas, metas, objetivos de la entidad y de las partes interesadas. En particular para la gestión tecnológica se encuentran los siguientes asociados al factor de corrupción (identificación base):

Area/proceso	Causas	Descripción	Consecuencias
GESTIÓN TECNOLÓGICA	Delegación de ingreso a sistemas de información a funcionarios no autorizados. Ataques cibernéticos. Divulgación inapropiada de las claves de acceso. Definición inadecuada de perfiles de usuario por parte de los líderes de los módulos de aplicaciones.	Manipulación y adulteración de la información contenida en los sistemas de información para beneficio propio o de un tercero.	Pérdida de la integridad de la información. Investigaciones y/o sanciones administrativas, penales y fiscales. Pérdida de credibilidad y confianza. Divulgación indebida de información. Pérdida de recursos financieros.

El detalle de esta identificación se encuentra acorde al Plan de direccionamiento Estratégico **PE01-PN01 - Plan Anticorrupción y Atención al Ciudadano.**

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 el documento “Recolección de activos de Información” del IDPYBA, disponible en el Portal Institucional.

En términos específicos se clasifican en:

i. 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.

ii. **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 e 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:

i. **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.

ii. **Impacto**: Hace referencia a las consecuencias que puede ocasionar 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 (incluídos 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	OPCION 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 acepta**r el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

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

Desde la vigencia 2018 como primera tarea se adelantó el autodiagnóstico del componente de seguridad de la información y se definieron varias actividades dentro de las que se incluye 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.

De esta forma, para 2020, se llevó a cabo la actualización de identificación de los riesgos de seguridad y privacidad de la información, como se muestra (extracto del mapa de riesgos) - Formato PE01-PR03-F01:

PROCESO / AREA	CAUSAS	DESCRIPCIÓN DEL RIESGO	TIPO	CONSECUENCIAS	EVALUACIÓN DEL RIESGO		ZONA DE RIESGO INHERENTE
					Probabilidad	Impacto	
GESTIÓN TECNOLÓGICA	Coordinación y Comunicación Desconocimiento de la Política de Seguridad de la Información por parte de los funcionarios de la Entidad.	Suministro, divulgación, alteración o fugas de información de la entidad, para uso indebido en beneficio propio o de un tercero.	TECNOLÓGICOS	Manipulación o pérdida de información vital del Instituto.	Rara vez	Mayor	MODERADO
	1. Hardware y/o Software desactualizados	Vulnerabilidad en los recursos de infraestructura tecnológica.	TECNOLÓGICOS	1. Manipulación o pérdida de información vital del Instituto.	Improbable	Moderado	MODERADO
	2.Carencia de un plan de mantenimiento preventivo para equipos y programas del sistema operativo.			2. Sanciones disciplinarias.			

PROCESO / AREA	CAUSAS	DESCRIPCIÓN DEL RIESGO	TIPO	CONSECUENCIAS	EVALUACIÓN DEL RIESGO		ZONA DE RIESGO INHERENTE
					Probabilidad	Impacto	
	3.Carencia de dispositivos de seguridad para evitar y controlar los daños o ataques a los sistemas informáticos ocasionados por programas elaborados intencionalmente por terceros.			3. Parálisis en el normal funcionamiento de las dependencias. 4. Limitaciones en la ejecución de alternativas de continuidad del negocio.			
	Deficiencias en la elaboración del Plan estratégico de tecnologias de la información.	Adquisición incorrecta de recursos informáticos (equipos, programas, aplicaciones, etc) por cambios tecnológicos y actualizaciones.	TECNOLÓGICOS	1. Pérdidas económicas. 2. Retraso en desarrollo de procesos. 3. Inconfomidad de los usuarios. 4.Imagen reputacional de la entidad desgastada.	Posible	Mayor	ALTO
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Operación no autorizada	Afectación de la disponibilidad de la base de datos.	TECNOLÓGICOS	Perdidad de acceso a la información	Rara vez	Mayor	MODERADO
	Administración indebida de datos			Daño (corrupción) de datos			
	Fraude o practicas de hacking			Perdida de acceso a los ciudadanos			
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Desactualización de las herramientas informáticas de desarrollo	Afectación de la operación de los sistemas tecnologicos como los de información	TECNOLÓGICOS	Resultados de informacion no confiables	Rara vez	Mayor	MODERADO
	Incorrecta aplicación del testing de software			Posibles investigaciones y sanciones.			
	Fallas tecnicas en el código del software			Resultados de informacion no confiables			

12. 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.

En la siguiente tabla se observan los riesgos inherentes con los controles pretendidos y la identificación del tipo de tratamiento.

PROCESO	CAUSAS	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS	CONTROLES	TRATAMIENTO
GESTIÓN TECNOLÓGICA	Coordinación y Comunicación Desconocimiento de la Política de Seguridad de la Información por parte de los funcionarios de la Entidad.	Suministro, divulgación, alteración o fugas de información de la entidad, para uso indebido en beneficio propio o de un tercero.	Manipulación o pérdida de información vital del Instituto.	Contar con las políticas de seguridad para el uso del correo electrónico, la intranet, redes sociales, equipos, infraestructura tecnológica, la selección del recurso humano y seguridad física y del entorno, establecidas en el Manual de Políticas de la Información.	Evitar
	1. Hardware y/o Software desactualizados	Vulnerabilidad en los recursos de infraestructura tecnológica.	1. Manipulación o pérdida de información vital del Instituto.	Actualizaciones de las herramientas con las que cuenta el Instituto.	Evitar
	2.Carencia de un plan de mantenimiento preventivo para equipos y programas del sistema operativo.		2. Sanciones disciplinarias.		
	3.Carencia de dispositivos de seguridad para evitar y		3. Parálisis en el normal funcionamiento de las dependencias.		

PROCESO	CAUSAS	DESCRIPCIÓN DEL RIESGO	CONSECUENCIAS	CONTROLES	TRATAMIENTO
	controlar los daños o ataques a los sistemas informáticos ocasionados por programas elaborados intencionalmente por terceros.		4. Limitaciones en la ejecución de alternativas de continuidad del negocio.		
	Deficiencias en la elaboración del Plan estratégico de tecnologias de la información.	Adquisición incorrecta de recursos informáticos (equipos, programas, aplicaciones, etc) por cambios tecnológicos y actualizaciones.	1. Pérdidas económicas. 2. Retraso en desarrollo de procesos. 3. Inconfomidad de los usuarios. 4.Imagen reputacional de la entidad desgastada.	Plan estratégico de Tecnología de la información y las comunicaciones - PETIC	Reducir
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Operación no autorizada	Afectación de la disponibilidad de la base de datos.	Perdidad de acceso a la información	Control de acceso a datos por usuarios y privilegios	Evitar
	administración indebida de datos		Daño (corrupción) de datos	Realizar el seguimiento a las buenas practicas de administracion de base de datos.	
	Fraude o practicas de hacking		Perdida de acceso a los ciudadanos	Aplicación de las políticas de seguridad en el ambiente de BD y Produccion, establecidas en el Manual de Políticas de la Información.	
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Desactualización de las herramientas informáticas de desarrollo	Afectación de la operación de los sistemas tecnologicos como los de información	Resultados de informacion no confiables	Realizar las actualizacion en el momentos que los fabricantes las disponen	Evitar
	Incorrecta aplicación del testing de software		Posibles investigaciones y sanciones.	Seguimiento al testing de software como plantea la metodologia de desarrollo	
	Fallas tecnicas en el código del software		Resultados de informacion no confiables	Realizar el seguimiento al desarrollo de software como plantea la metodologia de desarrollo	

13. MONITOREO A CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Se programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información 2020.

En la siguiente tabla se presenta el cronograma base del monitoreo para 2020-2024, se agregó la columna iterativo para esclarecer que las fechas fin implican iteración en las acciones a tomar y que las fechas finales proyectadas corresponderán a iteraciones en los periodos establecidos de actualización para este plan o en los que se requieran de acuerdo a la necesidad para cada uno.

AREA/PROCESO	DESCRIPCIÓN DEL RIESGO	ACCIONES A TOMAR	TIPO DE CONTROL	FECHA DE INICIO	FECHA FIN PROY.	META	INDICADOR EFECTIVIDAD	ITERATIVO
GESTIÓN TECNOLÓGICA	Suministro, divulgación, alteración o fugas de información de la entidad, para uso indebido en beneficio propio o de un tercero.	Documentar procedimiento control de acceso a sistemas de información, fortaleciendo el control conforme a la metodología.	Preventivo	1/03/20	31/12/20	Un procedimiento control de acceso a sistemas de información	El documento aprobado de control de acceso	NO
	Vulnerabilidad en los recursos de infraestructura tecnológica.	Continuar con las actualizaciones de hardware y software periódicamente.	Preventivo	1/03/20	31/12/20	10 reportes del sistema actualizado	Numero de máquinas actualizadas	SI
		Generar una herramienta de verificación de la capacitación a los usuarios en seguridad informática.	Preventivo	1/03/20	30/06/21	Una herramienta aprobada e implementada de verificación de la capacitación a los usuarios en seguridad informática.	herramienta aprobada e implementada de verificación de la capacitación a los usuarios en seguridad Cantidad de usuarios capacitados sobre la herramienta	NO
		Socializar el acuerdo de confidencialidad y resolución de tratamiento de datos personales.	Preventivo	1/03/20	31/12/20	3 socializaciones	Número de socializaciones del acuerdo de confidencialidad y resolución de tratamiento de datos personales/ socializaciones programadas	SI

AREA/PROCESO	DESCRIPCIÓN DEL RIESGO	ACCIONES A TOMAR	TIPO DE CONTROL	FECHA DE INICIO	FECHA FIN PROY.	META	INDICADOR EFECTIVIDAD	ITERATIVO
		Documentar procedimiento de mesa de servicios tecnológicos para los permisos de los servidores públicos.	Preventivo	1/03/20	30/06/21	Un procedimiento control de mesa de servicios	Procedimiento Aprobado	SI
	Adquisición incorrecta de recursos informáticos (equipos, programas, aplicaciones, etc) por cambios tecnológicos y actualizaciones.	Actualizar el plan estratégico de Tecnología de la información y las comunicaciones - PETIC con respecto al análisis de adquisición de recursos informáticos y sistemas de información.	Preventivo	1/03/20	31/12/20	Un plan estratégico de Tecnología de la información y las comunicaciones - PETI	Plan aprobado	SI
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Afectación de la disponibilidad de la base de datos.	Documentar procedimiento de control de acceso a sistemas de información, fortaleciendo el control conforme a la metodología.	Preventivo	1/03/20	31/06/21	Un procedimiento de control de acceso a sistemas de información	Procedimiento Aprobado	SI
		Generar una guía técnica de buenas practicas en el uso y administración de base de datos para el área		1/03/20	31/12/20	Una guía técnica de buenas practicas en el uso y administración de base de datos para el área	Procedimiento Aprobado	NO
		Documentar guia de la aplicación de las politicas de seguridad para los ambientes de BD y Produccion.		1/03/20	31/12/20	Una guia de la aplicación de las politicas de seguridad para los ambientes de BD y Produccion.	Guía aprobada	NO
GESTIÓN DE CONOCIMIENTO ASOCIADA A LA PYBA	Afectación de la operación de los sistemas tecnologicos como los de información	Documentar guia para la actualizacion de herramientas de desarrollo, estableciendo el control	Preventivo	1/03/20	31/12/20	Una guia para la actualizacion de herramientas de desarrollo	Guía aprobada	NO

AREA/PROCESO	DESCRIPCIÓN DEL RIESGO	ACCIONES A TOMAR	TIPO DE CONTROL	FECHA DE INICIO	FECHA FIN PROY.	META	INDICADOR EFECTIVIDAD	ITERATIVO
		Documentar guia de testing de software de acuerdo a la metodologia de desarrollo implantada, estableciendo el control		1/03/20	31/12/20	Una guia de testing de software de acuerdo a la metodologia de desarrollo implantada	Guía aprobada	NO
		Documentar guia de desarrollo de software de acuerdo a la metodologia de desarrollo implantada, estableciendo el control.		1/03/20	31/12/20	Una guía de desarrollo de software de acuerdo a la metodología de desarrollo implantada, estableciendo el control.	Guía aprobada	NO

14. 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-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informaci%C3%B3n-v_1.0.pdf