INSTITUTO MUNICIPAL PARA LA RECREACION Y EL DEPORTE
ALCALDÍA DE PASTO
PASTO DEPORTE
NIT 814000385-3

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

Fecha publicación: noviembre de 2021

Original firmado por:

CLAUDIA MARCELA CANO RODRIGUEZ
Directora

PLAN DE DESARROLLO: PASTO LA GRAN CAPITAL 2020-2023

Código: PT-A6. S2-01 **Versión:01** **Vigencia: 2021-12-31**

Coliseo Sergio Antonio Ruano – Av. Boyacá. Tel 7214442 Fax. 7214438.
E-mail: contactenos@pastodeporte.gov.co Portal Web: www.pastodeporte.gov.co
Pasto, Nariño, Colombia

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, de manera que, al comprender el concepto de riesgo, así como el contexto, 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 trazados en el Entorno TIC para el Desarrollo Digital.

Pasto Deporte requiere poner en marcha este plan para salvaguardar la información que se maneja en el desarrollo de sus actividades, también se busca consolidar una estructura de seguridad informática que permita optimizar el uso eficiente de datos e información y que además permita responder de manera acertada a un riesgo que tenga lugar en la ejecución de las acciones.

1. OBJETIVO

Definir la planificación de las actividades orientadas a gestionar y fortalecer el tratamiento de los riesgos asociados a la seguridad y privacidad de la información, que es generada, tratada y custodiada por PASTO DEPORTE; con el fin preservar la confidencialidad, integridad y disponibilidad, de la información en la entidad.

2. OBJETIVOS ESPEFICICOS

- Definir y divulgar las políticas, lineamientos, procedimientos, buenas prácticas y recomendaciones para establecer una cultura organizacional de Seguridad y Privacidad de la Información en PASTO DEPORTE.

- Realizar el seguimiento a las acciones pertinentes a reducir las brechas de cumplimiento de acuerdo con el autodiagnóstico del MIPG relacionado al habilitador transversal de seguridad y privacidad de información.

- Definir, gestionar y monitorear los riesgos de Seguridad y Privacidad de la Información.

- Apoyar la evaluación y documentación de la efectividad de los controles de Seguridad y privacidad de la Información identificados en la Declaración de Aplicabilidad que soportan el modelo de Seguridad de la Información establecidos.

3. ALCANCE

Los requisitos, lineamientos y acciones establecidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información son aplicables de forma anualizada a los procesos estratégicos, misionales, de apoyo y de evaluación, por lo cual deberán ser conocidos y cumplidos por todos los funcionarios, contratistas, y terceras partes vinculadas a la Entidad que accedan a los activos de información, sistemas de información e instalaciones físicas del Instituto.

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremos acorde con los lineamientos definidos por PASTO DEPORTE, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

4. DEFINICIONES

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta, el cual tiene valor para PASTO DEPORTE por lo tanto para ello se tienen contemplados los siguientes activos de información: personas, información/dato, hardware, software, redes, infraestructura y servicios.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Seguridad de la información: Conjunto de medidas que toman las personas y las organizaciones, que les permiten resguardar y proteger los activos de información, preservando su Confidencialidad, Integridad y Disponibilidad.

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Sistema de Gestión de Seguridad y Privacidad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

5. MARCO LEGAL

Dentro del marco legal más relevante para justificar el presente plan de seguridad y privacidad de la información se encuentran las siguientes normas:

- **Ley 1437 de 2011, Capítulo IV**, “utilización de medios electrónicos en el procedimiento administrativo”. “Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos.”

- **Ley 1581 de 2012**, **g) Principio de seguridad: “**La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”. Artículo 17, ítem d: “Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”.

- **Ley 1712 de 2014**, “principio de transparencia”: “Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley”.

- **Artículo 7:** “Disponibilidad de la información” “En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.”

- **Título III** “Excepciones acceso a la información” “Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.”

- **Conpes 3854 de 2016**, objetivo general “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.

- **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". ARTÍCULO 2.2.9.1.1.3. Principios. “Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano”.

- **Decreto 612 de 2018**, artículo 1. “Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”

6. TIPOS DE RIESGOS

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgo de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

7. POLÍTICA DE ADMINISTRACIÓN DE RIESGO

PASTO DEPORTE se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos, regulando los riesgos de los procesos, luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de estos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores de PASTO DEPORTE. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- **Evitar:** es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.

- **Prevenir:** corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

- **Reducir o mitigar:** corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia, planes de continencia y equipos de protección personal y ambiental.

- **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad.

- **Compartir:** es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados.

8. TIPOS DE CONTROLES

Preventivo: Cuando el punto de control se ubica al inicio del proceso, y las adecuaciones se enfocan a evitar los errores, antes de que afecten al proceso. Corresponden a esfuerzos de prevención y difusión. Anticipan eventos no deseados antes de que sucedan.

Defectivo: Cuando el punto de control se ubica dentro del proceso, y las adecuaciones se enfocan a detectar y compensar los errores o desviaciones, antes de que se elabore el resultado, corresponde a esfuerzos de contención. Identifican los eventos en el momento en que se presentan.

Correctivo: Cuando el punto de control se ubica al final del flujo de proceso, las adecuaciones se enfocan a corregir los errores sobre el resultado obtenido. Corresponden a esfuerzos de restauración, recuperación, rescate o reversión. Aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado.

9. PLANIFICACIÓN DE ACTIVIDADES

PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN			
Categoría MIPG	**Actividad**	**Resultados Esperados**	**Tiempo**
Implementación MIPG 2021	Definición y seguimiento del plan de tratamiento de riesgo de seguridad y privacidad de la información.	Definición del plan de tratamiento de riesgo seguridad y privacidad de la información.	1/11/2022 a 31/12/2022
Definición del marco de seguridad y privacidad de la información y de los sistemas de información	Actualización del perfil de riesgo de seguridad digital y protección de datos personales	Actualización del perfil de riesgos de seguridad y privacidad de la información	1/12/2021a 31/03/2022
		Definición de riesgos de protección de datos personales	1/12/2021 a 31/05/2022
		Definición del plan de tratamiento de riesgos de seguridad, privacidad de la información y protección de datos personales en la entidad	1/12/2021 a 31/05/2021
Plan de seguridad y privacidad de la información y de los sistemas de información	Implementación del plan de tratamiento de riesgos de seguridad digital.	Apoyar la gestión de solicitud de contratación de mantenimiento de equipos UPS y ejecución de este	1/12/2021 a 31/12/2022
		Planeación e Implementación de los controles de seguridad físicos de la data center principal y centro de cableado	1/12/2021 a 31/10/2022
		Revisión y actualización procedimiento de Gestión de sistemas de información	1/12/2021 a 30/11/2022
		Actualización e implementación del programa de Cultura de seguridad y privacidad de la información	1/01/2022 a 31/12/2022
		Revisar y actualizar la política de buen uso de los activos de información	1/01/2022 a 31/01/2023
		Revisión cumplimiento del MSPI (Modelo de Seguridad y privacidad de la Información).	31/01/2022 a 31/12/2022
		Realización, verificación y restauración de las Copias de Seguridad de los servidores TIC (Aplicaciones, Almacenamiento) de acuerdo con lo establecido en el Instructivo de copias de seguridad.	31/01/2022 a 31/12/2022

		Seguimiento con la atención y solución de tiques registrados en la mesa de servicios de acuerdo con lo establecido el procedimiento de Soporte Técnico, relacionados con seguridad y privacidad de la información	1/12/2022 a 31/12/2022

De acuerdo con lo anterior el plan de riesgos de seguridad y privacidad de la información busca salvaguardar la información que se maneja en la entidad, estableciendo lineamientos que permitan identificar los posibles riesgos para con ello adelantar acciones para poder evitar, mitigar y controlar dichos riesgos. De esta manera PASTO DEPORTE busca consolidar sus procesos y tener el pleno control de la gestión documental que requiere la entidad para el desarrollo de sus actividades misionales.

10. SEGUIMIENTO Y CONTROL DE LOS PROYECTOS

El seguimiento y el control del plan se realizará a través de cada vigencia por el área encargada de la ejecución de este. Igualmente, el área de Control Interno hace el monitoreo y evaluación de los resultados obtenidos en la ejecución de dicho plan.

11. CONTROL DE RIESGOS

Nombre del Riesgo	Causas	Consecuencias	Clasificación

12. ADMINISTRACIÓN Y GESTIÓN DOCUMENTAL

Control de Documentos									
IDENTIFICACIÓN		1ra. FASE: ARCHIVO DE GESTIÓN				2da. FASE: DISPOSICIÓN INICIAL (Archivo Central)			3ra. FASE: DISPOSICIÓN FINAL
COD	NOMBRE	ORDENACION DOCUMENTAL	RESPONSABLE	LUGAR	TIEMPO DE RETENCION	METODO UTILIZADO	RESPONSABLE	TIEMPO	METODO UTILIZADO

13. DOCUMENTOS DE REFERENCIA

- Plan De Tratamiento De Riesgos de Seguridad y Privacidad de la Información. INDEPORTES QUINDIO.
- Informe de Tratamiento de Riesgo MINTIC. Versión 2. Vigencia 2019.
- Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información. Ministerio del Deporte. Versión 2. Vigencia 2020.
- Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información – secretaria de cultura recreación y deporte de Bogotá - Vigencia 2021.
- Plan Tratamiento De Riesgo De Seguridad Y Privacidad De La Información- alcaldía mayor de Bogotá -- vigencia 2021
- MIPG:2017
- NTC-GP 1000:2009.
- MECI 1000:2014.
- Normas Técnicas Colombianas sobre Documentación, Instituto Colombiano de Normas Técnicas y Certificación, 1996.
- Normas APA – Edición 6 – 2016

14. CONTROL DE REVISIONES

VERSION	FECHA AA	MM	DD	RESPONSABLE	MOTIVO CAMBIO	EXTRACTO
01	2021	12	26	Control Interno, Contratista Auxiliar MIPG	Creación del Documento	

15. ANEXOS

NOTA: *Copia Controlada: si este documento se encuentra impreso no se garantiza su vigencia. La versión vigente reposa en la dirección de PASTO DEPORTE.*		
Elaborado por: Nombre: Cargo: Fecha: Firma:	**Revisado por:** Nombre: Cargo: Fecha: Firma:	**Aprobado por:** Nombre: Cargo: Fecha: Firma: