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

SERVICIUDAD E.S.P

DOSQUEBRADAS, AÑO 2022

TABLA DE CONTENIDO

INTRODUCCIÓN

La Seguridad de la Información en las Entidades tiene como foco la protección de los activos de información en cualquiera de sus estados ante posibles amenazas o brechas que generen riesgos sobre principios fundamentales de confidencialidad, integridad y disponibilidad de la información, es por eso que, a través de la identificación, análisis e implementación de controles sobre estos, se permite gestionar y reducir los riesgos e impactos a los cuales están expuestos los procesos de la Entidad. De este modo, SERVICIUDAD E.S.P presenta el Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información, el cual incluye el plan de acción para el tratamiento de riesgos con matriz de identificación, análisis, valoración y controles en cumplimiento con la Política de Seguridad y Privacidad de la información, aprobada por la Gerencia, y como herramienta para el logro de los objetivos de mantener la información de la Entidad de forma confidencial, integra y disponible.

De acuerdo a lo anterior, la metodología de gestión de riesgos definida por la Entidad requiere un análisis relacionado con el estado actual de la estructura de riesgos y un entendimiento estratégico enmarcado desde el Modelo de Planeación y Gestión “MIPG”. No obstante, la identificación y valoración de riesgos debe estar integrada en el desarrollo de la estrategia, la formulación de los objetivos y la implementación de éstos en la toma de decisiones al interior de cada proceso de la Entidad.

1. OBJETIVO

Diseñar el Plan de Tratamiento de Riesgos de Seguridad de la información alineado con la metodología de gestión de riesgos propuesta por el DAFP, con el fin de establecer una herramienta con enfoque holístico que proporcione las pautas necesarias para identificar, implementar y fortalecer una efectiva gestión de los riesgos de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de los activos de información al interior de la Entidad.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad de la Información de SERVICIUDAD E.S.P incluye la metodología para la administración de riesgos definida por el Departamento Administrativo de la Función Pública y la gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso, sistema de información o servicio de TI de la Entidad.

3. DEFINICIONES

Riesgo: Posibilidad de ocurrencia de un evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Administración del riesgo: Conjunto de elementos de control que brindan a la Entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: Cualquier información de valor para los procesos de la Entidad.

Disponibilidad: Propiedad de la información para su acceso y uso cuando lo requiera una Entidad o usuario autorizados.

Confidencialidad: Propiedad de la información para disposición de uso de usuarios o Entidades autorizados.

Integridad: Propiedad de exactitud y completitud.

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.

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

Valoración del Riesgo: Procedimiento de identificación, análisis y evaluación de los riesgos.

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

Control: Medida que permite reducir o mitigar un riesgo.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Activo: Elementos tales como aplicaciones de la Entidad, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la Entidad para funcionar en el entorno digital.

4. MARCO LEGAL

- **Constitución Política de Colombia 1991**: Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- **Decreto 612 de 4 de abril 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 1008 de 14 de junio de 2018**: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- **Decreto 1078 de 2015 -** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **ISO 27001:** Norma de la Seguridad de la Información
- **Resolución 00500 de marzo de 2022:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- **ISO 31000: Norma sobre gestión de riesgos**
- **Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas.**

5. RESPONSABLE

El responsable del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior de la Entidad es el Comité de Seguridad de Información.

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

6.1. ESTRATEGIA

SERVICIUDAD E.S.P a través de la adopción del Modelo de Seguridad y Privacidad de la Información, busca prevenir los impactos no deseados que se puedan presentar en afectación a la seguridad de la información, por lo cual es importante identificar, analizar, establecer y controlar los riesgos, con el fin de preservar y administrar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. De esta manera, para lograr el cumplimiento del Plan de Tratamiento de Riesgos se definen las siguientes estrategias:

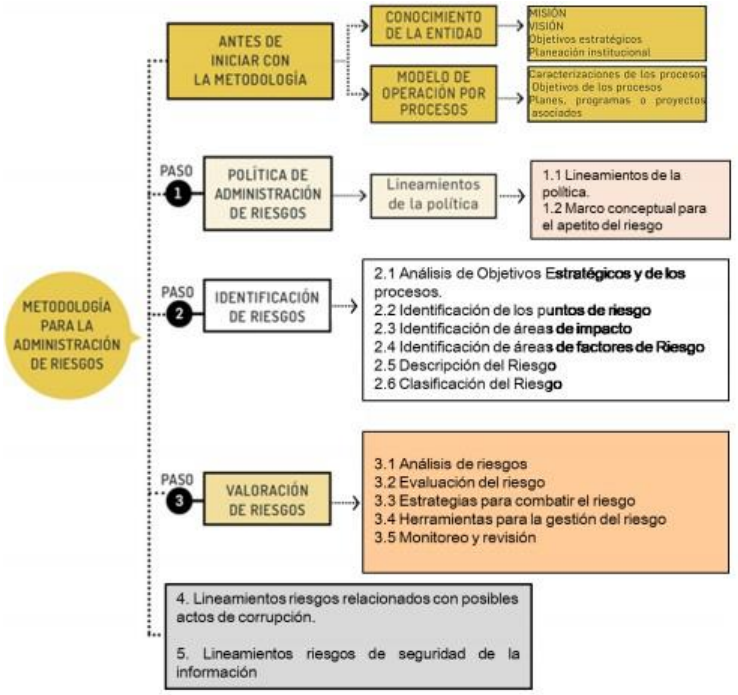
- Compromiso de la Alta Gerencia para promover, apoyar y gestionar recursos para la realización de los proyectos asociados a la gestión de los riesgos de seguridad de la información al interior de la Entidad.
- Realizar una gestión integral de los riesgos de seguridad de la información en la matriz de riesgos de la Entidad.
- Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva al interior de la Entidad.
- Promover una cultura de gestión y tratamiento de los riesgos al interior de la Entidad.

6.2. ETAPAS PARA LA GESTIÓN DEL RIESGO

Teniendo presente la guía para la administración de riesgos y el diseño de controles establecida por el Departamento Administrativo de la Función Pública DAFP, las etapas para la gestión del riesgo adoptadas por SERVICIUDAD E.S.P contemplan el compromiso y las responsabilidades de la Alta Dirección, el Comité de Seguridad de la Información, el Comité Institucional de Gestión y Desempeño y los lideres de procesos al interior de la Entidad, quiénes deben propender por una gestión integral de riesgos mediante una oportuna identificación, valoración e implementación de controles para el tratamiento de los mismos.

Por lo tanto, la guía metodológica para la administración de riesgos del DAFP es la hoja de ruta de navegación para la gestión y administración de riesgos en las Entidades públicas, alineada con el Manual Estándar de Control Interno para el Estado Colombiano y el Modelo Integrado de Planeación y Gestión, promoviendo la identificación, valoración, análisis, seguimiento y monitoreo de los riesgos de seguridad y privacidad de la información al interior de la Entidad. En ese sentido, se presenta a continuación la metodología para la administración de riesgos definida por el DAFP:

IMAGEN Nª1.METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6.2.1. CONOCIMIENTO DE LA ENTIDAD

Para la construcción de la matriz de riesgos, se tuvo presente el modelo estratégico y de procesos de la Entidad, ante lo cual se tomó como marco de referencia el Plan Estratégico de SERVICIUDAD E.S.P (PLANES ESTRATÉGICOS (serviciudad.gov.co)) y el mapa de procesos con toda la documentación del modelo de operación, la cual reposa en la intranet en el siguiente enlace (Planeación Estratégica (serviciudad.gov.co)). En ese sentido de acuerdo a la información se identificaron los procesos y objetivos y con base a ello, se definieron los riesgos para los procesos de carácter estratégico, misional, apoyo y de control y evaluación.

6.2.2. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política para la administración de riesgos de SERVICIUDAD E.S.P esta enfocada en tratar y manejar los riesgos de acuerdo a su valoración, con el fin de tomar decisiones para reducir el impacto de la materialización de riesgos al interior de los procesos, esta política se encuentra enmarcada en las estrategias para combatir los riesgos definidas en la Guía para la administración del riesgo

y el diseño de controles en Entidades Públicas, relacionadas y descritas a continuación:

- **Reducir el Riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
- **Transferir el Riesgo:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- **Mitigar el Riesgo:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente un control adicional.
- **Aceptar el Riesgo:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumirlo, conociendo los efectos de su posible materialización.
- **Evitar el Riesgo:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

6.2.3. IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo control en la Entidad, teniendo presente el contexto estratégico y el modelo de procesos sobre el que opera la misma. Del mismo modo, se deben evaluar los factores externos e internos identificando las amenazas y las vulnerabilidades del riesgo. Para efectos de los riesgos asociados con la seguridad de la información se deben identificar los activos de seguridad de la Información, teniendo presente la matriz de activos de información de la Entidad, donde se encuentran identificados y clasificados los activos de acuerdo a las directrices establecidas en la ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”

De acuerdo a lo anterior, los activos de información se clasifican en dos tipos:

Primarios:

- **Procesos o Subprocesos y actividades del Negocio:**

  - Procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la Entidad.
  - Procesos que implican tecnología para la operación.
  - Procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la Entidad.

- Procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- Procesos de propiedad intelectual que si se degradan hacen imposible la ejecución de las tareas de la Entidad.

- **Información:**
  - Información vital para la ejecución de la misión o el negocio de la Entidad.
  - Información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad.
  - Información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas.
  - Información de alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo e implican un alto costo de adquisición.

De Soporte:

- **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos.
- **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)
- **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la Entidad (Edificios, salas, y sus servicios, etc.)
- **Estructura organizativa:** Responsables, áreas, contratistas, etc.

La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios y expertos. La identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, se analizan para realizar la valoración del riesgo y aplicar los controles pertinentes.

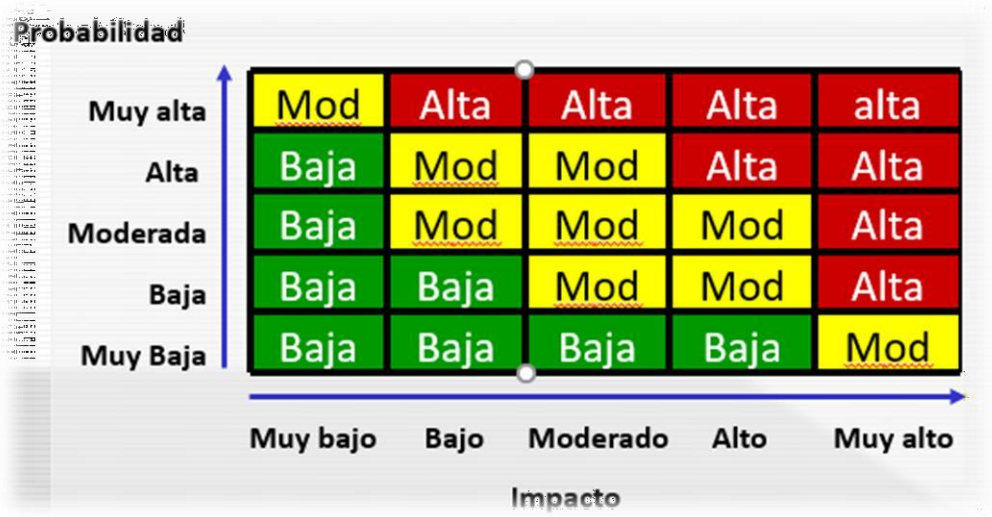
6.2.4. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En esta actividad se identifica el inventario de activos de información que intervienen en los procesos de la Entidad, que será base del enfoque de la

valoración de los riesgos de seguridad de la información. Definido el inventario, se describe cuantitativamente o cualitativamente, según el enfoque de la Oficina de Tecnologías de la Información y el activo correspondiente, para priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para SERVICIUDAD E.S.P.

Para la valoración de los riesgos se debe establecer la prioridad de ocurrencia de éste y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgos. De esta manera, los riesgos serán valorados de acuerdo a su probabilidad e impacto de la siguiente manera:

IMAGEN Nª2. MATRIZ DE PROBABILIDAD E IMPACTO



Fuente: Ver ***Matriz de Riesgos de Seguridad y Privacidad de la Información***

7. PLAN DE ACCIÓN

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron en el siguiente plan de acción para dar cumplimiento al objetivo propuesto en el plan, de acuerdo con el estado actual de la Entidad en términos de seguridad y privacidad de la información. Adicional a ello, se tuvieron en cuenta las directrices de la Guía de administración del riesgo propuesta por el DAFP.

TABLA Nº1. PLAN DE ACCIÓN

PROCESO	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODICIDAD
Gestión de Riesgos	Realizar análisis del modelo estratégico de la Entidad.	• Alinear los objetivos estratégicos con los riesgos de la Entidad	Subgerencia de Planeación	Semestral
	Realizar análisis del mapa de procesos de la Entidad	• Alinear los objetivos de los procesos con los riesgos de la Entidad	Subgerencia de Planeación	Anual
	Actualizar las directrices de atención sobre los riesgos	• Actualizar política y metodología de gestión de riesgos	Subgerencia de Planeación	Anual
	Realizar socialización y sensibilización de política y metodología de gestión y administración del riesgo.	• Socialización y sensibilización de la política de administración y metodología de gestión del riesgo.	Subgerencia de Planeación	Anual
	Identificar y clasificar los activos de información	• Identificar y clasificar los activos de información de acuerdo a las directrices	Comité Institucional de Gestión y	Semestral

PROCESO	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODICIDAD
		de la ley 1712 de 2014 "Ley de Transparencia y Acceso a la información pública"	desempeño	
	Construir la matriz de Activos de Información	• Construir la matriz de activos de información con los propietarios y periodicidad de suministro y actualización de información	Comité Institucional de Gestión y desempeño	Anual
	Realizar actualización de la matriz de activos de Información	• Seguimiento y control de la matriz de activos de información	Comité Institucional de Gestión y desempeño	Semestral
	Realizar publicación de la matriz de activo de información	• Publicación y actualización de la matriz de activos de información en el botón de transparencia en la página web, de acuerdo a las directrices de la ley 1712 de 2014 con respecto a	Oficina de TI	Por requerimiento

PROCESO	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODICIDAD
		"Instrumentos de gestión de información pública"		
	Ejecutar la metodología de identificación de riesgos.	• Identificación de los riesgos por proceso. • Evaluación del riesgo de acuerdo a probabilidad e impacto. • Valoración de los riesgos. • Definición de los controles y estrategias de mitigación del riesgo. • Construcción y aprobación de la matriz de riesgos	Subgerencia de Planeación	Anual
	Realizar socialización y sensibilización de la matriz de riesgos	• Socialización y sensibilización a líderes de procesos de la matriz de riesgos	Subgerencia de Planeación	Anual

PROCESO	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODICIDAD
	Realizar Seguimiento Fase de Tratamiento del riesgo	• Seguimiento al estado planes de tratamiento de riesgos identificados y verificación de evidencias	Subgerencia de Planeación/ Líderes funcionales de procesos	Cuatrimestral
	Realizar evaluación de riesgos residuales	• Valoración de riesgo de acuerdo a los controles implementados para su tratamiento	Subgerencia de Planeación/ Líderes funcionales de procesos	Cuatrimestral
	Realizar Publicación de matriz de riesgos	• Publicación y actualización de Matriz de riesgos	Subgerencia de Planeación	Por requerimiento
	Realizar Mejoramiento a la matriz de riesgos.	• Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Subgerencia de Planeación/ Líderes funcionales de procesos	Cuatrimestral

PROCESO	ACTIVIDADES	TAREAS	RESPONSABLE	PERIODICIDAD
	Realizar monitoreo y revisión	• Generación, presentación y reporte de indicadores de la matriz de riesgos de la Entidad	Subgerencia de Planeación/ Líderes funcionales de procesos	De acuerdo a periodicidad de indicadores

Fuente: Elaboración propia.

8. OPORTUNIDADES DE MEJORA

La Entidad no solo debe centrarse en los riesgos identificados, sino que también el análisis y los controles asignados a los riesgos deben propender a identificar oportunidades de mejora como consecuencia de mejoramiento frente al resultado del tratamiento de los riesgos.

9. RECURSOS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de SERVICIUDAD E.S.P, se encuentra apoyado en los siguientes recursos:

TABLA Nª2. MATRIZ DE RECURSOS

RECURSOS	VARIABLE
Humanos	La Dirección de la Oficina de TI es responsable de coordinar, modificar y realizar seguimiento a las políticas, estrategias, procedimientos y actividades en materia de seguridad y privacidad de la información al interior de la Entidad.
Técnicos	La Entidad para la construcción de la matriz de riesgos se apoyo en la guía para la administración del riesgo y el diseño de controles en entidades publicas propuesta por el DAFP.
Materiales	Instalaciones y locación que permitan impactar sobre los controles en riesgos identificados al interior de los procesos de la Entidad.

RECURSOS	VARIABLE
Financieros	Recursos disponibles para la implementación de controles en el tratamiento de riesgos identificados.
Tecnológicos	Plataforma de apoyo tecnológico para la identificación de brechas de seguridad de la información y aseguramiento de controles en la infraestructura tecnológica de la Entidad.

Fuente: Elaboración propia.

10. PRESUPUESTO

El análisis y priorización del presupuesto para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información identificados en la Entidad, corresponderá a las Subgerencias de Planeación y Financiera y Administrativa, mediante la asignación de recursos para la implementación de los controles definidos en la matriz de riesgos.

11. MEDICION

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de SERVICIUDAD E.S.P incluye una fase de medición para realizar seguimiento y control mediante el siguiente indicador

TABLA Nª3. INDICADO DEL PLAN DE TRATAMIENTO DE RIESGOS

HOJA DE VIDA INDICADORES MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
NOMBRE	Nivel de Cumplimiento del Plan de Tratamiento de Riesgos
OBJETIVO	Medir el porcentaje de implementación del Plan de Tratamiento de Riesgos con base a sus controles
DESCRIPCIÓN	Este indicador busca medir el nivel de avance en la implementación del Plan de Tratamiento de Riesgos del Modelo de Seguridad y Privacidad de la Información por parte de la Entidad, tomando como referencia cuáles de los controles definidos están siendo cumplidos
PERIODICIDAD	Semestral
PROCESO	Tecnología de la Información y la Comunicación
RESPONSABLE	Director Oficina de TI

HOJA DE VIDA INDICADORES MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
VARIABLES		
Orden	Nombre Variable	Und - Med
1	Cantidad de Controles Implementados en el PTR	Cantidad
2	Cantidad Total de Controles Planeados en el PTR	Cantidad

FORMULA DE CÁLCULO	
INDICADOR	Cantidad de Controles Implementados en el PTR / Cantidad Total de Controles Planeados en el PTR

MEDICIÓN DEL INDICADOR													
Orden	Variable	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Cantidad de Controles Implementados en el PTR												
2	Cantidad Total de Controles Planeados en el PTR												
Nivel de Cumplimiento del Plan de Tratamiento de Riesgos													

METAS DEL INDICADOR												
INDICADOR	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic

HOJA DE VIDA INDICADORES MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN												
Nivel de Cumplimiento del Plan de Tratamiento de Riesgos						80 %						80 %

Fuente: Elaboración Propia

BIBLIOGRAFIA

Unidad Nacional de Protección. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Gestión Tecnológica- GTE-PL-03-V3 [en línea], [revisado el 15 de junio de 2022]. Disponible en internet:gte-pl-03-v3-plan-de-tratamiento-de-riesgos-de-seguridad-y-privacidad-de-la-informacion.pdf (unp.gov.co)

Ministerio de Tecnologías de la Información y las ComunicacionesInforme_Tratamiento_de_Riesgos_MINTIC.doc. [en línea], [revisado el 15 de junio de 2022]. Disponible en internet: Plan de Tratamiento de Riesgos vigencia 2020 (mintic.gov.co)

Dirección de Gestión y Desempeño Institucional. Guía para la administración de riesgo y el diseño de controles en Entidades Públicas. [en línea], [revisado el 15 de Junio de 2022]. Disponible en internet: Guía