PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 2026

SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA

GESTIÓN DE SISTEMAS E INFORMACIÓN

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

Tabla de contenido

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

1. INTRODUCCIÓN

La Superintendencia de Vigilancia y Seguridad Privada, en su compromiso de garantizar la confiabilidad y seguridad del entorno digital y físico de la información, ha desarrollado el presente Plan de Tratamiento de Riesgos de Seguridad de la Información 2026. Este plan se basa en una estrategia preventiva que busca entender y gestionar adecuadamente los riesgos relacionados con la interrupción de las operaciones y la seguridad del entorno digital.

El plan prioriza acciones que permitan minimizar el impacto en la Superintendencia en caso de que estos riesgos se materialicen. Además, abarca la identificación, análisis, tratamiento, evaluación y monitoreo de riesgos de manera objetiva, destacando aquellas situaciones que puedan afectar el cumplimiento de los objetivos en áreas clave como el Desarrollo Digital, el empoderamiento ciudadano en el entorno digital, la Transformación Digital Sectorial y Territorial, y la Inclusión Social Digital.

Este enfoque se fundamenta en las disposiciones normativas colombianas, entre las que se destacan el CONPES 3995 de 2020, el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015), la Resolución 500 de 2021 que establece los lineamientos y estándares para la estrategia de seguridad digital, y el Modelo de Seguridad y Privacidad de información adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Adicionalmente, el plan se alinea con las buenas prácticas y los estándares internacionales ISO 27001, ISO 31000:2018, y la guía para la administración del riesgo y el diseño de controles en entidades públicas establecidos en el Modelo Integrado de Planeación y Gestión (MIPG). De esta manera, la Superintendencia de Vigilancia y Seguridad Privada establece un enfoque integral para la gestión de riesgos de seguridad de la información, fortaleciendo la confianza y la continuidad de sus operaciones en el entorno digital.

En atención a la evolución del panorama de amenazas digitales y al incremento de riesgos asociados a la ciberseguridad en las entidades públicas, el presente Plan de Seguridad y Privacidad de la Información incorpora un enfoque integral que articula la seguridad de la información con la seguridad digital y la ciberseguridad. Este enfoque considera riesgos emergentes como ataques de ingeniería social, ransomware, fuga de información, indisponibilidad de servicios digitales y compromiso de credenciales, en concordancia con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma NTC ISO/IEC 27001:2022.

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

2. OBJETIVO

Diseñar e implementar acciones para reducir los riesgos de seguridad y privacidad de la información en la Superintendencia de Vigilancia y Seguridad Privada, con el fin de mitigar la materialización de los efectos derivados y velar por el cumplimiento de los requerimientos legales, regulatorios y contractuales.

Establecer las estrategias, lineamientos y actividades orientadas a fortalecer la gestión de la seguridad, privacidad de la información y ciberseguridad en la Superintendencia de Vigilancia y Seguridad Privada, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, prevenir incidentes de seguridad digital, mitigar riesgos cibernéticos y contribuir con la continuidad de los servicios institucionales, en cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma NTC ISO/IEC 27001:2022 y el marco legal vigente.

2.1. Objetivos Específicos

El Plan de tratamiento de riesgos de seguridad y privacidad de la información da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

- Determinar el alcance de la gestión integral del riesgo enfocada en la seguridad y privacidad de la información en la Superintendencia.
- Establecer las fases y metodología para la gestión integral del riesgo asociado a los procesos de la Superintendencia.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
- Generar conciencia y cultura organizacional enfocada en la identificación de los riesgos de seguridad y privacidad de la información.
- Reducir la probabilidad de materialización de los riesgos sobre los activos de información de la Superintendencia.

3. ALCANCE

El presente Plan de Tratamiento de Riesgos de Seguridad de la Información 2026 tiene como alcance realizar una gestión eficiente de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción) en la Superintendencia de Vigilancia y Seguridad Privada.

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

Específicamente, el plan busca integrar en los procesos de la Superintendencia buenas prácticas que contribuyan a la toma de decisiones oportuna y eficaz, así como prevenir incidentes que puedan afectar el logro de los objetivos estratégicos de la entidad.

Adicionalmente, el plan establece los lineamientos y metodología para identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la Superintendencia, con especial énfasis en aquellos riesgos que se encuentren en los niveles moderado, alto y extremo, de acuerdo con los criterios de valoración definidos por la entidad.

Los riesgos que se identifiquen en niveles inferiores serán aceptados por la Superintendencia, dando prioridad a la gestión de los riesgos más críticos que puedan tener un mayor impacto en la continuidad de las operaciones y el logro de los objetivos organizacionales.

De esta manera, el Plan de Tratamiento de Riesgos de Seguridad de la Información 2026 de la Superintendencia de Vigilancia y Seguridad Privada abarca de manera integral la gestión de los riesgos en materia de seguridad y privacidad de la información, seguridad digital y continuidad de las operaciones, alineado con los lineamientos y buenas prácticas establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Incluye la gestión de riesgos de seguridad de la información y ciberseguridad asociados a amenazas internas y externas, tales como ataques informáticos, malware, ransomware, phishing, ingeniería social, accesos no autorizados, pérdida o fuga de información, fallas en la infraestructura tecnológica y afectaciones a la disponibilidad de los servicios digitales, aplicando controles preventivos y correctivos sobre los activos de información de la Superintendencia.

4. DEFINICIONES

A continuación, se describen algunos términos y definiciones relacionados con la gestión y tratamientos de los riesgos de seguridad y privacidad de la información:

- Aceptación del riesgo: Decisión informada de tomar un riesgo particular.
- Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- Causa: Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- Consecuencia: Resultado de un evento que afecta los objetivos.
- Control: Medida que modifica el riesgo.

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

- 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.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al 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).
- MSPI: Modelo de Seguridad y Privacidad de la Información
- Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- 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 de Seguridad de la Información: Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- Tratamiento del Riesgo: Proceso para modificar el riesgo.
- Vulnerabilidad: Debilidad de un activo que puede ser explotada por una o más amenazas

5. MARCO LEGAL

Marco legal del Plan de Tratamiento de Riesgos de Seguridad de la Información 2026 de la Superintendencia de Vigilancia y Seguridad Privada:

- Constitución Política de Colombia, artículos 15, 209 y 269, Ley 1581 de 2012 - Ley de Protección de Datos Personales
- Decreto 2609 de 2012 - Gestión Documental
- Decreto 1377 de 2013 - Reglamentación parcial de la Ley 1581 de 2012
- Decreto 886 de 2014 - Registro Nacional de Bases de Datos
- Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública
- Decreto 103 de 2015 - Reglamentación de la Ley 1712 de 2014
- Decreto 1074 de 2015 - Reglamentación parcial de la Ley 1581 de 2012
- Decreto 1078 de 2015 - Decreto Único Reglamentario del Sector TIC
- Decreto 1083 de 2015 - Decreto Único Reglamentario del Sector Función Pública
- CONPES 3854 de 2016 - Política Nacional de Seguridad Digital
- Ley 1915 de 2018 - Modificaciones a la Ley 23 de 1982 sobre Derechos de Autor
- Decreto 612 de 2018 - Integración de planes institucionales y estratégicos
- Decreto 2106 de 2019 - Estrategia de seguridad digital en trámites digitales

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

- Ley 1952 de 2019 - Código General Disciplinario
- Resolución 500 de 2021 - Lineamientos y estándares para la estrategia de seguridad digital
- Guía para la Administración del Riesgo y el diseño de controles, DAFP 2020
- Guía de gestión del riesgo, Modelo de Seguridad y Privacidad de la Información, MinTIC
- Modelo Nacional de Gestión de Riesgos de Seguridad Digital, MinTIC
- Guía de orientación para la Gestión de Riesgos de Seguridad Digital, MinTIC
- NTC-ISO-IEC 27001:2022- Sistemas de Gestión de Seguridad de la Información
- NTC-ISO 31000:2018 - Gestión del Riesgo
- CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital)
- Ley 2300 de 2023 (Derechos de los consumidores digitales – impacto en datos)
- Guía MinTIC de Gestión de Incidentes de Seguridad Digital (CSIRT) versión vigente
- Modelo de Madurez MSPI – MinTIC
- Lineamientos actualizados MinTIC de Seguridad Digital

6. DESARROLLO DEL PLAN

A continuación, se describe el ciclo que se ejecutará para la gestión de riesgos de seguridad de la información, siguiendo las metodologías publicadas por el DAFP y Min Tic, la cual será desarrollada a través de la ejecución de las actividades propuestas en el numeral 7.

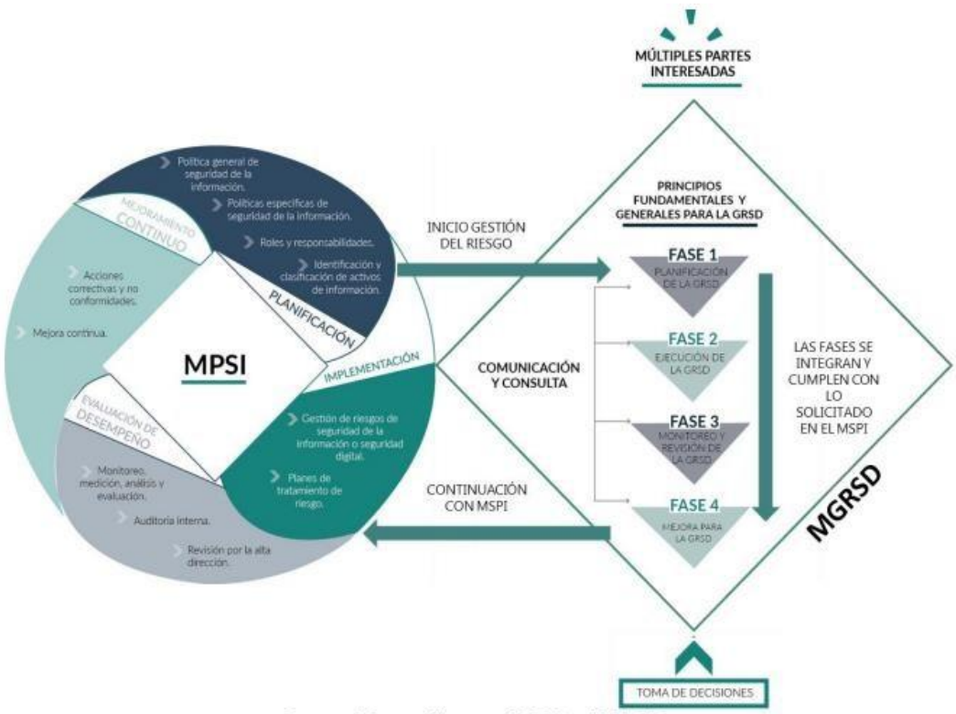


Imagen 1. Interacción entre el MSPI y el MGRSD.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

La implementación de los controles de seguridad se realizará conforme a la estructura establecida en la norma NTC ISO/IEC 27001:2022, considerando controles organizacionales, de personas, físicos y tecnológicos, orientados a la protección contra malware, seguridad en el uso de servicios en la nube, respaldo y recuperación de la información, monitoreo de eventos de seguridad y concientización del personal, con el propósito de reducir la probabilidad e impacto de los riesgos de seguridad de la información y ciberseguridad.

6.1. Análisis de información

La primera actividad clave para la identificación de riesgos es el levantamiento, clasificación y actualización de los activos de información por parte de los líderes de cada proceso institucional. Estos deberán priorizar aquellos activos que hayan sido calificados con un nivel de riesgo alto, así como otros que consideren críticos para la organización.

6.2. Identificación de riesgos

Una vez priorizados los activos, se procede a la etapa de identificación de riesgos. En esta fase se determinarán las posibles amenazas, vulnerabilidades y consecuencias que puedan afectar a uno o más de estos activos, así como la probabilidad de ocurrencia y el nivel de impacto que la materialización de estos riesgos tendría sobre la integridad, confidencialidad o disponibilidad de la información, teniendo en cuenta el siguiente cuadro:

Probabilidad			
Valor	**Nivel**	**Descripción**	**Frecuencia**
1	Rara vez	El evento puede ocurrir solo en Circunstancias excepcionales y/o la eficacia de los controles es alta.	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento y/o la eficacia de los controles es moderada	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento y/o la eficacia de los controles es baja	Al menos una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias y/o la eficacia de los controles es nula.	Al menos una vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias y/o no existen controles o si existen es nula su eficacia.	Más de una vez al año

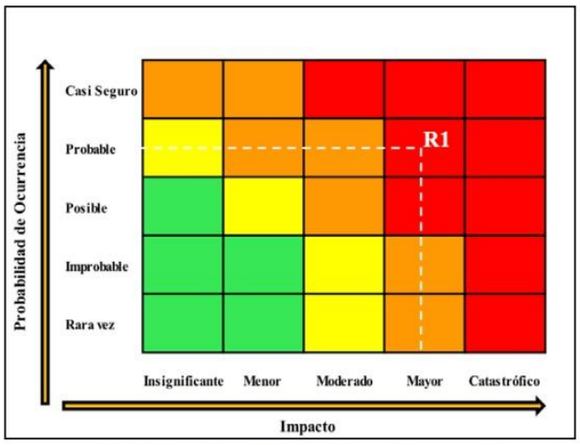
	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

6.3. Valoración y análisis del riesgo

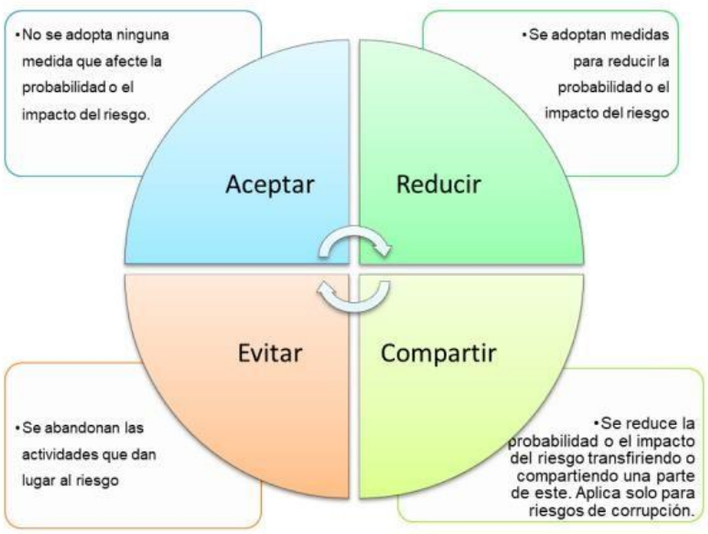
Para realizar la valoración y análisis de los riesgos, la Superintendencia establece criterios claros que permitan determinar la zona de riesgo inherente, es decir, antes de la implementación de controles. Esto se logrará a través de la estimación de la probabilidad y el impacto de cada riesgo identificado.



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. 2017.

6.4. Control del riesgo

Una vez valorados los riesgos, se procederá a la etapa de control del riesgo. En esta fase, la Superintendencia se basará en los controles propuestos en la norma NTC-ISO-IEC 27001:2022, con el objetivo de mitigar y tratar adecuadamente los riesgos asociados a posibles incidentes de seguridad. La implementación oportuna y eficaz de estos controles será fundamental para reducir la probabilidad de materialización de los riesgos.



	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

6.5. Monitoreo de riesgos

Finalmente, el plan de tratamiento de riesgos contempla una etapa de monitoreo, en la cual se revisarán periódicamente los avances en la ejecución de las actividades establecidas. Esto permitirá analizar y verificar que se estén llevando a cabo las acciones necesarias para el tratamiento de los riesgos identificados. Asimismo, se realizarán ajustes y mejoras continuas al plan, a partir de los resultados obtenidos en el monitoreo y las lecciones aprendidas.

6.6. Gestión de Incidentes de Seguridad de la Información

La Superintendencia de Vigilancia y Seguridad Privada implementará un proceso formal de gestión de incidentes de seguridad de la información y ciberseguridad, orientado a identificar, reportar, analizar, contener y recuperar oportunamente los eventos que puedan afectar la confidencialidad, integridad y disponibilidad de la información o la continuidad de los servicios institucionales.

Este proceso incluirá la definición de grupos o roles y responsabilidades, mecanismos de notificación interna, criterios de clasificación de incidentes, acciones de respuesta y recuperación, así como la documentación de lecciones aprendidas, en concordancia con los lineamientos del MSPI, la norma NTC ISO/IEC 27001:2022 y las guías emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, incluyendo el escalamiento a las instancias correspondientes cuando aplique.

7. CRONOGRAMA DE ACTIVIDADES

Para la vigencia 2026 se definen las siguientes actividades a desarrollar:

No.	Actividad	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total
1	Actualizar el Plan de Tratamiento de Riesgos alineado con ISO/IEC 27001:2022 y MSPI	X	X											100%
2	Actualizar el inventario y clasificación de activos de información		X	X										100%
3	Identificar y valorar riesgos de seguridad de la información y ciberseguridad			X	X									100%
4	Actualizar el mapa institucional de riesgos de seguridad de la información				X	X								100%

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18

No.	Actividad	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total
5	Implementar controles de seguridad alineados con ISO 27001:2022 (organizacionales, físicos, personas y tecnológicos)					X	X	X						100%
6	Ejecutar análisis y remediación de vulnerabilidades tecnológicas						X	X	X					100%
7	Fortalecer controles de acceso, autenticación multifactor y seguridad en teletrabajo						X	X	X					100%
8	Implementar y operar el proceso de gestión de incidentes de seguridad de la información						X	X	X					100%
9	Monitorear riesgos, eventos de seguridad e indicadores clave (KRI)								X	X	X	X	X	100%
10	Realizar campañas de sensibilización y capacitación en seguridad de la información				X				X			X		100%
11	Realizar revisión anual del Plan de Tratamiento de Riesgos y ajustes finales									X				100%

Cordialmente,

Mariana Quintero Tejada
Jefe Oficina de Sistemas

	NOMBRE Y CARGO	PROCESO
Elaboró	Paola Andrea Calderon Ramirez – Contratista Oficina de Sistemas	Gestión de Sistemas e información
Revisó y Aprobó	Mariana Quintero Tejada - Jefe Oficina de Sistemas	Gestión de Sistemas e información

Dirección: Calle 24A No. 59-42 Torre 4
Piso 3 Centro Empresarial Sarmiento Angulo
Conmutador: (+601) 307 8038
Línea gratuita: 01 8000 119703

Código: FOR-GDO-330-010
Fecha aprobación: 5/06/2024
Versión: 18