PLAN DE SEGURIDAD Y PRIVACIDAD 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

Supervigilancia

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 cumplimiento de la normatividad vigente, ha diseñado el presente Plan de Seguridad y Privacidad de la Información. Este plan se enmarca en la implementación de la Política de Gobierno Digital, establecida en el Decreto 767 de 2022 y compilada en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015.

La Política de Gobierno Digital y Seguridad Digital tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Uno de los habilitadores fundamentales de esta política es la Seguridad y Privacidad de la Información, que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En este contexto, la Superintendencia de Vigilancia y Seguridad Privada ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información, apoyada en un proceso de gestión del riesgo que brinde confianza a las partes interesadas.

Este documento presenta el Plan de Seguridad y Privacidad de la Información de la Superintendencia de Vigilancia y Seguridad Privada, que define los lineamientos, estrategias y actividades a implementar para contribuir con la adecuada gestión de la seguridad y privacidad de la información en la entidad.

También contempla la gestión y mitigación de riesgos de ciberseguridad que puedan afectar los activos de información de la Superintendencia. Estos riesgos incluyen, de manera explícita, ataques de ransomware, campañas de phishing, técnicas de ingeniería social o fuga de información, indisponibilidad de servicios digitales, así como el compromiso, uso indebido o robo de credenciales de acceso. La identificación, tratamiento y monitoreo de estos riesgos serán parte integral del Modelo de Seguridad y Privacidad de la Información, con la aplicación de controles preventivos y correctivos orientados a preservar la confidencialidad, integridad y disponibilidad de la información institucional.

	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

Establecer las estrategias y actividades orientadas a fortalecer la gestión de la seguridad y privacidad de la información generada, tratada y custodiada por la Superintendencia de Vigilancia y Seguridad Privada, con el fin de preservar su confidencialidad, integridad y disponibilidad, en cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y el marco legal aplicable, para generar confianza en los grupos de interés.

2.1. Objetivos Específicos

El Plan de Seguridad y Privacidad de la Información da cumplimiento al objetivo general a través de los siguientes objetivos específicos:

- Consolidar el Sistema de Gestión de Seguridad de la Información (SGSI) de la Superintendencia, mediante la implementación y mejora de los controles de seguridad establecidos en el MSPI, alineados con la norma NTC ISO/IEC 27001:2022.

- Definir y divulgar a los colaboradores de la entidad, las políticas, documentación asociada y buenas prácticas que permitan fortalecer la cultura institucional en torno a la seguridad y privacidad de la información.

- Realizar el seguimiento y evaluación de las acciones orientadas a reducir las brechas de cumplimiento de la Política de Gobierno Digital, de acuerdo con los resultados del autodiagnóstico del Modelo Integrado de Planeación y Gestión (MIPG).

- Garantizar el cumplimiento de los requisitos legales y normativos en materia de seguridad y privacidad de la información, gobierno digital y protección de datos personales.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información aplica a todos los procesos identificados en el modelo de operación por procesos de la Superintendencia de Vigilancia y Seguridad Privada, involucrando a todos los funcionarios, contratistas, proveedores y terceros que, en el cumplimiento de sus funciones, compartan, utilicen, recolecten, procesen, intercambien o consulten la información de la entidad.

De esta manera, el alcance del plan abarca:

	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

- Todos los procesos, trámites, servicios, sistemas de información, infraestructura y, en general, todos los activos de información de la Superintendencia.

- Todos los funcionarios, tanto de planta como contratistas, que tengan acceso y manipulen información de la entidad.

- Todos los proveedores y terceros que, en el marco de sus contratos o acuerdos, interactúen con la información de la Superintendencia.

- Cualquier persona o entidad que, por razones del cumplimiento de sus funciones, tenga acceso y haga uso de la información de la Superintendencia de Vigilancia y Seguridad Privada.

- El plan busca establecer los lineamientos, estrategias y actividades necesarias para preservar la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y el marco normativo aplicable.

- Incluye los entornos tecnológicos tradicionales y digitales emergentes, tales como servicios en la nube, plataformas de teletrabajo, accesos remotos, dispositivos móviles institucionales y soluciones de terceros, contribuyendo a que todos los puntos de acceso a la información cuenten con controles de seguridad adecuados, autenticación y mecanismos de monitoreo.

4. DEFINICIONES

- Activos de Información: Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Agencia Nacional de Seguridad Vial.

- Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- Control: Medida que permite reducir o mitigar un riesgo.

- Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

- Integridad: Propiedad de exactitud y completitud.

	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

- MIPG: Modelo Integrado de Planeación y Gestión.

- MSPI: Modelo de Seguridad y Privacidad de la Información.

- 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.

- Sistema de Gestión de Seguridad de la información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una institución 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

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

- Ley 1702 de 2013. Por la cual se crea la Agencia Nacional de Seguridad Vial y se dictan otras disposiciones.

	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

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1499 de 2017. Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión.

- Decreto 1008 del 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.

- Resolución 025 de 2020. Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación.

- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.

- CONPES 3975 DE 2019 Política Nacional para la Transformación Digital e
Inteligencia Artificial.

- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital, su propósito es fortalecer la capacidad para gestionar los riesgos de seguridad digital y ciberseguridad.

- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- Resolución 500 de 2021. 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.

	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

- Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- Resolución 460 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se expide el Plan Nacional de Infraestructura de Datos y Su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.

- Circular 01 de 2022 - Departamento Administrativo de la Presidencia de la República. Recomendaciones de uso de servicios en la nube como medida para mitigar riesgos de seguridad digital.

- Decreto 255 de 2022 - Ministerio de Comercio, Industria y Turismo. Por el cual se adiciona la Sección 7 al Capítulo 25 del Título 2 de la Parte 2 del Libro 2 de/ Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países.

- Directiva 02 de 2022 - Presidencia de la República. Reiteración de la política pública en materia de seguridad digital.

- Decreto 338 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por el cual se adiciona el Título 21 a la Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

- Resolución 746 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamentos adicionales a los establecidos en la Resolución No. 500 de 2021.

- Resolución 01117 de 2022 - Ministerio de Tecnologías de la Información y las Comunicaciones. Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.

- Resolución 7870 de 2022 Ministerio de Defensa Nacional – Política General de seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en la Unidades Ejecutoras o Dependencias del Ministerio de Defensa

	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

Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa

- Decreto 767 de 2022 - Presidencia de la República. 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.

- Ley 2294 de 2023 – Plan Nacional de Desarrollo 2022- 2026 "Colombia potencia mundial de la vida". Artículo 143. Transformación digital como motor de oportunidades e igualdad. Numeral 4.

- SO/IEC 27002:2022 – Catálogo actualizado de controles, en el cual se presenta un diseño para apoyar la implementación y mejora de un Sistema de Gestión de Seguridad de la Información.

- Guías del MinTIC de Gestión de Incidentes y CSIRT, donde se establecen lineamientos técnicos y operativos para la identificación, reporte, análisis, contención, erradicación y recuperación de incidentes de seguridad de la información y ciberseguridad.

- Modelo de Madurez del MSPI, herramienta que permite a las entidades públicas evaluar el nivel de implementación, efectividad y mejora continua de su Sistema de Gestión de Seguridad de la Información.

- Ley 2300 de 2023, establece disposiciones orientadas a fortalecer los derechos de los ciudadanos en los entornos digitales.

6. DESARROLLO

La Oficina de Sistemas de la SVSP establece las siguientes actividades para la implementación del El Modelo de Seguridad y Privacidad de la Información MSPI.

	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

6.1. Gestión de Inteligencia de Amenazas

La Oficina de Sistemas realizará actividades de monitoreo y análisis de inteligencia de amenazas, apoyándose en alertas emitidas por entidades gubernamentales, CSIRT nacional, MinTIC y otras fuentes oficiales. Esta información permitirá identificar riesgos emergentes como campañas de phishing, ransomware, vulnerabilidades críticas y ataques dirigidos, facilitando la adopción oportuna de medidas preventivas y correctivas que fortalezcan la postura de seguridad institucional.

6.2. Gestión de Incidentes de Seguridad de la Información

La entidad fortalecerá el proceso de gestión de incidentes de seguridad mediante la definición de procedimientos formales para la detección, clasificación, contención, erradicación, recuperación y análisis posterior de eventos de seguridad. Los incidentes serán categorizados según su nivel de criticidad y se establecerán tiempos máximos de atención y escalamiento. Así mismo, cuando aplique, se realizará la notificación a las autoridades competentes y a los titulares de la información, en cumplimiento de la normatividad de protección de datos personales.

6.3. Seguridad en Servicios en la Nube

Para el uso de servicios en la nube, la Superintendencia establecerá requisitos mínimos de seguridad que incluyan, autenticación multifactor, control de accesos basado en grupos o roles, respaldo automático de información y monitoreo. Asimismo, se realizará la evaluación periódica

	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

de los proveedores tecnológicos para verificar el cumplimiento de estándares de seguridad, protección de datos y continuidad del servicio.

6.4. Actualización de Controles de Seguridad conforme a ISO/IEC 27001:2022

La Superintendencia fortalecerá su Sistema de Gestión de Seguridad de la Información mediante la adopción y actualización de los controles establecidos en la norma ISO/IEC 27001:2022, priorizando aquellos relacionados con la seguridad de los dispositivos finales, protección contra software malicioso, seguridad en los servicios de terceros, monitoreo de eventos de seguridad. Así mismo, se implementarán mecanismos de evaluación periódica para verificar la efectividad de los controles, garantizar su alineación con los riesgos institucionales y promover la mejora continua del SGSI.

6.5. Seguridad para Teletrabajo, Acceso Remoto y Dispositivos Móviles

La Superintendencia implementará controles de seguridad específicos para los esquemas de teletrabajo, trabajo remoto y modalidades híbridas, así como para el uso de dispositivos móviles institucionales y equipos autorizados para el acceso a recursos tecnológicos. Estos controles incluirán, como mínimo, el uso obligatorio de autenticación multifactor, conexiones seguras mediante redes privadas virtuales (VPN), cifrado de la información, gestión de dispositivos finales, políticas de uso aceptable y monitoreo de accesos. Lo anterior permitirá reducir los riesgos asociados al acceso fuera del perímetro institucional y contribuir con la protección de los activos de información en entornos digitales distribuidos.

7. CRONOGRAMA DE ACTIVIDADES

La Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada ejecutará durante la vigencia 2026 las siguientes actividades orientadas a la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), en cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 y los lineamientos de Gobierno Digital.

	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	Responsable	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total
1	Monitoreo y análisis de inteligencia de amenazas (CSIRT, MinTIC y fuentes oficiales)	Oficina de Sistemas	X	X	X	X	X	X	X	X	X	X	X	X	100 %
2	Gestión de incidentes de seguridad de la información (detección, contención y recuperación)	Oficina de Sistemas	X	X	X	X	X	X	X	X	X	X	X	X	100 %
3	Actualización e implementación de controles ISO/IEC 27001:2022	Oficina de Sistemas	X	X	X			X	X	X					100 %
4	Evaluación y remediación de vulnerabilidades tecnológicas	Oficina de Sistemas		X	X			X	X						100 %
5	Implementación y fortalecimiento de controles de seguridad en servicios en la nube	Oficina de Sistemas		X	X	X			x	X	X				100 %
6	Implementación de controles de teletrabajo, acceso remoto y dispositivos móviles (VPN, MFA, cifrado)	Oficina de Sistemas	X	X	X	X	X	X							100 %
7	Monitoreo de accesos remotos y eventos de seguridad	Oficina de Sistemas	X	X	X	X	X	X	X	X	X	X	X	X	100 %
8	Capacitaciones institucionales en seguridad de la información y teletrabajo seguro	Oficina de Sistemas	X		X		X		X		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	Responsable	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total
9	Simulacros de incidentes de ciberseguridad	Oficina de Sistemas			X						X				100 %
10	Autoevaluación del SGSI (MSPI – ISO/IEC 27001:2022)	Oficina de Sistemas							X	X	X				100 %
11	Realizar revisión anual del Plan de Tratamiento de Riesgos y ajustes finales	Oficina de Sistemas								X					100 %

Tabla 1 Cronograma de actividades

8. RESPONSABILIDAD

Este documento y la ejecución de las actividades es responsabilidad de la Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada.

La Oficina de Sistemas liderará la coordinación del Sistema de Gestión de Seguridad de la Información, apoyándose en las áreas misionales y administrativas de la entidad. Así mismo, se promoverá la conformación de un Comité de Seguridad de la Información encargado de realizar seguimiento estratégico, aprobar planes de mejora, evaluar riesgos críticos y apoyar la toma de decisiones en materia de seguridad digital.

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