Resolución N°

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación de la Superintendencia de Vigilancia y Seguridad Privada"

EL SUPERINTENDENTE DE VIGILANCIA Y SEGURIDAD PRIVADA,

En ejercicio de sus facultades constitucionales y legales, en especial las conferidas por el Decreto Ley 356 de 1994, Decreto 2355 de 2006, la Ley 1437 de 2011, la Ley 1581 de 2012, y demás normas concordantes,

CONSIDERANDO

La **Ley 1266 de 2008** regula el manejo de la información contenida en bases de datos personales, estableciendo las disposiciones generales del habeas data y delineando las obligaciones de las entidades en relación con la seguridad de la información.

La **Ley 1581 de 2012** desarrolla las disposiciones generales para la protección de datos personales, estableciendo los principios y obligaciones que deben seguirse en el tratamiento de datos personales para garantizar su confidencialidad, integridad y disponibilidad.

La **Ley 1273 de 2009** tipifica penalmente las conductas contra la confidencialidad, integridad y disponibilidad de la información, estableciendo la protección de los datos como un bien jurídico tutelado.

La **Ley 1712 de 2014**, conocida como la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, regula el acceso a la información pública y establece los procedimientos y garantías para asegurar la transparencia en la administración pública, incluyendo la protección de la información y los datos personales.

Que el **Decreto 1078 de 2015** expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que incorpora normativas sobre la gestión de la seguridad de la información y establece los lineamientos generales para la protección de los activos de información en las entidades públicas.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Resolución N°

La Superintendencia mediante **Resolución 20171400016907 de 2017** "adopta el Manual de Políticas de Seguridad de la Información de la Superintendencia de Vigilancia y Seguridad Privada".

Que la Superintendencia se alinea a la **Resolución 7870 de 2022** del Ministerio de Defensa Nacional, Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos de las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector defensa.

Que la Superintendencia de Vigilancia y Seguridad Privada ha adoptado la Norma Técnica Colombiana NTC-ISO/IEC 27001 como base para la implementación, mantenimiento y mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI), alineándose con los estándares internacionales y con el Modelo de Seguridad y Privacidad de la Información del Gobierno Digital (MinTIC).

La Superintendencia de Vigilancia y Seguridad Privada reconoce la importancia de la seguridad de la información como un activo estratégico para el cumplimiento de su misión de control, inspección y vigilancia de los servicios de vigilancia y seguridad privada. Por tanto, es esencial que todas las actividades relacionadas con la gestión de la información se realicen bajo un marco normativo sólido que garantice la protección adecuada de los datos y activos de información.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO PRIMERO: Adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación de la Superintendencia de Vigilancia y Seguridad Privada, la cual está alineada con la Norma Técnica Colombiana NTC-ISO/IEC 27001 y el Modelo de Seguridad y Privacidad de la Información del Gobierno Digital (MinTIC).

ARTÍCULO SEGUNDO: Designar a la Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada como la encargada de liderar la implementación, monitoreo y actualización continua de la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación. Esta oficina será responsable de asegurar que los controles de seguridad definidos en la política se apliquen adecuadamente, así como de

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Resolución N°

coordinar las estrategias de capacitación y concienciación en seguridad de la información para todos los empleados y contratistas.

ARTÍCULO TERCERO: Derogar cualquier resolución, acto administrativo o disposición que sea incompatible con lo dispuesto en la presente Resolución.

ARTÍCULO CUARTO: La presente Resolución entrará en vigor a partir de la fecha de su publicación. La Oficina de Comunicaciones será responsable de su divulgación y de garantizar que sea incluida en el plan institucional de capacitación e inducción.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

YENNIFFER EDILMA PARRA MOSCOSO
SUPERINTENDENTE DE VIGILANCIA Y SEGURIDAD PRIVADA

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN

SUPERINTENDENCIA DE VIGILANCIA Y SEGURIDAD PRIVADA

Mayo 2025

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN

TABLA DE CONTENIDO

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

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

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN

1. INTRODUCCIÓN

La Política de Seguridad y privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación de la Superintendencia de Vigilancia y Seguridad Privada (en adelante SuperVigilancia), permite tener un panorama resumido de los requerimientos y normatividad que se contempla con respecto a la seguridad integral de la información de la entidad, que busca proteger la información generada, compartida, comunicada o almacenada.

La superintendencia de Vigilancia y Seguridad Privada ejerce, control, inspección y vigilancia e impulsa la legalidad en la prestación del servicio en la industria de los servicios de seguridad privada, a través de mecanismos que generen transparencia, confianza y eficiencia, para fortalecer la seguridad humana basada en la igualdad en todo el territorio nacional.

La implementación de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN como pilar del Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ISO/IEC 27001, busca para la Superintendencia de Vigilancia y Seguridad Privada fortalecer los procesos y aplicar las mejores prácticas de seguridad de la información, seguridad digital, ciberseguridad y continuidad de la operación contribuyendo al mejoramiento continuo y al logro de los objetivos estratégicos.

La información puede existir en muchas formas, digital, impresa, en papel, se almacena en archivos físicos o electrónicos, se transmite por correo físico, electrónico u otro medio de intercambio electrónico, también se considera información la comunicada de manera oral, ya sea en una conversación o en una capacitación.

Con base en lo anterior, la Seguridad de la información tiene como objetivo la protección de esta ante una serie de riesgos que atenten contra los principios fundamentales de la misma, es decir; la confidencialidad, la integridad y la disponibilidad de la información en cualquiera de sus estados, teniendo en cuenta las partes interesadas internas como Responsables de procesos, Funcionarios y Contratistas, Oficina de Sistemas, entre otros y Partes interesadas externas como Entes Reguladores, Proveedores, Grupos al Margen de la Ley, Hackers y Clientes entre otros.

La Política de Seguridad de la Información Seguridad Digital, Ciberseguridad y Continuidad de la Operación de la SuperVigilancia, toma como base los controles y requisitos identificados en el estándar ISO/IEC 27001, así como la Resolución 7870 del 26/12/2022 del Ministerio de Defensa Nacional y la Directiva Permanente N°. DIR2014-18 "Política de Seguridad de la Información para el Sector Defensa" del Ministerio de Defensa Nacional.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Las normas incluidas en la presente política constituyen parte fundamental del Modelo de Gestión de Seguridad de la Información de la SuperVigilancia y son la base para la implementación de controles, procedimientos y demás documentos requeridos para el desarrollo del SGSI. La Seguridad de la Información, la Seguridad Digital, la Ciberseguridad y la Continuidad de la Operación, son prioridad para la entidad y por ende es responsabilidad de todos los funcionarios y contratistas velar por el continuo cumplimiento de lo emanado en la política y los lineamientos definidos para el desarrollo del SGSI.

2. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios y, en consecuencia, debe ser protegido.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Auditoría: Proceso sistemático independiente y documentado que permite obtener evidencia de auditoría y evaluar de manera objetiva para determinar en qué medida son alcanzados los criterios de auditoría.

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo.

Custodio del activo de información: Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Evaluación de riesgos: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gestión de Incidentes de Seguridad de la Información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información (ISO/IEC 27001).

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

ISO 27001: Estándar para sistemas de gestión de la Seguridad de la Información adoptado por ISO/IEC.

ISO 22301: Requisitos para un Sistema de gestión de la Continuidad del negocio

No repudio: Es un concepto que garantiza que alguien no puede negar algo Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la Seguridad de la Información.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI: Sistema de Gestión de Seguridad de la Información.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

3. OBJETIVOS DE LA PRESENTE PÓLITICA

3.1. Objetivo General

Establecer, implementar, mantener, mejorar y socializar la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN, documento que define lineamientos y comportamientos que deben seguir todos los funcionarios, contratistas, terceros o cualquier persona que tenga una relación contractual con la SuperVigilancia, frente al uso y manejo de la información en la Superintendencia de Vigilancia y Seguridad Privada, Política basada en el modelo MSPI de MINTIC y la norma ISO/IEC 27001, alineada a las directrices del Ministerio de Defensa Nacional y al cumplimiento de los objetivos estratégicos de la SuperVigilancia.

La presente Política busca proteger la Confidencialidad, Integridad y Disponibilidad de la información en los activos y procesos, fortalecer la seguridad digital, la ciberseguridad y la continuidad de las operaciones administrativas, operativas y logísticas de la SuperVigilancia e incluye:

- Establecer los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, continuidad y no repudio de la información en Superintendencia de Vigilancia y Seguridad Privada.

- Definir los lineamientos necesarios para mitigar los incidentes y gestionar los riesgos y controles de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad, y Continuidad de la Operación, de acuerdo con la normatividad y disposiciones legales vigentes aplicables a la SuperVigilancia.

- Prevenir los incidentes de Seguridad de la Información, Seguridad Digital y Ciberseguridad, implementando controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y alto desempeño del sistema de gestión de seguridad de la información.

- Gestionar los riesgos de Seguridad de la Información que involucran los activos de información de la SuperVigilancia.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango - Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano - Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez - Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Garantizar la continuidad de la operación de la SuperVigilancia.

- Capacitar y Concienciar a los funcionarios, contratistas y demás partes interesadas en Seguridad de la Información.

3.2. Objetivos Específicos

- Proteger los recursos de información frente a amenazas internas y externas, deliberadas o accidentales, preservando la confidencialidad, integridad y disponibilidad de la información, implementando los controles requeridos.

- Fortalecer el modelo organizacional de Seguridad de la Información, definiendo los roles y responsabilidades de los funcionarios, contratistas y terceros que interactúan con el SGSI.

- Promover, mantener y realizar un mejoramiento continuo a nivel de cultura en Seguridad de la Información.

- Lograr la concienciación de todos los funcionarios, contratistas y demás partes interesadas que interactúen con los sistemas y activos de información de la SuperVigilancia, minimizando la ocurrencia de incidentes de Seguridad de la Información.

- Mantener actualizada la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación y promover su cumplimiento al interior de la SuperVigilancia.

4. ALCANCE

La Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación y sus posteriores actualizaciones, acorde con la naturaleza jurídica, misión y visión de la Superintendencia de Vigilancia y Seguridad Privada, busca establecer y mantener en el tiempo los controles de seguridad de la información, seguridad digital, ciberseguridad y continuidad de la operación que garanticen la integridad, disponibilidad y confidencialidad de la información en nuestros procesos institucionales, misionales de apoyo, estratégicos y procesos de evaluación, sus plataformas tecnológicas, activos de información y sus riesgos.

5. DESTINATARIOS

La presente Política aplica a toda la entidad, funcionarios servidores públicos, contratistas y terceros, que hacen uso de los recursos y activos de información de la SuperVigilancia, así como a los designados para su uso y custodia, siendo de obligatorio cumplimiento.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

6. RESPONSABLE DEL CUMPLIMIENTO

La Oficina de Sistemas de la Superintendencia de Vigilancia y Seguridad Privada, será la encargada de la implementación de la presente Política y velará por su estricto cumplimiento.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento con la presente política.

El incumplimiento a la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación o las que se requieran para desarrollar el SGSI que puedan afectar la integridad, disponibilidad y confidencialidad de la información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

7. MARCO NORMATIVO

LEYES

Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", Reglamentada Parcialmente por el Decreto 1074 del 2015.

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", Reglamentada por el Decreto 1081 del 2015.

Ley 1523 de 2012" Por la cual se adopta la política nacional de gestión de desastres y se establece El Sistema Nacional de Gestión del Riesgo de Desastres.

DECRETOS

Decreto Único Reglamentario 1074 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo" (Capítulo 25: reglamenta parcialmente la Ley 1581 de 2012 y, Capítulo 26: reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos).

Decreto 1078 de 2015 Expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, que incorpora normativas sobre la gestión de la seguridad de la información y establece los lineamientos generales para la protección de los activos de información en las entidades públicas.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

Decreto 1081 de 2015 "por medio del cual se reglamenta la Ley 1712 de 2014, en lo relativo a la gestión de la información pública".

Decreto 1499 de 2017 "por medio del cual se modifica el Decreto número 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".

Decreto 612 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 767 de 2022 "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".

RESOLUCIONES

Resolución 20171400016907 de 2017 "Por medio del cual se adopta el Manual de Políticas de Seguridad de la Información de la Superintendencia de Vigilancia y Seguridad Privada".

Resolución 0500 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".

Resolución 7870 de 2022 "Por la cual se emite y adopta la política General de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de los servicios tecnológicos de la unidades ejecutoras o Dependencias del Ministerio de defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa".
Resolución 746 de 2022 "Por la cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021".

Resolución 0644 de 2025 "Por la cual se adopta la Política Sectorial de Interoperabilidad para el Sector Defensa."

NORMAS

NTC ISO/IEC 22301:2019 Gestión de Continuidad de Negocio.

NTC ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad, y protección de la privacidad.

NTC ISO/IEC 31000:2018 Gestión de Riesgos.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

CONPES 3854 de 2016 Incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

CONPES 3995 de 2020 Política Nacional para ampliar la Confianza y Seguridad Digital en Colombia.

8. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN.

La supervigilancia cuenta con la siguiente estructura organizacional para los temas de Seguridad de la información:

1. El Comité Institucional de Gestión y Desempeño.
2. El CIO (Jefe de la Oficina de Sistemas)
3. El Oficial de Seguridad de la Información.
4. El líder o propietario de cada proceso
5. Los propietarios de los activos de Información

El Comité Institucional de Gestión y Desempeño ha aprobado la resolución No. 2020—0008067 del 20 de febrero de 2020 que deroga la resolución No. 20181210069057 del 03 de septiembre de 2018, *"Por medio de la cual se adopta los Comités Internos en la Superintendencia de Vigilancia y Seguridad Privada y se modifica la Resolución No. 20153100057947 del 29 de septiembre de 2015"*, que en su CAPÍTULO IX define entre sus otras las acciones relacionadas con la Seguridad de la Información enmarcadas en las áreas de Gobierno Digital y Seguridad Digital.

El mencionado comité está conformado por:

1. El Superintendente de Vigilancia y Seguridad Privada o su delegado
2. El Secretario General
3. El jefe de la Oficina Asesora de Planeación, quién actuará como Secretario Técnico.
4. El Superintendente Delegado para la Operación
5. El Superintendente Delegado para el Control
6. El jefe de la Oficina Asesora Jurídica
7. El jefe de la Oficina de Sistemas

La Oficina de Control Interno participa con voz y sin voto.

El oficial de seguridad de la información o quien haga sus veces, podrá asistir cuando el comité se reúna con el propósito de tratar temas de seguridad digital y de la información o relacionadas con estas.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

El Coordinador de Gestión Documental o quien haga sus veces, podrá asistir cuando el comité se reúna con el propósito de tratar temas de actualización y conservación de documentos y registros relacionados con el SGSI.

El Comité Institucional de Gestión y Desempeño se reunirá ordinariamente por lo menos una vez (1) cada tres meses, con la mitad más uno de sus miembros, y sus decisiones serán tomadas por la mayoría simple, pero podrá reunirse extraordinariamente cada vez que sea necesario. A dichas reuniones podrán asistir como invitadas las personas que se consideren necesarias de acuerdo con los asuntos a debatir.

8.1. Roles y Responsabilidades con el SGSI.

A continuación, se describen los roles y responsabilidades en seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación, que son asignados en la Supervigilancia, a fin de reducir el riesgo de materialización de un incidente de seguridad de la información.

ROL/ÁREA	RESPONSABILIDADES
Comité Institucional de Gestión y Desempeño	• Aprobar las políticas de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Aprobar los lineamientos de seguridad de la información que se deben implementar para mantener las limitaciones que los propietarios de la información requieren.
Alta Dirección	• Ser propietario legal de los activos de información. • Brindar los recursos necesarios para garantizar el cumplimiento de las políticas de política de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Verificar el cumplimiento de la normatividad vigente, en particular la difusión y adopción de las políticas, normas y estándares de política de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Promover el desarrollo de una cultura de Seguridad de la Información mediante campañas de sensibilización y concientización. • Implementar, apoyar y soportar el Sistema de Gestión de Seguridad de la Información. • Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal en temas relacionados con Seguridad de la Información.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

	• Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del sistema de gestión de Seguridad de la Información.
Jefes	• Asegurar que las personas que se encuentran bajo su control protejan la información de conformidad con las normas y directrices de la SuperVigilancia • Promover el desarrollo de una cultura de Seguridad de la Información mediante campañas de sensibilización y concientización. • Promover el cumplimiento por parte del personal bajo su responsabilidad de. las políticas de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación.
CIO (jefe de la Oficina de Sistemas)	• Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo. • Definir e implementar la estrategia de concientización y capacitación en Seguridad de la Información para los funcionarios, contratistas y demás terceros, cuando aplique. • Custodiar la información y los medios de almacenamiento bajo su responsabilidad. • Gestionar la plataforma tecnológica que soporta los procesos de la entidad. • Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los funcionarios y contratistas. • A través de las áreas de Seguridad de la Información debe:

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

	➢ Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros. ➢ Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad. ➢ Establecer, documentar y dar mantenimiento a los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información administrada por esta oficina. ➢ Gestionar la Inteligencia de Amenazas cibernéticas al interior de la Oficina de Sistemas. ➢ Gestionar los incidentes de Seguridad de la Información que se presenten en la SuperVigilancia. ➢ Mantener listado actualizado de contacto con autoridades en caso de incidentes que así lo ameriten y grupos de interés que apoyen los conocimientos sobre ciberseguridad y seguridad de la información.
Oficial de Seguridad de la Información	• Asesorar a la alta dirección en todo lo relacionado con el SGSI. • Desarrollar políticas, procedimientos y normas para garantizar la seguridad, confidencialidad y la privacidad de la información que sea consistente con la normatividad vigente y aplicable a la SuperVigilancia. • Evaluar riesgos basados en informes de inteligencia de amenazas. • Supervisar e informar sobre cualquier incidente de información por intrusión y activar las estrategias para evitar nuevos incidentes. • Asegurar que a los activos de información se han asignado las clasificaciones de seguridad apropiadas. • Mantener y conservar los activos de información como se define por el propietario. • Velar por que la implementación de cualquier cambio se realice de acuerdo con el procedimiento de gestión de cambios. • Velar por la actualización de la información del registro de inventario de activos. • Definir e implementar las salvaguardas apropiadas para preservar la confidencialidad, integridad y

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

	disponibilidad de la información y los activos que la contienen. • Hacer una evaluación y seguimiento de medidas de seguridad para garantizar su cumplimiento y reportará las situaciones de incumplimiento. • Mantener listado actualizado de contacto con autoridades en caso de incidentes que así lo ameriten y grupos de interés que apoyen los conocimientos sobre seguridad de la información.
Todos los funcionarios	• Mantener los comportamientos que minimicen los riesgos de Seguridad de la Información. • Promover la adopción de una cultura de seguridad de la información. • Ser capacitados en Seguridad de la Información para generar conciencia de los riesgos, sus responsabilidades y la necesidad de respetar las políticas de Seguridad de la Información, en el ejercicio normal sus actividades. • Informar sobre cualquier violación a la seguridad de la información siguiendo los procedimientos definidos.
custodios de información	• Asegurar que a los activos de información se han asignado las clasificaciones de seguridad apropiadas. • Velar que las limitaciones aprobadas por el comité se mantengan para cada activo de información. • Aprobar los usuarios que están autorizados para pertenecer a cada rol informático, de acuerdo con lo mencionado en la matriz de roles y responsabilidades.
El propietario de la Información (El líder o propietario del proceso)	• Mantener actualizado el inventario de activos de información. • Clasificar los activos de Información. • Asignar custodios de seguridad de cada activo de información que se use en su proceso. • Identificar el nivel de clasificación adecuado para los mismos. • Definir e implementar las salvaguardas apropiadas para preservar la confidencialidad, integridad y disponibilidad de la información y los activos de información que la contienen. • Evaluar y hacer seguimiento a las medidas de seguridad para garantizar su cumplimiento y reportar las situaciones de incumplimiento. • Comunicar sus requerimientos de seguridad de información al líder del área de Seguridad de la Información de la Oficina de Sistemas.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

	• Determinar y autorizar todos los privilegios de acceso a sus activos de información. • Comunicar al Área de Seguridad de la Información sus requerimientos en capacitación sobre temas de seguridad la información. • Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
Oficina de Recursos Humanos	• Incluir en los programas de inducción y de reinducción lo relacionado con Seguridad de la Información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público.
Oficina de Control Interno	• Evaluar la aplicación y cumplimiento de la política de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación definida en esta Directiva, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.
Funcionarios, contratistas y terceros	• Cumplir con las políticas de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación. • Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.

9. REVISIONES Y ACTUALIZACIONES A LA PRESENTE POLÍTICA.

Las revisiones y actualizaciones a la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación, se realizarán periódicamente alineadas con las necesidades del negocio, las regulaciones y los riesgos cambiantes. Las revisiones a la presente política aseguran el compromiso de buscar una mejora continua del SGSI de la SuperVigilancia. Esto permite estar alineados en el cumplimiento de la Política de Gobierno Digital emanada por el estado colombiano, MINTIC y las Directrices del Ministerio de Defensa Nacional en temas de Seguridad Digital.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Se realizará una revisión anual de la política para evaluar su efectividad, el cumplimiento de sus objetivos y su adecuación a las necesidades actuales de la organización.
- La política será revisada cuando se produzcan cambios estructurales significativos en la organización, tales como reestructuraciones de áreas o procesos, que puedan afectar su implementación o alcance.
- Se actualizará la política cuando ocurran cambios en el entorno normativo, regulatorio o tecnológico que requieran ajustes en los controles de seguridad y privacidad.
- En caso de incidentes de seguridad que revelen vulnerabilidades significativas o fallos en los controles actuales, se realizará una revisión y actualización de la política para fortalecer su efectividad.
- El Oficial de Seguridad de la Información será responsable de supervisar la implementación de los cambios necesarios y de coordinar con las áreas correspondientes para asegurar que las actualizaciones se implementen de manera efectiva. Además, el Oficial deberá comunicar las modificaciones de la política a todos los empleados y partes interesadas para garantizar su conocimiento y cumplimiento.

a. Garantías y Principios.

i. Garantías

La presente Política de Seguridad y Privacidad de la Información, Seguridad Digital Ciberseguridad y Continuidad de la Operación permitirá garantizar los adecuados niveles de:

- Confidencialidad, garantizando el acceso sólo para los usuarios autorizados.
- Integridad, evitando modificaciones no autorizadas.
- Disponibilidad, garantizando que la información esté disponible cuando se necesite.
- Minimizar el riesgo en las funciones más importantes de la entidad, incluidos los riesgos ambientales que puedan afectar la seguridad de la información.
- Cumplimiento de principios de seguridad de la información.
- Cumplimiento de los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Apoyar las acciones que contribuyan a minimizar el impacto del cambio climático como por ejemplo acciones que aporten ahorro de energía en la entidad.

- Proteger los activos tecnológicos.

- Fortalecer los contactos con Autoridades y Grupos de Interés para generar Inteligencia de amenazas que pueda ayudar a prevenir riesgos y minimizar posibles impactos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación.

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas, terceros, aprendices, practicantes y clientes de La Supervigilancia.

- Garantizar la continuidad del negocio frente a varios tipos de incidentes, incluyendo escenarios de desastres naturales relacionados con el cambio climático.

- La Supervigilancia ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

ii. Principios

- El SGSI apoya el cumplimiento de los objetivos corporativos, la misión y la visión de la SuperVigilancia.
- La SuperVigilancia debe tener en cuenta todos los requisitos legales, reglamentarios y contractuales en la gestión del SGSI con el fin de evitar el incumplimiento de sus obligaciones en materia de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación.

- La SuperVigilancia debe establecer y aplicar un programa documentado para la gestión del riesgo de seguridad de la información de acuerdo con los requisitos de la norma ISO/IEC 31000. Los criterios para la evaluación y aceptación de los riesgos deben ser establecidos, formalizados y aprobados por la alta dirección de la entidad. Se contemplará la evaluación de riesgos climáticos para asegurar la protección de la información.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Los riesgos de Seguridad de la Información serán monitoreados y se tomarán acciones pertinentes cuando los mismos cambien o no sean aceptables.

- Se pondrán en conocimiento de todos los funcionarios de la SuperVigilancia, sus responsabilidades con relación al SGSI y la seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación que sean pertinentes al rol desempeñado.

- Las Directivas de la SuperVigilancia reconocen que la gestión de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación forma parte de la cultura organizacional, por lo cual se comprometen con el cumplimiento de los objetivos y alcance del sistema, asegurando que los recursos necesarios estén disponibles para ello.

- La presente Política se soporta técnica y operativamente en el SGSI de la Supervigilancia y en su Manual de Políticas de Seguridad de la Información Código: MAN-GSI-140-029.

10. ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN.

A continuación, se relacionan algunas acciones identificadas que afectan la disponibilidad, confidencialidad e integridad y que ponen en riesgo la Seguridad de la Información:

- Permitir que personas ajenas a la SuperVigilancia ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
- Tomar fotos, selfis o imágenes donde se evidencia información de la SVSP

- No clasificar y/o etiquetar la información.

- No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral.

- No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

- Reutilizar papel que contenga información sensible.

- Dejar documentos o notas escritas con información sensible sobre las mesas.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – Jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Dejar en los equipos destinados a capacitación información sensible o confidencial.

- Hacer uso de la red de datos de la SuperVigilancia para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

- Instalar software en la plataforma tecnológica de la SuperVigilancia cuyo uso no esté autorizado por la Oficina de Sistemas, y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.

- Enviar información clasificada de la SuperVigilancia por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

- Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la SuperVigilancia.

- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de la SuperVigilancia sin la debida autorización.

- Ingresar a la red de datos de la SuperVigilancia por cualquier servicio de acceso remoto sin la autorización de la Oficina de Sistemas.

- Usar servicios de internet en los equipos de la SuperVigilancia, diferente al provisto por la Oficina de Sistemas.

- Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la SuperVigilancia para beneficio personal.
- Uso de la identidad institucional digital (cuenta de usuario y contraseña) de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario o contratista.

- Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.

- Retirar de las instalaciones de la SuperVigilancia computadores de escritorio, portátiles e información física o digital clasificada, sin autorización o abandonarla en lugares públicos o de fácil acceso.

- Entregar, enseñar o divulgar información clasificada de la SuperVigilancia a personas o entidades no autorizadas.

- Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de la SuperVigilancia o de terceras partes.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		

- Ejecutar cualquier acción que difame, afecte la reputación o imagen de la SuperVigilancia o alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.

- Realizar cambios no autorizados en la Plataforma Tecnológica de la SuperVigilancia.
- Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

- Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación.

- Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo.

- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la Seguridad de la Información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso.

11. VIGENCIA

La presente política entrará en vigor a partir de la fecha de su publicación oficial y será divulgada por la oficina de Comunicaciones a todos los funcionarios de planta, contratistas y partes interesadas de la Superintendencia de Vigilancia y Seguridad Privada.

	NOMBRE Y CARGO	PROCESO
Elaboró	Miguel Antonio García Arango – Seguridad de la Información	GESTIÓN DE SISTEMAS E INFORMACIÓN
Revisó	Juan Sebastián Hernández Serrano – Oficina Jurídica	GESTIÓN JURIDICA
Revisó y Aprobó	Sol Marina Cure Flórez – jefe Oficina de Sistemas	GESTIÓN DE SISTEMAS E INFORMACIÓN
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma		