MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN SUPERVIGILANCIA

SISTEMA GESTIÓN DE LA CALIDAD
Código: MAN-GSI-140-029
Fecha aprobación: 04/07/2020
Versión: 9

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

TABLA DE CONTENIDO

RESUMEN

La Política de Seguridad de la Información 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 al SGSI de la entidad, que busca proteger la información, independiente de cuál sea su forma, incluso esta puede ser compartida, comunicada o almacenada.

INTRODUCCIÓN

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.

La Política de Seguridad de la Información de la SuperVigilancia, toma como base los controles y requisitos identificados en el estándar ISO/IEC 27001:2013, así como en la Directiva Permanente N°. DIR2014-18 “Política de Seguridad de la Información para el Sector Defensa” del Ministerio de Defensa Nacional.

Las normas incluidas en el presente manual 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 es 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.

Mediante los controles de seguridad de la información establecidos por el SGSI se busca minimizar el riesgo empresarial asociado, y maximizar el retorno de las inversiones y oportunidades de negocios alineadas al cumplimiento de los objetivos del negocio.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

CAPITULO I GENERALIDADES

1. OBJETIVOS DEL SGSI

1.1 Objetivo General

Establecer, Implementar, mantener, mejorar y socializar el ***Sistema de Gestión de Seguridad de Información - SGSI*** basado en la política de Gobierno Digital y la norma ISO/IEC 27001:2013, alineado al cumplimiento de los objetivos estratégicos de la SuperVigilancia.

El documento define los criterios y comportamientos que deben seguir todos los funcionarios, contratistas, terceros o cualquier persona que tenga una relación contractual con la SuperVigilancia, o que tenga acceso a los activos de información y al SGSI.

Se busca proteger la Confidencialidad, Integridad y Disponibilidad de la información y fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad e incluye:

- Definir políticas, procedimientos y formatos asociados al cumplimiento del SGSI.
- Minimizar los riesgos de Seguridad de la Información asociados al SGSI.
- Alinear el SGSI con la normatividad y disposiciones legales vigentes aplicables a la SuperVigilancia.
- Gestionar los riesgos de Seguridad de la Información que involucran los activos de información de la SuperVigilancia.
- Cumplir las obligaciones legales, regulatorias y contractuales relacionadas con Seguridad de la Información.
- Gestionar los incidentes de Seguridad de la Información.
- Capacitar y Concienciar a los funcionarios, contratistas y demás partes interesadas en Seguridad de la Información.

1.2 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.
- Establecer un 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 la política de Seguridad de la Información actualizada.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

2. ALCANCE DEL SGSI

El presente manual y la política de Seguridad de la Información y sus posteriores actualizaciones aplica a todos funcionarios, 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.

El incumplimiento de lo estipulado en el presente manual, política de seguridad de la información o las que se requieran para desarrollar el SGSI que puedan afectar la integridad, disponibilidad y confidencialidad de la información, acarrean sanciones disciplinarias de acuerdo con las obligaciones, deberes y responsabilidades definidas.

3. DEFINICIONES

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición.

Acción preventiva: Medida de tipo proactivo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

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.

Acuerdo de Confidencialidad: Es un documento en el cual los funcionarios o terceras partes manifiestan su voluntad de mantener la reserva de la información, comprometiéndose a no divulgar, usar o explotar la información a la que tengan acceso en virtud de la labor que desarrollan.

Administración de riesgos: (Gestión de riesgos) Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales.

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.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditor: Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

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.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad.

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

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

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información.

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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización, tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

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.

Evento: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de Seguridad de la Información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

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.

Impacto: Resultado de un incidente de Seguridad de la Información.

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).

Ingeniería Social: Es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización.

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO 27001: Estándar para sistemas de gestión de la Seguridad de la Información adoptado por ISO. Es certificable. La versión actual es la publicada en el año 2013.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo.

No repudio: 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.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

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.

Plan de tratamiento de riesgos: Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de Seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

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.

Registros de Auditoría (Log de auditoria): Son archivos donde se registran los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

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.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

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

Vulnerabilidades: Son las debilidades, huecos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables (amenazas), las cuales se constituyen en fuentes de riesgo.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La SuperVigilancia consiente del valor de la información, como activo vital, siendo una herramienta de gran importancia para la toma de decisiones y en cumplimiento de su misión, visión y valores corporativos, protege la información propia y en custodia, garantizando 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.

Tomando como base que la efectividad de la política depende del comportamiento de las personas, (por lo que saben, lo que sienten y de que estén dispuestos a realizar) y los controles establecidos en las políticas de seguridad descritas en el presente documento,

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información de Gobierno Digital.

4.1 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 de la Información.
- 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 31000:2018. Los criterios para la evaluación y aceptación de los riesgos deben ser establecidos, formalizados y aprobados por la alta dirección de la entidad.
- 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 de la Información que sean pertinentes al rol desempeñado.
- Las Directivas de la SuperVigilancia reconocen que la gestión de seguridad de la información 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.

5. 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.
- No diligenciar la evaluación de la mesa de ayuda cuando se resuelve un ticket.
- 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.
- 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 Informática y 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 Informática y Sistemas.

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

- 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 de la Información.

- 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.

6. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Seguridad de la información está compuesta por:

1. El Comité Institucional de Gestión y Desempeño.
2. El CIO (Jefe de la Oficina de Informática y 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 estará 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 Informática y Sistemas
8. El Asesor del Grupo de Recursos Humanos
9. El Asesor de Comunicaciones
10. El Asesor del Grupo de Recursos Financieros

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.

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.

7. ROLES Y RESPONSABILIDADES CON EL SGSI

ROL/ÁREA	RESPONSABILIDADES
Comité Institucional de Gestión y Desempeño	• Aprobar las políticas de seguridad de la Información. • 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 Seguridad de la Información. • Verificar el cumplimiento de la normatividad vigente, en particular la difusión y adopción de las políticas, normas y estándares de Seguridad de la Información. • 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. • 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 de la Información.
CIO (jefe de la Oficina de Informática y Sistemas)	• Promover el cumplimiento por parte del personal bajo su responsabilidad de las políticas de Seguridad de la Información. • Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información. • Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de Seguridad de la Información. • 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: ➢ 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 los incidentes de Seguridad de la Información que se presenten en la SuperVigilancia.
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. • 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 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.
El Gestor de Información	• Proporcionar asesoramiento especializado en relación con las prácticas de gestión de seguridad de la información. • Contribuir a la dirección estratégica de la gestión de la información dentro de la SuperVigilancia. • Ayudar a las unidades de negocio a definir y comprender sus responsabilidades con relación a la gestión de seguridad de la información. • Ayudar a las unidades de negocio para identificar sus necesidades y requerimientos en materia de seguridad de la información. • Planificar e implementar los sistemas de administración de los activos de información de la SuperVigilancia.
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 Informática y Sistemas. • 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	• Validar por la aplicación y cumplimiento de las políticas de Seguridad de la Información definidas 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 de la Información. • Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.

8. RESULTADOS ESPERADOS

- Los Incidentes de Seguridad de la Información no resultarán en costos considerables e inesperados o en graves perturbaciones de los servicios y actividades de negocio.
- Se implementarán controles de Seguridad de la Información adecuados y proporcionados para proteger los activos de información y generar confianza en las partes interesadas.
- Las decisiones sobre asuntos de Seguridad de la Información se basarán en una evaluación de riesgos formulada por la SuperVigilancia.
- Se cumplirán los requisitos legales, reglamentarios y contractuales aplicables a la SuperVigilancia en términos de Seguridad de la Información.
- Las mejoras al sistema de gestión de seguridad de la información – SGSI – tendrán como insumo, las revisiones que se realicen por entes externos con el fin de validar el grado de implementación o de madurez del sistema, las cuales se deben realizar por lo menos dos veces al año, las cuales podar ser de tipo auditoria, gap, preauditoria o revisión del SGSI. Estas revisiones deben ser realizadas por un especialista en la norma ISO 27001 vigente o por una empresa especializada que permita a la entidad llegar a certificarse en esta norma en el año 2021 para de esta manera apoyar el cumplimiento de la política de gobierno digital emanad por el estado colombiano.

9. REFERENCIA NORMATIVA

9.1 Antecedentes

La información es un activo vital para el éxito y el cumplimiento de la misión de la SuperVigilancia, el presente documento se encuentra alineado con la política de Gobierno Digital y la familia de normas de la serie ISO 27000 vigentes como marco de referencia para la implementación de su sistema de gestión de Seguridad de la Información y se alinea con la normatividad colombiana vigente que le aplica.

La información y la plataforma tecnológica que la soporta es considerada un activo estratégico para la SuperVigilancia, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información. Estos activos de información se constituyen en el soporte de la misión y la visión, por lo que requieren ser utilizados y manejados dentro de un entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

La implementación de un Sistema de Gestión de Seguridad de la Información está orientada a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información bajo los criterios de preservación de la confiabilidad, disponibilidad e integridad de la información.

9.2 Referencias Normativas

A continuación, se hace referencia a la normatividad base para el desarrollo e implementación de la tecnología y los sistemas de información del sector defensa:

Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000.	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Decreto 1747 de 2000.	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: “Las entidades de certificación, los certificados y las firmas digitales”.
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos Administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1266 de 2008	Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información.
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 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.
Decreto 4890 de 2011	Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional y Se dictan otras disposiciones.
CONPES 3701 de julio del 2011	Lineamientos de política para ciberseguridad y ciberdefensa
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales y su decreto reglamentario 1377 del 27 de junio de 2013.
Decreto 19 de 2012	Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

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.
Resolución No. 03049 del 24 de agosto de 2012	Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información.
Resolución 1374 de 2012	Por la cual se adiciona la resolución 127 de 2012 “Por la cual se crean y organizan Grupos Internos de Trabajo del Ministerio de Defensa Nacional”.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
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.
Resolución 10584 de 2014	Por la cual se modifica parcialmente la resolución 1374 de 2012, -para ajustar las funciones del Grupo de Tecnología de Información y las Comunicaciones TIC.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014 - 2018.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones – Título 9 – Capítulo I.
CONPES 3854 de abril del 2016	Política Nacional de Seguridad Digital
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del Sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 620 de 2020	El cual subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, y busca establecer los lineamientos generales para regular las interacciones entre los ciudadanos y la administración pública a través de los medios electrónicos.
Norma Técnica Colombiana NTC – ISO/IEC 27001:2013	Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.
Directiva Permanente N°. DIR2014-18	Política de Seguridad de la Información para el Sector Defensa” del Ministerio de Defensa

CAPITULO II POLÍTICAS GENERALES

1. POLÍTICA DE CONTROL DE ACCESO A LOS SISTEMAS

Los responsables y/o dueños de la información deben determinar las reglas de control de acceso apropiadas de acuerdo con las actividades que desarrolla cada uno de los funcionarios, según su rol dentro de la compañía y evaluando los riesgos asociados al uso de esta. Por lo tanto, son ellos quienes autorizan o retiran los permisos para el uso de un activo de información teniendo en cuenta lo establecido en:

- Los procedimientos de control de acceso físico definidos.
- El acceso a servidores, bases de datos, Internet, correo electrónico y aplicaciones deben realizarse bajo los lineamientos definidos y establecidos por la Oficina de Informática y Sistemas.
- La administración de usuarios debe realizarse bajo los lineamientos definidos por la Oficina de Informática y Sistemas.
- Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
- Los usuarios SuperAdministradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado y digitalmente en un gestor de contraseñas como *"keepas*[i]*"* en un área segura donde designe la entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite ante una amenaza de compromiso de estas.
- Todas las contraseñas utilizadas por usuarios y administradores de sistemas deben cumplir con los lineamientos definidos por la Oficina de Informática y Sistemas.
- La interconexión con redes externas debe ser configurada bajo los lineamientos definidos por la Oficina de Informática y Sistemas.

Para la implementación de controles de acceso que no estén descritos en este documento, se tendrá como referencia la legislación vigente aplicable a la SuperVigilancia y la necesidad de conocer.

1.1 Segregación de Funciones

- Todos los funcionarios, contratistas o terceros que tengan acceso a la infraestructura tecnológica o a los sistemas de información de la SuperVigilancia, deben contar con una definición clara de los roles y funciones sobre estos para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.
- La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por la Oficina de Informática y Sistemas con el fin de mantener actualizada dicha información y acorde con la realidad de cada una de las dependencias de la SuperVigilancia.

Los usuarios son responsables de realizar un adecuado uso de las herramientas de seguridad y de las actividades realizadas con sus cuentas de usuario o mecanismos de autenticación asignados que se ponen a su disposición.

En el documento "Estándar de Contraseñas" se amplían los lineamientos relacionados con las contraseñas al interior de la Entidad.

2. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Se debe proteger la integridad, disponibilidad y confidencial de la información en tránsito frente a interceptaciones, copia, modificación o destrucción no autorizadas, que puedan afectar los principios de integridad, disponibilidad o confidencialidad de la información, todo intercambio de información con Clientes, Proveedores o terceros debe quedar formalizado en un acuerdo de Intercambio de Información que será un anexo del contrato suscrito entre las partes.

3. POLÍTICA DE USO ADECUADO DE LOS RECURSOS

Los funcionarios, contratistas y/o terceros tendrán a su disposición el uso de recursos tecnológicos y/o de infraestructura, de acuerdo con las funciones laborales que así lo requieran, para el uso de estos recursos, los funcionarios, contratistas y/o terceros aceptan y se acogen a las Políticas de Seguridad de la Información incluyendo el cumplimiento de las siguientes responsabilidades o deberes:

- Los recursos deben usarse estrictamente para fines laborales y nunca deben transmitir, procesar y/o almacenar información personal.
- No se permite transmitir, almacenar y/o procesar información que atente contra la propiedad intelectual o derechos de autor.
- Se prohíbe la transmisión, almacenamiento y/o procesamiento de SPAM (Correo no deseado o no solicitado) y/o cualquier tipo de archivo de procedencia desconocida o infectado con algún tipo de software malicioso.
- Se prohíbe la transmisión, almacenamiento y/o procesamiento de material relacionado con pornografía, armas, alcohol o actividades ilícitas.
- Se prohíbe el uso e instalación de software ilegal o sin licenciar, al igual que todo tipo de programas (Keyloggers, Crackers, entre otros.) que atenten o faciliten la perdida de la integridad, disponibilidad o confidencialidad de la información.
- Todo intercambio de información se debe acoger a lo mencionado en la Política de Intercambio de Información.
- Los recursos tecnológicos pueden ser accedidos y monitoreados por un ente de control de la SuperVigilancia, sin incurrir en violación de la privacidad, puesto que dichos recursos son asignados para la labor contratada.
- La instalación de cualquier tipo de software en los equipos de cómputo es responsabilidad exclusiva de la Oficina de Informática y Sistemas, por tanto, son los únicos autorizados para realizar esta labor.
- Ningún activo de información adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador.
- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por la Oficina de Informática y Sistemas.
- Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.
- Los requerimientos de recursos tecnológicos de las diferentes áreas deben ser avalados por la Oficina de Informática y Sistemas.
- Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por la Oficina de Informática y Sistemas.

- Los equipos de cómputo asignados deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o contratista responsable de dicho equipo finalice su vinculación con la SuperVigilancia.

- De acuerdo con el literal anterior, la SuperVigilancia no debe almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de estos.

3.1 Correo Electrónico

La asignación de una cuenta de correo electrónico de la SuperVigilancia se da como herramienta de trabajo para cada uno de los funcionarios que la requieran dentro del desempeño de sus funciones, así como a contratistas que lo requieran para el desempeño de su labor; su uso se encuentra sujeto a las siguientes reglas:

- El correo electrónico debe utilizarse únicamente para labores propias de la SuperVigilancia.

- No se debe enviar información de la entidad a cuentas de correo personales o divulgar información de esta en las redes sociales, excepto aquellas que, por motivo de la operación de la SuperVigilancia, se han establecido con los clientes o terceros y autorizados por el área indicada para intercambio de información.

- Todos los mensajes de correo deben ir firmados según el Estándar de Firmas de Correo Electrónico.

- Los mensajes y la información contenida en los buzones de correo son de propiedad de la SuperVigilancia y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y tráfico de esta se considera de interés de las Entidades del Sector Defensa.

- El tamaño de los buzones y mensajes de correo serán determinados por la Oficina de Informática y Sistemas.

- No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:

  - Enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

  - Enviar mensajes no autorizados con contenido religioso o político.

  - El envío de archivos adjuntos con extensiones como .mp3, .wav, .exe, .com, .dll, .bat, .msi o cualquier otro archivo que ponga en riesgo la Seguridad de la Información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por la Oficina de Informática y Sistemas.

  - El envío de información relacionada con la defensa y la seguridad nacional a otros dominios diferentes al de cada una de las entidades y dependencias que conforman el Sector Defensa, sin la autorización previa del Despacho y el respectivo propietario de la información.

  - El envío masivo de mensajes corporativos deberá ser solicitado por el jefe del Área que lo requiere y debe contar con la aprobación de la respectiva Oficina de Informática y Sistemas.

- Toda información generada que requiera ser transmitida fuera de la SuperVigilancia, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Sólo puede ser enviada en el formato original bajo la

responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido y deben conservar, en todos los casos, el mensaje legal institucional de confidencialidad.

- Todo correo electrónico deberá tener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

  - El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.

  - El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.

  - En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

  - Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

3.2 Red e Internet

El uso de la red e Internet como herramienta de trabajo permite a los funcionarios y contratistas acceder a sitios relacionados con el desarrollo las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes normas:

- No se debe hacer uso del servicio de navegación en ningún servidor de, se exceptúa el proceso de actualización de parches y definiciones de antivirus y todos aquellos requeridos por los proveedores previa aprobación mediante el respectivo control de cambios.

- Todos los accesos a internet de los equipos institucionales deben ser realizados a través de los canales provistos por la entidad

- La navegación en Internet es controlada de acuerdo con las restricciones de navegación definidas para los usuarios y está destinada únicamente a las actividades laborales de la Supervigilancia.

- No se permite la navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

- No se permite la publicación o envío de información confidencial sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

- No se permite la utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados por la Oficina de Informática y Sistemas.

- No se permite la publicación de anuncios comerciales o material publicitario, salvo la oficina de Comunicaciones cuando lo requiera. Estas solicitudes, deben ser justificadas por el jefe de la oficina de Comunicaciones y avaladas por el despacho del Superintendente.

- No se permite la descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.

- Está prohibido el uso de cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la SuperVigilancia para el envío o recepción de información institucional.

- No se permite el uso de herramientas de mensajería instantánea no autorizadas por la Oficina de Informática y Sistemas.

- Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios, contratistas y demás terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

- Se podrá permitir el acceso a redes sociales solamente en los horarios y condiciones definidos por la Supervigilancia.

3.3 Computadores Portátiles y de Escritorio

- Los funcionarios y contratistas no podrán usar al interior de la SuperVigilancia computadores portátiles y/o de escritorio personal que no sean autorizados por la SuperVigilancia.

- Cada usuario es responsable de velar por el respaldo de la información de sus equipos de trabajo.

- Los usuarios deben bloquear la sesión de sus equipos de trabajo, cuando se ausenten de su puesto.

- Se prohíbe la conexión de dispositivos de almacenamiento externos, diferentes a los proporcionados por la SuperVigilancia para el objeto de la labor contratada.

- Los equipos que hacen parte de la infraestructura tecnológica de la SuperVigilancia deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado a los mismos.

- La SuperVigilancia adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

- Los funcionarios y contratistas velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.

- Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática y Sistemas, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.

- Los equipos portátiles deberán estar asegurados con la guaya o el mecanismo que se defina para su protección

- La SuperVigilancia garantizará la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

3.4 Computación Móvil dispositivos móviles

- Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso y mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.

- La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por la Oficina de Informática y Sistemas, previa autorización

del jefe inmediato y la verificación de contar con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la información y la infraestructura que la contiene.

3.5 Medios de Almacenamiento

- Se prohíbe el ingreso a las instalaciones de cualquier medio de almacenamiento que no sea propiedad de la entidad (USB, Discos Externos, CD, Cámaras Fotográficas o de Video, etc) y su posterior conexión en la infraestructura tecnológica. En los casos que se requiera por motivos laborales o del negocio, el ingreso debe ser autorizado por el jefe del área.

- Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica de la SuperVigilancia, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

- Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.

- La SuperVigilancia definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas por la Oficina de Informática y Sistemas, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.

- Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.

- Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir, según sea el caso con la destrucción física del mismo o borrado seguro.

3.6 Seguridad de los Equipos Fuera de las Instalaciones

- Los usuarios que requieran usar los equipos fuera de las instalaciones de la SuperVigilancia deben velar por la protección de estos sin dejarlos desatendidos en lugares públicos o privados en los que se puedan ver comprometidos la imagen o información sensible.

- En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información sensible relacionada con la defensa y la seguridad nacional, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento Gestión de Incidentes de Seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.

- Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la SuperVigilancia deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene.

3.7 Uso de Computación en la Nube

- La SuperVigilancia podrá implementar servicios privados en la nube, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.
- Los servidores públicos y contratistas no tienen permitido almacenar información en la nube (Dropbox, Onedrive y similares) que no hayan sido autorizados por la oficina de Informática y Sistemas

3.8 Uso de Redes Inalámbricas

- Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.

- La Oficina de Informática y Sistemas será la responsable de validar a quien se le asignarán los servicios a través de redes inalámbricas.

- En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

3.9 Control de Acceso

- El Datacenter cuenta con un sistema de control de acceso biométrico (huella dactilar), tarjeta de proximidad y clave para su ingreso. Además, cuenta con una cámara que graba únicamente cuando existe actividad al interior por medio de un sensor de movimiento. Las personas que ingresan al Data Center quedan registradas en el software instalado en el equipo del administrador de red y el jefe de la Oficina de Informática y Sistemas.

- Los sistemas de información, dispositivos de procesamiento y comunicaciones definidos por la Oficina de Informática y Sistemas contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

- Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática y Sistemas de la SuperVigilancia deberá estar creado previa autorización del jefe inmediato.

- Todo identificador de usuario establecido para un tercero o contratista debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.

- La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario se determina por La Oficina de Informática y Sistemas y deben revisarse a intervalos regulares y modificar o reasignar estos cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

- Los equipos de contratistas y demás terceros que requieran acceder a las redes de datos de la SuperVigilancia deben cumplir un procedimiento de verificación de cumplimiento de informática antes de concedérseles dicho acceso.

- Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de Informática y Sistemas, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

4. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA DESPEJADA

Todos los funcionarios, Contratistas o terceros que hagan uso de la infraestructura de la SuperVigilancia, para el desarrollo de sus labores deben:

- Mantener la información objeto de su labor debidamente custodiada y salvaguardada del acceso de personas no autorizadas, de acuerdo con la clasificación de los activos de información.

- Mantener los puestos de trabajo organizados y la información clasificada como Confidencial, deberá guardarse bajo llave o en lugares vigilados mientras el funcionario responsable de la misma no esté trabajando con ella.

- Conservar la pantalla libre de accesos directos a información clasificada como Confidencial.

- Verificar que en los equipos asignados o bajo su responsabilidad se bloquee la sesión de trabajo, cuando se ausenten.
- Evitar que los documentos que contengan información clasificada como Confidencial, se expongan en las impresoras, fax, fotocopiadoras y escáneres.
- Evitar riesgos de pérdida o deterioro de la información que reposa en los puestos de trabajo por acciones que atenten contra las normas corporativas.
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
- Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del usuario.
- Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la SuperVigilancia, el cual se activará automáticamente después del tiempo de inactividad definido por la Oficina de Informática y Sistemas, y se podrá desbloquear únicamente con la contraseña del usuario.
- Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
- No se deberá reutilizar papel que contenga información sensible.
- Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.
- Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

5. POLÍTICA DE COMPUTACIÓN MÓVIL

Los funcionarios, contratistas y/o terceros de la SuperVigilancia que tienen a su cargo equipos de computación y comunicación móvil asignados y/o autorizados por la compañía, deberán custodiar dichos equipos para evitar la fuga, pérdida o alteración de la información consignada en los mismos y propia de su labor, teniendo en cuenta:

5.1 Normas para uso de equipos de computación móvil (portátiles)

- Evitar el acceso a redes públicas.
- No acceder a paginas no autorizadas (Pornografía, Redes sociales, Paginas de Música o descargas, etc.) que puedan colocar en riesgo la información de la compañía.
- Cambiar periódicamente la contraseña.
- Tener cuidado de ser observado por terceros.
- Evitar dejar el equipo en lugares no seguros.
- Abstenerse de tener carpetas o discos compartidos.
- Realizar los backups periódicamente.
- Abstenerse de instalar aplicaciones o programas no autorizados.

- Velar por que la información almacenada en el equipo se encuentre debidamente cifrada o protegida.

- Devolver el equipo al finalizar su relación contractual.

6. POLÍTICA DE RESPALDO DE INFORMACIÓN

La SuperVigilancia velara por la conservación de la información, realizando copias de respaldo de esta, para tal fin, la Oficina de Informática y Sistemas es responsables de aplicar el proceso definido para ello, teniendo en cuenta:

- Se debe mantener y actualizar un inventario específico de la información a respaldar. El tipo, la frecuencia, sitio de almacenamiento y el tiempo de retención de los respaldos de la información deben ser definidos teniendo en cuenta la clasificación de la información y la normatividad vigente.

- Todas las copias de respaldo de la SuperVigilancia deben ser incrementales. La copia de seguridad incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación en los archivos, comparándola con la hora y fecha del último backup. La aplicación de backup identifica y registra la fecha y hora de realización de las operaciones de backup para identificar los archivos modificados desde esas operaciones. Como una copia de seguridad incremental sólo copia los datos a partir del último backup de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de una copia de seguridad incremental es que copia una menor cantidad de datos que una copia de seguridad completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio de almacenamiento.

- Se debe asegurar que la información definida en conjunto por la Oficina de Informática y Sistemas y las dependencias responsables de la misma, y que se encuentra contenida en la plataforma tecnológica de la SuperVigilancia, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el Procedimiento Gestión de Copias de Respaldo y recuperación.

- Los medios de las copias de respaldo se almacenarán localmente y en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

- Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia.

- Para garantizar que la información de los funcionarios y contratistas sea respaldada, es responsabilidad de cada uno mantener copia de la información que maneja.

- La Oficina de Informática y Sistemas de la SuperVigilancia, establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia e identificación, y definirá conjuntamente con las dependencias los períodos de retención de esta.

- Se debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada en el Data Center.

7. POLÍTICA DE USO DE CONTROLES CRIPTOGRÁFICOS

Teniendo en cuenta la información de acuerdo con su clasificación y criticidad, normatividad vigente y/o acuerdos contractuales, esta se debe proteger con mecanismos de cifrado, contemplando:

- Información transmitida por canales de comunicación.
- Información contenida en medios de almacenamiento (USB, Discos, CDs, DVDs, Cintas, otros).
- Copias de Respaldo.
- Información propia de la compañía transmitida a otras entidades.
- Información propia de la compañía correspondiente a ideas, estrategias, conceptos, propuestas, costos e información contable en general, cuando sea transmitida a destinatarios externos a la compañía.
- Información que se tenga almacenada en los datacenter internos o externos (datacenter, proveedores, cloud).
- Las páginas web publicadas a Clientes o en Internet deberán contar con certificado digital.

8. POLÍTICA DE USO DE CONTRASEÑAS

Toda cuenta de usuario es de uso personal e intransferible, su utilización debe ser exclusiva para fines laborales objeto de la labor contratada,

Como una de las buenas prácticas para el aseguramiento de la información propia, los funcionarios, contratistas o terceros que hacen uso de la infraestructura tecnológica de la SuperVigilancia son responsables de:

- Mantener la confidencialidad de las contraseñas.
- Evitar conservar registros físicos de las contraseñas.
- No compartir la contraseña de sus cuentas de usuario asignadas.

Las contraseñas que se asignan a los Clientes para acceso y utilización de aplicativos o sistemas de información, deberán ser entregadas físicamente vía correo personalizado o certificado, o telefónicamente.

- La administración, así como la entrega de las contraseñas a los usuarios deberá realizarse por la Oficina de Informática y Sistemas.
- Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:
  - Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
  - Las contraseñas no deberán ser reveladas.
  - Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento establecido por la Oficina de Informática y Sistemas.
  - Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la SuperVigilancia.

- Las contraseñas no se deben guardar de forma automática en los inicios de sesión de las aplicaciones (Correo Electrónico, Orfeo, etc); igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.

- Es deber de cualquier funcionario y contratista reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

Cualquier incidente de seguridad de información que se presente por el mal uso de una contraseña, será responsabilidad del propietario de la cuenta y deberá ser informado a Seguridad de la información.

9. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

En la SuperVigilancia la información estará clasificada dentro los niveles definidos y se deberá mantener un inventario actualizado de los activos de información teniendo en cuenta:

- Procedimiento de Inventario y Clasificación de Activos de Información.
- Procedimiento de Etiquetado de Activos de Información.
- Estándar de Manejo de Activos de Información.

Se consideran **ACTIVOS DE INFORMACIÓN**, aquellos propios de las labores para ejercer su objeto de negocio. La información que por la naturaleza del negocio se procesa, almacena y custodia datos de terceros (clientes, proveedores, etc.), no se consideran activos de información propios puesto que corresponden a activos del tercero, sobre los cuales aplican las políticas y procedimientos que éste ha definido en materia de clasificación y etiquetado. Los líderes de procesos son responsables de actualizar e informar a Seguridad de la Información de todo cambio o novedad relacionada con los activos de información bajo su responsabilidad. El área de seguridad de información es responsable de realizar en conjunto con los líderes de proceso el inventario, la actualización de este y clasificación de los activos de información por lo menos una vez por año.

9.1 Gestión de Activos de Información

- La SuperVigilancia tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.

- La SuperVigilancia debe identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.

- La SuperVigilancia debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

- Se debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa su seguridad: confidencialidad, integridad y disponibilidad.

- La SuperVigilancia deberá definir procedimientos para el rotulado y manejo de información de acuerdo con el esquema de clasificación definido.

9.2 Trabajo en Áreas Protegidas

- En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:
  - No se deben consumir alimentos ni bebidas.
  - No se deben ingresar elementos inflamables.
  - No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
  - No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
  - No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
  - No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.
- Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

10. POLÍTICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE INFORMACIÓN

La gestión de riesgos de seguridad de la información forma parte de la cultura organizacional y se promueve a todos los niveles de la SuperVigilancia, cuyo fin es garantizar el cumplimiento de los objetivos dentro de un ámbito de seguridad que permita la menor exposición al riesgo dentro de los criterios establecidos.

Para su cumplimiento la Alta Dirección, es la responsable de proveer y garantizar los recursos necesarios para la adecuada Gestión de Riesgos de Seguridad de la Información, así como de velar por el cumplimiento de todas las actividades concernientes a la identificación, planeación, administración, seguimiento y control de los riesgos de seguridad de la información.

La gestión de riesgos de seguridad de la información se realizará conforme a los lineamientos descritos en el Procedimiento de Gestión de Riesgos de Seguridad de la Información.

11. POLÍTICA DE TRABAJO REMOTO O TELETRABAJO

Considerando la necesidad de brindar agilidad en el desarrollo de las labores diarias de la SuperVigilancia se permite el acceso desde redes externas solo en los siguientes casos:

- **Soporte técnico**: Por parte del personal de tecnología para labores de soporte a la plataforma tecnológica, que estén justificadas con base en la criticidad de la operación o actividad a realizar.
- **Acceso de clientes o proveedores**: Para acceso de los clientes o proveedores a aplicaciones desarrolladas como objeto del negocio contratado con los mismos. Los permisos para descargar e imprimir información deberán estar autorizados formalmente, teniendo en cuenta que se deben cumplir las normas vigentes de seguridad de la información.

Quienes deban realizar un tipo de conexión como los mencionados anteriormente deben estar autorizados por los dueños de los procesos correspondientes previo cumplimiento de las normas y lineamientos emanados por el área de Seguridad de Información y solicitados formalmente mediante la herramienta que disponga la SuperVigilancia.

Cuando se establezcan contratos con terceros de monitoreo, soporte u operación de la plataforma tecnológica se deberán:

- Establecer acuerdos de confidencialidad y manejo seguro de la información.
- Limitar dentro del contrato los tipos de acceso que se tendrán y la responsabilidad del tercero con respecto a la información a monitorear o que reside en los equipos objeto de soporte u operación.
- Generar logs de las actividades realizadas con el fin de contar con los reportes que serán revisados por los diferentes entes de Control o Seguridad de la Información según sea el caso.

Para los casos en los que se autorice el trabajo remoto o teletrabajo se tiene que cumplir con:

- El teletrabajador debe resguardar la información institucional, impidiendo el acceso a terceras personas, en consecuencia, el acceso a la información de la Supervigilancia será ejecutado bajo la responsabilidad del teletrabajador dando cumplimiento a las normas establecidas en la entidad.
- El teletrabajador debe utilizar la información, incluyendo los datos personales, únicamente para las labores propias de su cargo.
- El acceso de los teletrabajadores a los sistemas de información de la entidad se realizará a través de una VPN o mecanismo seguro aprobado por la oficina de Informática y Sistemas.
- El teletrabajador debe cumplir las mismas medidas de seguridad definidas como si estuviera laborando en las instalaciones de la entidad.
- Queda prohibido la cesión de cualquier tipo de datos a terceros, ni siquiera a efectos de conservación.
- El teletrabajador debe evita compartir información de la entidad con familiares, amigos o terceros.
- En caso de usar una red inalámbrica para sus conexiones, la misma debe tener las características de una red segura tal como la que se maneja en las instalaciones de la Supervigilancia.

12. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Todos los funcionarios y contratistas de la SuperVigilancia son responsables de reportar los eventos e incidentes de Seguridad de Información de los cuales tengan conocimiento, es responsabilidad del grupo de Seguridad de Información gestionar el reporte e investigación de estos, de acuerdo con las siguientes definiciones:

- **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio, red o del entorno que indica una posible violación de las políticas de seguridad de la información de la SuperVigilancia, falla en los controles o situación previamente desconocida que puede ser relevante para la seguridad de la información.

- **Incidente de Seguridad de la Información:** Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones de la SuperVigilancia y amenazan la confidencialidad, integridad y/o disponibilidad de la información.

Para dar cumplimiento a lo mencionado anteriormente se debe:

- En todos los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática se deberán generar registros de eventos (logs) que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.

- El tiempo de retención de los logs estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.

- Todo evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la Oficina de Informática y Sistemas mediante el procedimiento de Gestión de Incidentes de seguridad.

12.1 Gestión de Incidentes de Seguridad de la Información

- Los funcionarios y contratistas de la SuperVigilancia deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
- Para gestionar los incidentes de Seguridad de la Información deberá existir como mínimo un funcionario con conocimientos en el manejo de incidentes en las Áreas de Seguridad de la Información.

- Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.

- Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad de la Información para la Entidad.

- Se debe llevar un registro detallado de los incidentes de Seguridad de la Información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.

- Las áreas de Seguridad de la Información deben propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de Seguridad de la Información.

- Los resultados de las investigaciones que involucren a los funcionarios de la SuperVigilancia deberán ser informados a las áreas de competencia.

- La SuperVigilancia deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de Seguridad de la Información.

13. POLÍTICA DE SEGURIDAD INFORMÁTICA

Para velar por la seguridad de la información se debe cumplir con las siguientes directrices las cuales buscan generar conciencia a los funcionarios y contratistas sobre la importancia y sensibilidad de los procesos y recursos críticos que permiten a la SuperVigilancia crecer y mantener su competitividad, para ello se debe garantizar la Seguridad Informática teniendo en cuenta lo siguiente:

13.1 Protección contra Software Malicioso

- Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y Seguridad de la Información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar ante posibles fallos ocasionados por código malicioso.

- Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Oficina de Informática y Sistemas, y deberán ser actualizados permanentemente.

- No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.

- Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de la SuperVigilancia deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la Seguridad de la Información.

- La SuperVigilancia será responsable de velar que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

- Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

13.2 Seguridad de Equipos de Cómputo

- Habilitar y tener configurado en todos los equipos de escritorio y portátiles un software de firewall personal, cuyas reglas no puedan ser modificadas por los usuarios, ni detener el servicio.
- Habilitar y tener configurado en todos los equipos de cómputo de la SuperVigilancia, software de protección contra software malicioso, ajustado para actualizarse de forma automática y realizar evaluaciones periódicas de los sistemas, cuyas reglas no puedan ser modificadas por los usuarios, ni detener el servicio.

- Mantener actualizado todos los equipos de cómputo de la SuperVigilancia con los últimos parches de seguridad proporcionados por los fabricantes. La aplicación de los parches debe realizarse dentro de un periodo máximo de un mes a partir de su liberación (previa verificación de la no existencia de fallos o errores en el parche a aplicar).

- Deben estar activos los registros de auditoria localmente, se deben registrar los eventos de seguridad y aquellos que sean definidos en las guías de Hardening.

- Realizar un borrado seguro para todo equipo (PC, Servidor, otros equipos asignados para el desarrollo de las labores diarias) que deba ser reasignado, trasladado o dado de baja.

- Devolver el equipo al finalizar su relación contractual con la SuperVigilancia.

13.3 Seguridad de la red

- Mantener un diagrama actualizado de la red de la SuperVigilancia.

- Impedir la conexión directa de entrada o salida de tráfico entre Internet y las redes de la SuperVigilancia.

- Ubicar los sistemas que proporcionan servicios de acceso público dentro de un esquema de zona segura (DMZ, Zona Desmilitarizada) que permita limitar el tráfico.

- Ubicar los sistemas de bases de datos en una red interna segregada de la zona segura.

- Restringir los servicios prestados o suministrados por su dirección IP.

- Realizar la configuración de la seguridad en firewalls según Estándar de Seguridad de Firewalls, adicionalmente se debe validar que toda regla está documentada en el Firewall y que el uso de todos los protocolos se encuentre justificado.

- Mantener un documento actualizado de los servicios, protocolos y puertos abiertos en firewalls, en el mismo se debe incluir la justificación pertinente en los casos que se estén utilizando protocolos no seguros (HTTP, FTP, Telnet, IMAP, POP3,

SNMP, entre otros). Este documento debe estar disponible en caso de ser solicitado por los entes de control y/o auditorias de certificación.

- Seguir el procedimiento de control de cambios, definido por la SuperVigilancia, teniendo en cuenta que todo cambio en la configuración de firewalls, routers y VPNs debe ser realizado por el área de Informática y Sistemas, el cual debe ser documentado y contar con la aprobación del dueño del proceso o área solicitante; con previo cumplimiento de los lineamientos emanados por el área de Seguridad de la información.

- Realizar una inspección semestral de la configuración de firewall y routers por parte de las áreas de Informática y Sistemas y el área de Seguridad de la Información.

- Cambiar las credenciales, configuraciones y demás valores que los dispositivos de red traen incorporados de fábrica, las mismas deben ser modificadas antes de su salida al ambiente de producción.

- Deshabilitar las cuentas de usuario innecesarias que los dispositivos de red traen incorporados de fábrica, deben ser modificados antes de su salida al ambiente de producción.

- Configurar los sistemas críticos de la SuperVigilancia con base en los manuales de blindaje que son provistos y actualizados por el área de Seguridad de la Información.

- Asegurar y afinar todo Servidor antes de su paso a producción con base en los manuales de blindaje que son provistos y actualizados por el área de Seguridad de la Información.

- Evitar la configuración o la existencia de más de una función o rol (se exceptúan los servicios o roles instalados por limitaciones técnicas de la plataforma) que requieren diferentes niveles de seguridad en un mismo servidor.
- Habilitar sólo servicios y protocolos seguros que sean necesarios según lo requiera la función del sistema.

- Cifrar todo acceso administrativo a sistemas críticos de la SuperVigilancia que no sean realizados directamente sobre la consola.

- Sincronizar el reloj a nivel de sistema operativo en todos los sistemas (servidores, equipos activos de red y máquinas de usuarios), teniendo como referencia el NTP autorizado. No se debe permitir la desactivación del sistema de sincronización o la manipulación manual de la hora.

- Habilitar y/o configurar un certificado digital en las aplicaciones web publicadas en internet para acceso a información de clientes o información crítica del negocio o cuando sea requerido contractualmente, el certificado digital debe ser emitido por una entidad certificadora reconocida y valida.

- Asegurar que los servicios o aplicaciones que sean publicados para su acceso a través de la red cuenten con un nombre descriptivo a través del cual puedan ser identificados por medio de los servidores DNS locales, en lugar de utilizar la dirección IP donde se encuentre dicho servicio o aplicación.

- Realizar pruebas de vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios por lo menos semestralmente.

- Realizar una prueba de penetración semestralmente o en caso de realizar cambios críticos en la infraestructura.

- No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la Oficina de Informática y Sistemas, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los

activos informáticos de la SuperVigilancia, o a la utilización de estos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

- Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.

- El área de Seguridad de la Información de la Entidad realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

- Periódicamente, la correspondiente Área de Seguridad de la Información realizará una verificación de alertas de seguridad emitidas por organizaciones y foros de Seguridad de la Información de orden nacional y/o internacional, con el fin de verificar la información más reciente que se encuentre disponible respecto a vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

- La Oficina de Informática y Sistemas de la SuperVigilancia realizará las revisiones de las alertas de seguridad informadas por sus respectivas Áreas de Seguridad de la Información y dado el caso en que las alertas sean válidas en el entorno de operación de las plataformas tecnológicas asociadas, se deberá definir por parte de dichas oficinas un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

13.4 Documentación de procedimientos operativos

- La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

- Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas.

- La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por la Oficina de Informática y Sistemas y el Jefe de la dependencia que usa la aplicación.

- Los procedimientos operativos deben contener instrucciones para el manejo de errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

13.5 Control de Cambios Operativos

- Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la Oficina de Informática y Sistemas de la SuperVigilancia, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

- Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de Control de Cambios. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

El área de Informática y Sistemas debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la SuperVigilancia a los funcionarios y contratistas, los cuales deberán estar debidamente

documentados y distribuidos de acuerdo con la matriz de Roles y responsabilidades definida por la Entidad.

Para atender las solicitudes de soporte de los usuarios cuenta con varios niveles de Soporte Técnico que le ayudarán a resolver los problemas o tomar decisiones certeras de uso relacionadas con los equipos e infraestructura de cómputo, los niveles establecidos son:

- **Soporte Técnico Nivel 1**: (*El soporte de primer nivel podrá ser desempeñado por un funcionario de planta o quien la entidad designe para el desarrollo de estas actividades*) Es el primer punto de contacto con el usuario, levantamiento del requerimiento o incidencia y determinación del problema. Consiste en atención en primera instancia siendo el objetivo de este grupo manejar entre el 70%-80% del de los problemas del usuario antes de concluir en la necesidad de escalar la incidencia a un nivel superior.

- **Soporte Técnico Nivel 2**:(*El soporte de nivel dos en la entidad, será desempeñado exclusivamente por un funcionario de planta, el cual dispondrá del conocimiento necesario para esta actividad*), En caso de ser necesario la atención más especializada se canalizada a nuestro pool de soporte especializado, donde será atendido por un especialista con más experiencia en el tema.

- **Soporte Técnico Nivel 3**: En caso de que el problema no pueda ser resuelto por el pool de nivel 2, Una vez analizado el caso y según se requiera, se debe proceder con el escalamiento al proveedor para dar solución a la solicitud.

14. POLÍTICA DE ELIMINACIÓN O DESTRUCCIÓN DE INFORMACIÓN

Está prohibida la eliminación y destrucción indiscriminada de información propia, esta actividad se deberá realizar teniendo en cuenta el Estándar para la Eliminación o Destrucción de Información. La información propia que corresponde específicamente a información contable, informes de gestión, propuestas, contratos, información de personal, informes de seguridad, o información de proyectos especiales, sólo se podrá eliminar o destruir con autorización por escrito del jefe del área, previa validación por el dueño del proceso y que no vaya en contravía de la normatividad vigente.

15. POLÍTICA DE DESARROLLO DE SOFTWARE

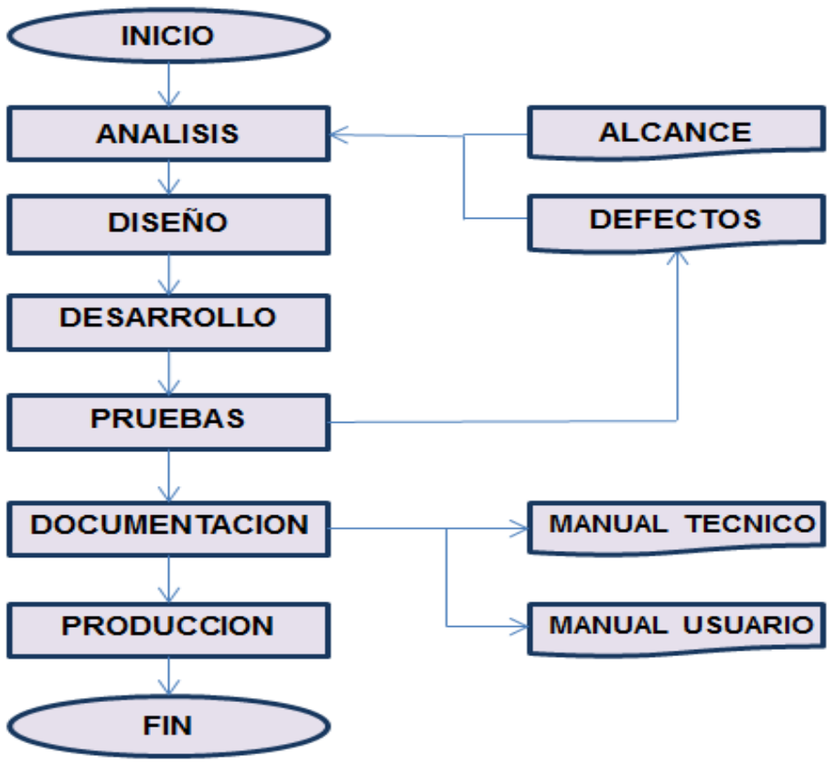
El ciclo de vida del software considera dentro de sus aspectos fundamentales lineamientos de seguridad de la información, aplicables tanto para software desarrollado por proveedores como el desarrollado internamente.

Dichos lineamientos incluyen requisitos y estándares en el desarrollo de software, incluyendo los siguientes aspectos:

- Conocimientos y entrenamiento
- Modelamiento de amenazas
- Requisitos técnicos de seguridad: autenticación, autorización, validaciones, auditoría, etc.
- Arquitectura de seguridad
- Pruebas y revisiones de seguridad
- Seguridad en el ambiente
- Control de cambio y liberación
- Roles y responsabilidades

15.1 Ciclo de Desarrollo de Software

Cada fase es asignada a uno de los estados del ciclo básico de desarrollo como los muestra la figura a continuación:



a. Análisis

La etapa de análisis está a cargo de los miembros del equipo de desarrollo o persona (funcionario o contratista), responsable por recolectar la información de las fuentes: alcance del desarrollo, errores reportados por los usuarios o identificados por el proceso de Gestión de Incidentes Respecto a los Servicios TIC. El cambio a la etapa de diseño se hace cuando a partir de cada requerimiento del usuario o cliente se tenga uno o varios casos de uso o su respectivo ajuste.

b. Diseño

El estado diseño indica las funcionalidades que se encuentran especificadas en su respectivo caso de uso. Cuando exista un diseño que contemple la implementación del caso de uso, el equipo de desarrollo puede avanzar a la etapa de desarrollo.

c. Desarrollo o Adaptación

Durante la etapa de desarrollo se hace la implementación del diseño establecido en los estados anteriores. En desarrollo o adaptación pueden estar funcionalidades que vienen de la etapa de diseño o que fueron devueltas de la etapa de pruebas.

d. Pruebas

La etapa de pruebas se le aplica a las funcionalidades que están listas para ser aprobadas por el equipo o persona (funcionario o contratista) encargado del aseguramiento de su calidad y que se encuentran desplegadas en un ambiente de pruebas, como por ejemplo el personal encargado de realizar las pruebas para verificar que el desarrollo cumpla con las necesidades establecidas en los requerimientos. En caso de que el resultado de las pruebas no sea satisfactorio, debe

ser devuelta a la etapa de desarrollo junto con la explicación de porqué no paso la prueba.

e. Documentación:

Una vez culminada la etapa de pruebas, se elaborará por parte del equipo o persona (funcionario o contratista) encargada del desarrollo la documentación técnica del nuevo aplicativo o adaptación; igualmente, debe elaborar el manual del usuario final que le permita entender el manejo del sistema.

f. Producción

La etapa de producción permite establecer que una funcionalidad se encuentra en ambiente de producción. Si la funcionalidad no muestra errores en el ambiente de producción equivale a una aceptación por parte de la persona (funcionario) encargada de la supervisión del proyecto. Si la funcionalidad muestra algún tipo de error, es devuelta a la fase de desarrollo junto con su respectiva explicación de las incidencias que presenta.

g. Plan de Capacitación

Se realizarán capacitaciones a los administradores del sistema desarrollado y a los usuarios finales encargados de recibir y cargar contenidos al sistema. Al final de todas las sesiones de capacitación, cuando sea dirigida a personal de la SuperVigilancia, se realizarán pruebas sobre los conocimientos adquiridos en las capacitaciones, se considerará exitosa la capacitación cuando se logre una calificación promedio superior a 3.5 sobre 5.

Dentro de la metodología de capacitación se dará especial atención al logro de objetivos en las siguientes tres vertientes:

- Asimilación de Conocimientos ---------- TEORÍA.
- Adquisición de Habilidades ---------- PRÁCTICA.
- Cambio de Actitudes ---------- COMPORTAMIENTOS Y CULTURA ORGANIZACIONAL.

15.3 Separación de ambientes de desarrollo

- La SuperVigilancia proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.
- Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
- No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.
- El ambiente de prueba debe emular el ambiente de producción lo más estrechamente posible.
- No se permite la copia de información sensible desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe

ser previamente ofuscada y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y se elimine de forma segura después de su uso.

- Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

15.2 Control de Versiones Desarrollo de Software

- Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma. Así, el número de versión se irá incrementando en cada cambio que se genere sobre la misma aplicación, de acuerdo con el procedimiento Manual Política de paso a Producción de Sistemas de Información y Control de Versiones.

- El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.

- Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.

- Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

15.3 Derechos de Propiedad Intelectual

- La SuperVigilancia cumplirá con la reglamentación de propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

- No se permite el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

- Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

- Los procesos de adquisición de aplicaciones y paquetes de software deben cumplir con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

- El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios directos o contratistas, serán de uso exclusivo y la propiedad intelectual será de la SuperVigilancia.

16. POLÍTICAS DE SEGURIDAD FÍSICA

16.1 Seguridad física y ambiental

- Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por los respectivos dueños de los procesos, a fin de permitir el acceso solo a personal autorizado.

- Para la selección de las áreas protegidas y la ubicación del Centro de Datos se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.

- Las plataformas tecnológicas serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

- El cableado de energía eléctrica y comunicaciones que transportan datos o brindan apoyo a los servicios de información estarán protegidos contra intercepción o daños.

- Se deberá garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

  - Sistema Eléctrico suplementario

  - Sistema de Control de Acceso

  - Sistema de protección contra incendios

16.2 Administración y Control de acceso al Datacenter

Para el cuidado y protección de la información que reside en el datacenter, se ha definido lo siguiente:

- Los funcionarios y contratistas deben contar con una tarjeta de proximidad para el ingreso al Centro Empresarial Sarmiento Angulo, Torre 4, Piso 3, donde se encuentran las instalaciones de la SuperVigilancia. Las tarjetas de proximidad las controla el área de Recursos Físicos de la Entidad, teniendo en cuenta el número de funcionarios vinculados y la caducidad de las actividades de los contratistas.

- En el tercer piso se encuentra la recepción de la SuperVigilancia, donde los funcionarios registran su ingreso con por medio de su huella dactilar.

- En la recepción se encuentran dos vigilantes de la empresa de seguridad privada, encargados del control del acceso de las personas a la SuperVigilancia.

- Todas las puertas de acceso deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y contratistas evitar que las puertas se dejen abiertas.

- Las personas que tengan acceso al Datacenter serán definidas única y exclusivamente por la Oficina de Informática y Sistemas.

- Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por la SuperVigilancia mientras permanezca dentro de sus instalaciones.
- Los visitantes se deben registrar en la recepción y deberán permanecer acompañados de un funcionario cuando se encuentren dentro de las instalaciones de la SuperVigilancia.

- Es responsabilidad de todos los funcionarios y contratistas borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y garantizar que no queden documentos o notas escritas sobre las mesas.

- Es responsabilidad de todos los funcionarios y contratistas acatar las normas de seguridad y mecanismos de control de acceso de la SuperVigilancia.

17. POLÍTICAS DE ACCESO A LA RED

17.1 Gestión de Terceros

- En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica y que deban desarrollarse dentro de las instalaciones de la SuperVigilancia, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar para el acceso a información sensible.

- En ningún caso se otorgará acceso a terceros a la información sensible, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

- Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

  - Forma en los que se cumplirán los requisitos legales aplicables

  - Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad

  - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.

  - Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.

  - Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

  - Niveles de seguridad física que se asignará al equipamiento tercerizado.

  - Derecho a la auditoría por parte de la SuperVigilancia.

18. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, busca proteger los procesos críticos contra fallas mayores en los sistemas de información o contra desastres y debe garantizar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una eventual contingencia.

Prevenir interrupciones en las actividades de la plataforma informática de la SuperVigilancia que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de la SuperVigilancia podrán ser restaurados dentro de escalas de tiempo razonables.

La SuperVigilancia deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de la SuperVigilancia de acuerdo con su impacto en el cumplimiento de la misión de la entidad.

- Documentación de la estrategia de continuidad del negocio.

- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.

- Plan de pruebas de la estrategia de continuidad del negocio.

La continuidad del negocio deberá ser gestionada por la Dirección de la SuperVigilancia, que será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La oficina de Informática y Sistemas se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de estas.

CAPITULO III ANEXOS

1. ACUERDOS DE CONFIDENCIALIDAD

Todos los funcionarios, contratistas y demás terceros deben firmar la cláusula y/o acuerdo de confidencialidad y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada, de acuerdo con el formato de confidencialidad. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

2. CONCIENCIACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- La SuperVigilancia debe mantener un programa anual de concientización y capacitación para todos los funcionarios y contratistas que interactúen con la información institucional y desarrollen actividades en sus instalaciones. Esto con el fin de proteger la información y la infraestructura tecnológica que la soporta.

- Todos los funcionarios y contratistas al servicio de la SuperVigilancia deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.

3. SANCIONES PREVISTAS POR INCUMPLIMIENTO

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente política de seguridad, conforme a lo dispuesto por las normas estatutarias escalafonarias y convencionales que rigen al personal del Sector Defensa y en caso de corresponder, se realizarán las acciones correspondientes ante el o los organismos pertinentes.

Las sanciones solo pueden imponerse mediante un acto administrativo que así lo disponga, cumpliendo las formalidades impuestas por los preceptos constitucionales, la ley de procedimientos administrativos y demás normativas específicas aplicables.

Además de las sanciones disciplinarias o administrativas, la persona que no da debido cumplimiento a sus obligaciones puede incurrir también en responsabilidad civil o patrimonial, cuando ocasiona un daño que debe ser indemnizado y/o en responsabilidad penal cuando su conducta constituye un comportamiento considerado delito por el código penal y leyes especiales.

4. DECLARACIÓN DE APLICABILIDAD

En la declaración de aplicabilidad se mencionan los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información y realizar el análisis de riesgos, igualmente se incluyen los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y, por ende, en las definiciones dadas en el plan de tratamiento del riesgo.

Lo controles se han basado en los definidos en el anexo A de la norma ISO/IEC 27001:2013.

La declaración de aplicabilidad debe ser documentada y actualizada cuando cambian las condiciones de la SuperVigilancia, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros.

5. DOCUMENTOS DE APOYO AL SGSI

Para desarrollar las políticas mencionadas en el presente documento se deben generar estándares, guías y procedimientos necesarios para facilitar el cumplimiento de lo emanado en el SGSI de la Supervigilancia, a partir de la aprobación del presente manual y ajustadas a los cambios normativos que así lo requieran.

6. RESPONSABLE DEL DOCUMENTO

El presente documento debe ser actualizado o modificado por el Jefe de Área de Informática y Sistemas en conjunto con el Oficial de Seguridad de la Información.

[i] **Keepas:** Es una herramienta libre para sistemas Windows que permite almacenar de forma segura y cifrada todas las contraseñas de nuestros servicios protegidas bajo una contraseña maestra.

Superintendencia de Vigilancia y Seguridad Privada
Centro de Información al Ciudadano: Calle 24ª No. 59 – 42 Torre 4 Piso 3
Sede Administrativa: Avenida Calle 26 # 57-41 Torre 8 - Piso 11
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co