MANUAL DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

INTRODUCCION

Este documento describe la Política de Seguridad de la Información de la Superintendencia de Vigilancia y Seguridad Privada. Para su elaboración, se toman como base los controles y requisitos identificados en el estándar ISO/IEC 27001, 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 políticas incluidas en este manual se constituyen como parte fundamental del Modelo de Gestión de Seguridad de la Información de la Entidad y se convierten en la base para la implantación de los controles, procedimientos y estándares. La Seguridad de la Información es una prioridad para la Superintendencia de Vigilancia y Seguridad Privada y por tanto es responsabilidad de todos los funcionarios velar por el continuo cumplimiento de las políticas definidas en el presente documento.

1 OBJETIVOS Y ALCANCE

1.1 Objetivo General

Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios directos, temporales, contratistas, practicantes, terceros o cualquier persona que tenga una relación contractual con la SuperVigilancia, o que tenga acceso a los activos de información, con el propósito de preservar la Confidencialidad, Integridad y Disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas de la Entidad, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información. Para tal efecto, se obrará en concordancia con las disposicion es legales vigentes.

1.2 Objetivos Específicos

- Proteger los recursos de información y tecnología frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles efectivos.

- Establecer un modelo organizacional de Seguridad de la Información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la política.

- Promover, mantener y realizar mejoramiento continuo del nivel de cultura en Seguridad de la Información, así como lograr la concientización de todos los funcionarios y contratistas y demás personas que interactúen con la SuperVigilancia, para minimizar la ocurrencia de incidentes de Seguridad de la Información.

- Mantener la política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y eficacia.

1.3 Alcance

El presente documento define la política, controles y directrices para el sistema de gestión de Seguridad de la Información de la SuperVigilancia. La política establecida y sus posteriores actualizaciones aplican a todos los recursos y activos de información de la Entidad, así como a los designados para su uso y custodia.

2 MARCO DE REFERENCIA

2.1 Antecedentes

Teniendo en cuenta que la información es un activo vital para el éxito y el cumplimiento de la misión de la SuperVigilancia, este documento se encuentra alineado con la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su sistema de gestión de Seguridad de la Información.

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001 sobre los requisitos para el establecimiento del sistema de gestión de Seguridad de la Información.

La información, así como 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 de la Entidad. 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 adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

Hoy por hoy, las organizaciones tanto públicas como privadas se están tornando altamente dependientes de sus sistemas de información y de los recursos informáticos que los soportan, por lo que se convierte en una decisión estratégica el implementar un Sistema de Gestión de Seguridad de la Información que esté directamente relacionado con las necesidades, objetivos institucionales y direccionamiento estratégico.

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.

2.2 Referencias Normativas

- 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 "Protección de la Información y de los Datos".
- Documento 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.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- 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.
- Norma Técnica Colombiana NTC – ISO/IEC 27000

3 MISIONES GENERALES Y PARTICULARES

3.1 Misión General Ministerio de Defensa

El Ministro de Defensa Nacional emite la directiva Permanente N°. DIR2014-18 con el fin de Estandarizar las Políticas de Seguridad de la Información para todas las dependencias y entidades que conforman el Sector Defensa, las cuales se dictan en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la Seguridad de la Información, los sistemas informáticos y los ambientes tecnológicos. Estas políticas, deberán ser conocidas, difundidas y cumplidas por todo el personal que tenga relación con activos de información de la Superintendencia de Vigilancia y Seguridad Privada.

3.2 Misiones Particulares

3.2.1 Despacho Superintendencia de Vigilancia y Seguridad Privada

- Verificar el cumplimiento de la presente Directiva, 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 a través de 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 de las áreas de tecnología 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.

3.2.2 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 usuarios; así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software base y de aplicaciones.
- Gestionar la adquisición de software y hardware.
- Asignar los equipos de cómputo a los funcionarios y/o contratistas.
- A través de las áreas de Seguridad de la Información se debe:

  i. Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
  ii. Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
  iii. 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.

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

iv. Gestionar los incidentes de Seguridad de la Información que se presenten en la organización.

3.2.3 Oficina de Recursos Humanos[1]

Incluir en los programas de inducción y de re-inducción el tema de 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.

3.2.4 Oficina de Control Interno

Validar 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 de l Sistema de Gestión de Seguridad de la Información.

3.2.5 Dueños de los procesos

Definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

3.2.6 Propietarios de los Activos de Información

- Los funcionarios y contratistas son responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en la SuperVigilancia, para lo cual deben alimentar los datos que son editables en forma íntegra y veraz.
- 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.
- 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.

[1] ISO/IEC 27001 Anexo A, Item 8.1.2

3.2.7 Funcionarios, contratistas y terceros

- Cumplir con las políticas de Seguridad de la Información, contempladas en la presente Directiva.
- Velar por el cumplimiento de las políticas de Seguridad de la Información dentro de su entorno laboral inmediato.
- Reportar de manera inmediata y a través de los canales establecidos, la sospecha u ocurrencia de eventos considerados incidentes de Seguridad de la Información.
- Utilizar los sistemas de información y el acceso a la red únicamente para los propósitos que lo vinculan.
- Utilizar únicamente software y demás recursos tecnológicos autorizados.

4 ACCIONES QUE AFECTAN LA SEGURIDAD DE LA INFORMACIÓN

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

i. Dejar los computadores encendidos en horas no laborables.

ii. Permitir que personas ajenas a la SuperVigilancia ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.

iii. No clasificar y/o etiquetar la información.

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

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

vi. Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.

vii. 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.

viii. 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.

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

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

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

xii. Ingresar a la red de datos de Entidad por cualquier servicio de acceso remoto sin la autorización de la Oficina de Informática y Sistemas.

xiii. Usar servicios de internet en los equipos de la Entidad, diferente al provisto por la Oficina de Informática y Sistemas.

xiv. Promoción o mantenimiento de actividades personales, o utilización de los recursos tecnológicos de la SuperVigilancia para beneficio personal.

xv. 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.

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

xvii. 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.

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

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

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

xxi. Realizar cambios no autorizados en la Plataforma Tecnológica de la Entidad.

xxii. Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

xxiii. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de Seguridad de la Información.

xxiv. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.

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

xxvi. 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 a los procedimientos establecidos para cada caso.

5 POLITICAS GENERALES

5.1 Documentación de procedimientos operativos[2]

a. 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.

b. 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.

c. 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.

d. 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.

5.2 Control de Cambios Operativos[3]

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la

[2] ISO/IEC 27001 Anexo A, Item 10.1
[3] ISO/IEC 27001 Anexo A, Item 10.1.2

Oficina de Informática y Sistemas de la Entidad, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

b. 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.

5.3 Control de Versiones[4]

a. 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*.

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

c. 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.

d. 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.

5.4 Concientización y Capacitación en Seguridad de la Información[5]

a. 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.

b. Todos los funcionarios y contratistas al servicio de la Entidad 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.

[4] ISO/IEC 27001 Anexo A, Items 12.4.3 y 12.5.1
[5] ISO/IEC 27001 Anexo A, Item 8.2.2

5.5 Finalización de la Relación Laboral[6]

Al momento de la desvinculación o cambio de roles en la Entidad, todo funcionario o contratista debe hacer entrega de todos los activos de información que le hayan sido asignados.

5.6 Gestión de Incidentes de Seguridad de la Información[7]

a. Los funcionarios y contratistas de la Entidad 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.

b. 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.

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

d. 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.

e. 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.

f. 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.

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

h. La Entidad 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.

[6] ISO/IEC 27001 Anexo A, Item 8.3
[7] ISO/IEC 27001 Anexo A, Items 13.1 y 13.2

5.7 Seguridad de la Información en la Continuidad del Negocio[8]

a. La Seguridad de la Información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.

b. La Entidad deberá contar con un Plan de Recuperación ante Desastres (DRP) que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.

c. Para el Sector Defensa su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.

d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Recuperación ante Desastres.

e. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Recuperación ante Desastres.

5.8 Derechos de Propiedad Intelectual[9]

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

b. No se permitirá 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.

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

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

e. El desarrollo de software a la medida adquirido a terceras partes o realizados por funcionarios de la Entidad, serán de uso exclusivo de la SuperVigilancia y la propiedad intelectual será de quien lo desarrolle.

[8] ISO/IEC 27001 Anexo A, Item 14.1
[9] ISO/IEC 27001 Anexo A, Item 15.1.2

5.9 Sanciones Previstas por Incumplimiento[10]

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.

6 POLIÍTICAS DE SEGURIDAD FÍSICA

6.1 Seguridad física y ambiental[11]

a. Las áreas protegidas y el Centro de Datos se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Oficina de Informática y Sistemas, a fin de permitir el acceso solo a personal autorizado.

b. 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.

c. 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.

d. El cableado de datos que se incluya en cualquier proyecto en las instalaciones de la Entidad debe ser categoría 7A.

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

[10] ISO/IEC 27001 Anexo A, Item 15.1
[11] ISO/IEC 27001 Anexo A, Item 9

f. 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

6.2 Administración y Control de usuarios al Datacenter[12]

La seguridad física es importante para el cuidado y protección de la información, por esto se han definido las siguientes reglas:

a. 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 a la SuperVigilancia y la caducidad de las actividades de los contratistas.

b. En el tercer piso se encuentra la recepción de la Entidad, 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 Entidad.

c. Todas las puertas que utilicen sistema de control 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.

d. 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 permanezcan dentro de sus instalaciones.

e. Los visitantes se deben registrar en la recepción y deberán permanecer acompañados de un funcionario cuando se encuentren dentro de las instalaciones de la Entidad.

f. 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.

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

[12] ISO/IEC 27001 Anexo A, Item 9.1

6.3 Trabajo en Áreas Protegidas[13]

a. 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.

b. 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.

6.4 Seguridad y Mantenimiento de los Equipos[14]

a. 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.

b. La Entidad 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.

c. 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.

[13] ISO/IEC 27001 Anexo A, Item 9.1.5
[14] ISO/IEC 27001 Anexo A, Item 9.2

d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, 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.

e. Los equipos portátiles deberán estar asegurados con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la Entidad.

f. La Entidades 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.

6.5 Seguridad de los Equipos Fuera de las Instalaciones[15]

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

b. 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.

c. 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.

6.6 Gestión de Medios Removibles[16]

a. 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.

b. 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.

[15] ISO/IEC 27001 Anexo A, Item 9.2.5
[16] ISO/IEC 27001 Anexo A, Item 10.7.1

c. La Entidad 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.

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

e. 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.

f. El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

7 POLÍTICAS DE ACCESO A LA RED

7.1 Gestión de Terceros[17]

a. 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.

b. 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.

c. 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

[17] ISO/IEC 27001 Anexo A, Item 6.2.2

- 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

7.2 Acuerdos de Confidencialidad[18]

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 al 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.

7.3 Computación Móvil[19]

a. 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.

b. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser autorizada por la Oficina de Informática y Sistemas, previa verificación de que cuenten con las condiciones de seguridad y estableciendo mecanismos de control necesarios para proteger la infraestructura de la Entidad.

7.4 Control de Acceso[20]

a. El Data Center 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.

[18] ISO/IEC 27001 Anexo A, Item 6.1
[19] ISO/IEC 27001 Anexo A, Item 11.7
[20] ISO/IEC 27001 Anexo A, Item A.11

b. 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.

c. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la Entidad deberá estar autorizado por la respectiva Oficina de Informática y Sistemas.

d. Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.

e. 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.

f. La asignación de privilegios en las aplicaciones para los diferentes identificadores de usuario estarán determinados 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.

g. Los equipos de contratistas y demás terceros que requieran acceder a la redes de datos de la Entidad deben cumplir un procedimiento de sanitización[21] informática antes de concedérseles dicho acceso.

h. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder de forma permanente a la red de la Entidad, sólo podrán hacerlo una vez se haya cumplido con el procedimiento inicial de formateo de discos duros y/o medios de almacenamiento, y posteriormente deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido.

i. 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.

7.5 Administración de Contraseñas[22]

[21] Sanitización en manejo de información confidencial o sensible es el proceso lógico y/o físico mediante el cual se remueve información considerada sensible o confidencial de un medio ya sea físico o magnético, ya sea con el objeto de desclarificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.
[22] ISO/IEC 27001 Anexo A, Item 11.2

Superintendencia de Vigilancia y Seguridad Privada
Calle 24ª No. 59 – 42 Torre 4 Piso 3 Centro Empresarial Sarmiento Angulo
PBX: (571) 3078038 Línea Gratuita Nacional: 01 8000 119703
www.supervigilancia.gov.co

a. La administración así como la entrega de las contraseñas a los usuarios deberá realizarse por la Oficina de Informática y Sistemas.

b. 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:

   i. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
   ii. Las contraseñas no deberán ser reveladas.
   iii. 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.
   iv. Los funcionarios y contratistas deben digitar siempre su usuario y contraseña para acceder a las diferentes aplicaciones de la Entidad; la contraseña no se deben guardar de forma automática en los inicios de sesión de las aplicaciones (Correo Electrónico, Orfeo, SIMA, etc); igualmente al terminar la jornada deben cerrar las sesiones abiertas antes de apagar el equipo.
   v. 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.

8 POLÍTICAS DE SEGURIDAD LÓGICA

8.1 Gestión de Activos de Información[23]

a. 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.

b. La Entidad 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.

c. La Entidad 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.

[23] ISO/IEC 27001 Anexo A, Items 7.1.1 y 7.1.2

d. Debe realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confiedencialidad, integridad y disponibilidad.

e. La Entidad deberá definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación definido.

8.2 Uso Adecuado de los Activos de Información[24]

La información, los sistemas, las aplicaciones, los servicios y los equipos (equipos de escritorio, portátiles, impresoras, redes, Internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) de todas y cada una de las dependencias y entidades del Sector Defensa, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus respectivas actividades laborales. La SuperVigilancia se reservan el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en la presente política, en el manual MAN-GIS - 7300-006: Manual de Políticas para el Buen uso de Internet, Correo Electrónico y Chat Institucional, así como en la legislación vigente.

8.2.1 Uso de Internet

Internet es una herramienta de trabajo que permite navegar en sitios relacionados o no con las actividades diarias, por lo cual el uso adecuado de este recurso se controla, verifica y monitorea, considerando para todos los casos, las siguientes políticas:

a. La navegación en Internet estará controlada de acuerdo con las restricciones de navegación definidas para los usuarios; sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

- 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.

- Publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere fuera de los límites permitidos.

- 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.

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

[24] ISO/IEC 27001 Anexo A, Item 7.1.3

- 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.

- Promover o mantener asuntos o negocios personales.

- Descarga, instalación yutilización 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.

- Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Entidad.

- Uso de herramientas de mensajería instantánea no autorizadas por la Oficina de Informática y Sistemas.

- Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

b. 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.

c. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

8.2.2 Uso del 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 para el desempeño de sus funciones, así como a contratistas y otros terceros previa autorización; su uso se encuentra sujeto a las siguientes reglas:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas en la SuperVigilancia.

b. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Entidad 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 la misma se considera de interés de las Entidades del Sector Defensa.

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

d. 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 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.

e. 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.

f. 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.

g. 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.

8.2.3 Uso de Redes Inalámbricas

a. 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.

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

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

8.2.4 Uso de Computación en la Nube

a. Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos.

b. Ningún servicio de carácter misional, operativo o institucional de la SuperVigilancia deberá ser contratado en Servicios en la Nube públicos o híbridos.

c. 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.

8.2.5 Sistemas de Acceso Público

a. La información pública producida por las dependencias de la Entidad deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

b. El portal institucional deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.

c. La Entidad deberá garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la Seguridad de la

Información ingresada a través de ellos, aclarando que no se es responsable de la veracidad de la misma.

d. Toda la información publicada en el portal institucional o cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina de Comunicaciones.

8.2.6 Uso de recursos tecnológicos

La asignación de los diferentes recursos tecnológicos se da como herramientas de trabajo para uso exclusivo de los funcionarios y contratistas. El uso adecuado de estos recursos se encuentra sujeto a las siguientes reglas:

a. 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.

b. 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.

c. 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.

d. Los equipos de cómputo deberán ser bloqueados, por los usuarios que los tienen a cargo, cada vez que se retiren del puesto de trabajo.

e. Los requerimientos de recursos tecnológicos de las diferentes áreas deben ser avalados por la Oficina de Informática y Sistemas.

f. 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.

g. 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.

h. De acuerdo con el literal anterior, la Entidad no debe almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

8.3 Segregación de Funciones[25]

a. Todas las personas que tengan acceso a la infraestructura tecnológica o a los sistemas de información, 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.

b. 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 Entidad.

8.4 Separación de ambientes[26]

a. 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.

b. 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.

c. 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.

d. El ambiente de prueba debe emular el ambiente de producción lo más estrechamente posible.

e. 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.

f. 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.

[25] ISO/IEC 27001 Anexo A, Item 10.1.3
[26] ISO/IEC 27001 Anexo A, Item 10.1.4

8.5 Protección contra Software Malicioso[27]

a. 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 posibles fallos dados por código malicioso.

b. 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.

c. 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.

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

e. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por la Oficina de Informática y Sistemas.

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

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

8.6 Administración de Backups, Recuperación y Restauración de la información[28]

a. Todas las copias de respaldo de la Entidad deben ser incrementales. El backup 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 un backup 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 un backup incremental es que copia una

[27] ISO/IEC 27001 Anexo A, Item 10.4
[28] ISO/IEC 27001 Anexo A, Item 10.5.1

menor cantidad de datos que un backup completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio de almacenamiento.

b. 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 Entidad, 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. Es por esto que las aplicaciones alojadas en los servidores del centro de cómputo de la SuperVigilancia se les realizarán copias de respaldo automáticas todos los días a las 8 pm. Estas aplicaciones son SIMA, Ares, ORFEO, INFODOC, Suite Vision Empresarial, Humano. Las aplicaciones PQR, Reporte Información Financiera y Portal Web se encuentran alojadas en los servidores de la empresa Micrositios, con sus respectivas cláusulas de copias de seguridad y restauración. Finalmente, para las aplicaciones RENOVA, APO y Sanciones, la Oficina de Informática y Sistemas realiza diariamente las copias de seguridad.

c. 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.

d. 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.

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

f. 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 la misma.

g. 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.

8.7 Gestión de Registros (logs)[29]

[29] ISO/IEC 27001 Anexo A, Item 10.10

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

b. 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.

c. Todo aquel 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.

8.8 Gestión de Vulnerabilidades Técnicas[30]

a. La Oficina de Informática y Sistemas de la Entidad se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

b. La Oficina de Informática y Sistemas será responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la Entidad.

c. 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 los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

d. 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.

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

f. 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.

[30] ISO/IEC 27001 Anexo A, Item 12.6

g. La Oficina de Informática y Sistemas de la Entidad 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.

9 POLÍTICAS DE EQUIPOS CLIENTE

9.1 Bloqueo de Sesión, Escritorio y Pantalla Limpia[31]

a. 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.

b. 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.

c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la Entidad, 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.

d. Los usuarios deberán retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

e. No se deberá reutilizar papel que contenga información sensible.

f. 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.

g. 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.

10 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad menciona los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información y realizar el análisis de riesgos, así como 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.

[31] ISO/IEC 27001 Anexo A, Items 11.3.2 y 11.3.3

Estos controles están basados en los controles definidos en la norma ISO/IEC 27001.

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

11 Política de Roles

Para los procesos del manejo de activos de la información de la entidad se deben cumplir con los roles que se generan para las personas involucradas en el tratamiento de la información y los sistemas de información; se han constituido con el fin del tratamiento de la información y justos resultados.

Los roles son:

1. Propietario Legal

La superintendencia de Vigilancia y seguridad Privada debe ser propietario legal de los activos de información. Ningún individuo puede reclamar los derechos de propiedad intelectual de un activo de información, a menos que se acuerde y apruebe por la Administración de acuerdo contractual.

2. Delegado de Propiedad

El Superintendente tendrá autoridad para representar a la organización para la protección y la seguridad de la información de activos como la propiedad de los activos de información, se delega esta función organizativa.

El CEO aprobará la gestión de la información / Seguridad Política.

El Superintendente podrá delegar la propiedad total / parcial junto con las responsabilidades definidas a cualquier funcionario / contratista / tercero con derechos de explotación y responsabilidad.

Las Responsabilidades del propietario de activos son los siguientes:

- Actualización de la información de registro de inventario de activos ;
- Identificar el nivel de clasificación de los activos de información;
- Definición e implementación de las salvaguardas apropiadas para asegurar la confidencialidad, integridad y disponibilidad de la información de activos;
- Evaluación y seguimiento de medidas de seguridad para garantizar su cumplimiento y reporte de situaciones de incumplimiento;
- Autorizar el acceso a aquellos que tienen una necesidad comercial de la información , y Asegurar el acceso es

3. Lider de Información (Chief Information Officer)

El CIO es quien asegura que los procesos de planificación estratégica se lleven a cabo, de manera que se cumplan los requisitos de información y sistemas de apoyo e infraestructura; Además sean alineados con los requisitos legislativos y los objetivos estratégicos. El CIO asegura la información.

- Es el líder para las políticas de seguridad y prácticas de gobierno para garantizar la calidad y la integridad de los recursos de información del organismo y el apoyo a los sistemas de TI.
- Supervisa el desarrollo de instrumentos, sistemas y la infraestructura de tecnología de la información para maximizar el acceso y uso de los recursos de información de una agencia.

El CIO es responsable de:

- Interpretar las necesidades de utilidad y de información, y los deseos de la organización y su traducción a las iniciativas de TIC.
- Establece la Estrategia de la tecnología de la información y las comunicaciones y la gestión de la información.
- Busca que las TIC y la gestión de información de la inversión está alineada a los objetivos estratégicos de la organización.
- Procura que los proyectos y las iniciativas están alineados y coordinados para ofrecer el mejor servicio.
- Garantiza que la planificación de las TIC está integrada en la planificación de negocios.
- Identificar las oportunidades para el intercambio de información y la colaboración en proyectos e iniciativas.

4. Gestor de Información

- Proporciona asesoramiento especializado en relación con las prácticas de gestión de la información.
- Contribuye a la dirección estratégica de la gestión de la información dentro de la Organización.
- Coordinar el desarrollo y la aplicación de gestión de la información.
- Genera Prácticas en las políticas, normas, directrices y procedimientos.
- Ayuda a las unidades de negocio para definir y comprender sus responsabilidades en relación con gestión de la información.
- Ayuda a las unidades de negocio para identificar sus necesidades y requisitos de información.
- Trabaja con el CIO para planificar e implementar los sistemas de administrar eficazmente los activos de información de la Superintendencia de Vigilancia y seguridad Privada.

5. Oficial de Seguridad de la información

El oficial de seguridad de la información es responsable de desarrollar e implementar la política de seguridad de la información diseñado para proteger la información y el apoyo a cualquier sistema de información de cualquier acceso no autorizado, uso, divulgación, corrupción o destrucción.

El oficial de seguridad de la información deberá:

- Desarrollar políticas, procedimientos y normas para garantizar la seguridad, confidencialidad y la privacidad de la información que sea consistente con la información de la organización política de seguridad.
- supervisar e informar sobre cualquier incidente de información por intrusión y activar las estrategias para evitar nuevos incidentes.
- Trabajar con custodios de información para asegurar que los activos de información han sido asignadas clasificaciones de seguridad apropiadas.
- Mantenimiento y conservación del activo como se define por el propietario de los activos de reinicio y recuperación del sistema.
- La implementación de cualquier cambio de acuerdo con el procedimiento de gestión de cambios de copia de seguridad de la información.
- Actualización de la información de registro de inventario de activos;
- Identificar el nivel de clasificación de los activos de información;
- Definición e implementación de las salvaguardas apropiadas para asegurar la confidencialidad, integridad y disponibilidad de la información de activos;
- Evaluación y seguimiento de medidas de seguridad para garantizar su cumplimiento y reporte situaciones de incumplimiento;
- autorizar el acceso a aquellos que tienen una necesidad comercial de la información, y Asegurar el acceso.
- Se retira de los que ya no tienen una necesidad comercial de la información.

6. Responsables de la información.

Los empleados, terceros, Contratistas autorizado por el propietario / encargado de Acceso.
Cumple con las garantías establecidas por el propietario / encargado La información y el uso de.
Siendo el acceso a la información otorgada no implica ni confiere autoridad para conceder a otros usuarios el acceso a esa información.
Los usuarios están obligados por la política de uso aceptable de la organización.

7. Usuarios externos:
Los empleados, terceros, Contratistas autorizado por el propietario / encargado de Acceso Y/o usuarios externos que hagan uso de la información sin que puedan modificarla, tratarla o borrar la información.