MinDefensa
Ministerio de Defensa Nacional

PROSPERIDAD PARA TODOS

DIRECTIVA

Nº. DIR2014-18

Bogotá D.C. 19/06/2014

DIRECTIVA PERMANENTE

ASUNTO : POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR DEFENSA.

AL : COMANDANTE GENERAL DE LAS FUERZAS MILITARES, COMANDANTE DEL EJÉRCITO NACIONAL, COMANDANTE DE LA ARMADA NACIONAL, COMANDANTE DE LA FUERZA AÉREA COLOMBIANA, DIRECTOR GENERAL DE LA POLICÍA NACIONAL, VICEMINISTRO PARA LAS POLÍTICAS Y ASUNTOS INTERNACIONALES, VICEMINISTRA PARA LA ESTRATEGIA Y PLANEACIÓN, VICEMINISTRO DEL GRUPO SOCIAL Y EMPRESARIAL DEL SECTOR DEFENSA – GSED, SECRETARIA DE GABINETE DEL MINISTERIO DE DEFENSA NACIONAL, SECRETARIO GENERAL DEL MINISTERIO DE DEFENSA NACIONAL, DIRECTOR GENERAL DE SANIDAD MILITAR, DIRECTORA EJECUTIVA DE LA JUSTICIA PENAL MILITAR, DIRECTOR GENERAL MARÍTIMO, DIRECTORES EMPRESAS DEL GSED.

1. OBJETO Y ALCANCE

1.1. Objeto

Establecer y difundir los criterios y comportamientos que deben seguir todos los funcionarios y cualquier persona que tenga una relación contractual con el Sector Defensa (entiéndase terceros) 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 del Sector Defensa, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando la inversión en tecnologías de información.

1.2. Alcance

La presente directiva define la política, controles de uso aceptable y las directrices en lo relacionado con la seguridad de la información en las instituciones y entidades del Sector Defensa: Unidad de Gestión General, Dirección de Justicia Penal Militar, Dirección General Marítima, Comisión Colombiana del Océano, Comando General de las Fuerzas Militares, Ejército Nacional, Armada Nacional, Fuerza Aérea Colombiana, Policía

Nacional, Dirección General de Sanidad Militar y el Grupo Social y Empresarial de la Defensa – GSED con todas las empresas que lo conforman.

Las políticas establecidas en esta directiva, y sus posteriores actualizaciones, aplican a todos los recursos y activos de información de las instituciones y entidades que conforman el Sector Defensa, así como a los designados para su uso y custodia en el territorio nacional y fuera de él.

1.3. Referencias Normativas

a. Constitución Política de Colombia
b. Ley 80 de 1993 "Estatuto general de contratación de la administración pública".
c. Ley 87 de 1993 "Control Interno en los organismos del Estado".
d. Ley 527 de 1999 "Comercio Electrónico"
e. Ley 594 de 2000 "Ley General de Archivo"
f. Ley 599 de 2000 "Código Penal Colombiano".
g. Ley 603 de 2000 "Control de legalidad del software".
h. Ley 734 de 2002 "Código Disciplinario Único".
i. Ley 836 de 2003 "Régimen Disciplinario FF.MM".
j. Ley 1015 de 2006 "Régimen Disciplinario para la Policía Nacional".
k. Ley 1266 de 2008 "Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información".
l. Ley 1273 de 2009 "Protección de la Información y de los Datos".
m. Documento CONPES 3701 de julio del 2011 "Lineamientos de política para ciberseguridad y ciberdefensa".
n. 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.
o. Manual de Contrainteligencia FF.MM. 2-6 Reservado.
p. Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
q. 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 en la Policía Nacional de Colombia.
r. Norma Técnica Colombiana NTC – ISO/IEC 27000
s. Metodología para Análisis y Evaluación de Riesgos de la Unidad de Gestión General del Ministerio de Defensa Nacional.

Las demás normas vigentes aplicables.

1.4. Vigencia

Las disposiciones contenidas en la presente Directiva Permanente rigen a partir de la fecha de su expedición y deroga la Directiva Permanente No. 16 del 22 de mayo de 2009, Resolución 1566 del 2006, la Directiva Permanente 200-12 de 2006 y las demás normas que le sean contrarias.

2. INFORMACIÓN

2.1. Marco de Referencia

Teniendo en cuenta que la información es un activo vital para el éxito y el cumplimiento de la misión del Sector Defensa, este documento adopta la familia de normas de la serie ISO 27000, la cual proporciona 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 resaltan: ISO/IEC 27001:2005 sobre los requisitos para el establecimiento del sistema de gestión de seguridad de la información, ISO/IEC 27002:2005 - Código de práctica para la gestión de la seguridad de la información e ISO/IEC 27005:2008 relacionada con la gestión del riesgo.

2.2. Antecedentes

La información, así como la plataforma tecnológica que la soporta, son considerados activos estratégicos para el Sector Defensa, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información de las instituciones y entidades que lo conforman.

Estos activos de información se constituyen en el soporte de la misión y la visión de las instituciones y entidades del Sector, 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 instituciones 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.

2.3. Generalidades

El Ministerio de Defensa Nacional en cumplimiento de la normatividad emitida por el Gobierno Nacional, apoya y acompaña a las instituciones y entidades que conforman el Sector Defensa en la implementación de un Sistema de Gestión de Seguridad de la Información formalizado, documentado, alineado con los objetivos estratégicos del Sector Defensa, enfocado a gestionar y reducir los riesgos a un nivel aceptable, mejorando en forma continua los procesos de seguridad de la información; valiéndose de un talento humano capacitado, competente, comprometido con la seguridad de la información y el uso aceptable de los activos de información, con tecnología apropiada que satisfaga las necesidades del Sector Defensa en términos de disponibilidad, confidencialidad e integridad.

2.3.1. Objetivos de la Política de Seguridad de la Información para el Sector Defensa.

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

b. Implementar un Sistema de Gestión de Seguridad de la Información para el Sector Defensa, orientado 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 en las instituciones y entidades del sector.

c. Promover, mejorar y mantener un nivel de cultura en seguridad de la información, así como lograr la concientización de todos los funcionarios y terceros que interactúen con el Sector Defensa, para minimizar la ocurrencia de incidentes de seguridad de la información.

d. Coordinar los esfuerzos de las instituciones y entidades que conforman el Sector Defensa para proteger de forma consistente los activos de información.

e. Establecer los lineamientos para que el Plan de Continuidad de Negocio, definido en cada institución y entidad del sector, contemple de manera integral las políticas y requerimientos de seguridad de la información.

2.3.2. Análisis de Riesgos de Seguridad de la Información

Cada una de las instituciones y entidades que conforman el Sector Defensa, deberá realizar el análisis y evaluación de riesgos como base para identificar y controlar los riesgos de seguridad de la información a los cuales están expuestos los activos de información, con el objetivo de definir e implementar las opciones de tratamiento apropiadas.

Para la valoración de activos de información y sus riesgos asociados se recomienda emplear la metodología que, para este propósito, establece la norma ISO/IEC 27005. Por su parte, para ejecutar el análisis de riesgos se recomienda utilizar el esquema establecido en la norma ISO/IEC 27005. Para la identificación de opciones de tratamiento de riesgos se deberá seguir el procedimiento de identificación y tratamiento de riesgos (Anexo S).

El análisis y evaluación de riesgos deberá hacerse al menos una vez al año y cada vez que ocurran cambios significativos en la estructura orgánica de las instituciones y entidades que conforman el Sector Defensa, en sus plataformas tecnológicas o en sus procesos.

3. EJECUCIÓN

3.1. Misión General:

El Ministro de Defensa Nacional, emite la presente Directiva, con el fin de estandarizar las políticas de seguridad de la información para todas las instituciones 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, de los sistemas informáticos y de los ambientes tecnológicos. Estas políticas, deberán ser conocidas, difundidas y cumplidas por todo el personal que tenga relación con activos de información del Sector Defensa.

3.2. Misiones Particulares

3.2.1. Comandante General de las Fuerzas Militares, Comandantes de Fuerza, Director General de la Policía Nacional, Viceministros, Secretaria de Gabinete, Secretario General, Director Ejecutivo de la Justicia Penal Militar, Director General Marítimo, Director General de Sanidad Militar, Presidente de la Comisión Colombiana del Océano y directores de entidades adscritas y vinculadas que conforman el Grupo Social y Empresarial del Sector Defensa – GSED:

a. Verificar el cumplimiento de la presente Directiva.

b. Promover el desarrollo de una cultura de seguridad de la información a través de campañas de sensibilización y concientización.

c. Implementar el Sistema de Gestión de Seguridad de la Información, para posteriormente apoyarlo y soportarlo.

d. Apoyar los programas de capacitación, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con seguridad de la información.

e. 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.

f. Ordenar la inclusión, de temas relacionados con seguridad de la información, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares y Policía Nacional.

g. Apoyar la creación de los respectivos Equipos de Respuesta a Emergencias Informáticas (CSIRT) y Centros de Operaciones de Seguridad (SOC), con el propósito de apoyar a la gestión de incidentes.

3.2.2. Oficinas de Telemática, Informática, Sistemas o de Tecnología

a. Promover el cumplimiento, por parte del personal bajo su responsabilidad, de las políticas de seguridad de la información.

b. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.

c. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.

d. Incluir los controles de seguridad de la información en el diseño, desarrollo, instalación y mantenimiento de las aplicaciones bajo su responsabilidad.

e. Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.

f. Definir e implementar la estrategia de concientización y capacitación en seguridad de la información para los funcionarios y terceros, cuando aplique.

g. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.

h. Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.

i. Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas; así mismo, realizar el control y verificación de cumplimiento del licenciamiento software y aplicaciones asociadas.

j. Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.

k. Establecer, verificar, monitorear y validar los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

l. Establecer, documentar y actualizar los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.

m. Gestionar los incidentes de seguridad de la información que se presenten.

n. Realizar análisis de vulnerabilidades a la plataforma tecnológica con el fin de generar recomendaciones.

3.2.3. Unidades de Ciberseguridad y Ciberdefensa:

a. Grupo de Respuestas a Emergencias Cibernéticas de Colombia (colCERT): coordinar temas de Ciberseguridad y Ciberdefensa y la protección de la infraestructura crítica nacional.

b. Centro Cibernético Policial (CCP): desarrollar estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

c. Comando Conjunto Cibernético (CCOC): desarrollar estrategias, programas, proyectos y demás actividades requeridas para garantizar la Ciberdefensa de los activos críticos de las instituciones y entidades del Sector.

3.2.4. Oficinas de personal o de talento humano

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.

3.2.5. Oficinas o áreas de control interno

Realizar auditorias a los procesos del Sistema de Gestión de Seguridad de la Información, una vez implementado, como mínimo una vez al año.

3.2.6. Inspección General de las Fuerzas Militares - Inspector General de la Fuerza

Incluir dentro de los planes de inspección de las Unidades militares que integran el Comando General FF.MM., y cada Fuerza, revistas en los aspectos de seguridad de la información.

3.2.7. Jefatura de Inteligencia y Contrainteligencia Militar Conjunta – Jefatura de Inteligencia de la Fuerza o quien haga sus veces en las instituciones y entidades del Sector Defensa definidas en el alcance de esta Directiva.

a. Elaborar y actualizar los estudios de seguridad de personal (ESP), las promesas de reserva, las pruebas técnicas de confidencialidad y/o las tarjetas de autorización para manejo de documentación clasificada, de los funcionarios que laboran en áreas donde se maneja información sensible y/o clasificada.

b. Elaborar y actualizar los estudios de seguridad de personal (ESP) y las promesas de reserva del personal contratista y/o asesor externo que requiera interactuar con los activos de información de las instituciones y entidades que conforman Sector Defensa y de las diferentes unidades de las Fuerzas Militares.

c. Realizar monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información.

d. Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de las instituciones y entidades que conforman el Sector Defensa y de las diferentes unidades de las Fuerzas Militares.

3.2.8. Dirección de Inteligencia de la Policía Nacional

a. Elaborar y actualizar los estudios de seguridad de personal (ESP), las promesas o acuerdos de reserva, las pruebas técnicas de confidencialidad y/o las tarjetas de autorización para manejo de documentación clasificada de los funcionarios que laboran en áreas donde se maneja información sensible y/o clasificada.

b. Elaborar y actualizar los estudios de seguridad de personal (ESP) y las promesas o acuerdos de reserva, del personal contratista y/o asesor externo que requiera interactuar con los activos de información de las Unidades que integran la Policía Nacional.

3.2.9. 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.

3.2.10. Propietarios de la Información

a. Clasificar los activos de información bajo su responsabilidad de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad, así como verificar que se les proporcione un nivel adecuado de protección, de conformidad con los estándares, políticas y procedimientos de seguridad de la información.

b. Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos en caso de una interrupción extendida.

c. Definir los requerimientos de continuidad y de recuperación en caso de desastre.

d. Coordinar la realización de un análisis de riesgos como mínimo una vez al año, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.

e. Comunicar sus requerimientos de seguridad de información al área correspondiente.

f. Determinar y autorizar todos los privilegios de acceso a sus activos de información.

g. Comunicar al área correspondiente sus requerimientos en capacitación sobre seguridad de información.

h. Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo, verificando los resultados de las revisiones y reportando cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo G).

i. 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.

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, al poner en riesgo la disponibilidad, confidencialidad e integridad de la misma, se deben evitar:

a. Dejar los computadores encendidos en horas no laborables.

b. Permitir que personas ajenas a las instituciones y entidades del Sector Defensa, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.

c. No clasificar y/o etiquetar la información.

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

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

f. 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.

g. Hacer uso de la red de datos de las instituciones y entidades del Sector Defensa, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

h. Instalar software en la plataforma tecnológica de las instituciones y entidades del Sector Defensa, cuyo uso no esté autorizado por la Oficina de Tecnología o quien haga sus veces, atentando contra las leyes de derechos de autor o propiedad intelectual.

i. Destruir la documentación institucional, sin seguir los parámetros y normatividad vigente establecida para el proceso de gestión documental.

j. Descuidar información clasificada de las instituciones y entidades del Sector Defensa, sin las medidas apropiadas de seguridad que garanticen su protección.

k. Enviar información no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.

l. Almacenar y mantener información clasificada en dispositivo de almacenamiento de cualquier tipo que no sean de propiedad de las respectivas instituciones y entidades del Sector Defensa.

m. Conectar computadores portátiles u otros dispositivos electrónicos personales, a la red de datos de las instituciones y entidades del Sector Defensa, sin la debida autorización.

n. Ingresar a la red de datos de las instituciones y entidades del Sector Defensa, por cualquier servicio de acceso remoto, sin la autorización de la oficina de tecnología o la que haga sus veces.

o. Usar servicios de internet en los equipos de la institución, diferente al provisto por la oficina de tecnología o la que haga sus veces.

p. Promover o mantener actividades personales utilizando los recursos tecnológicos de las instituciones y entidades del Sector Defensa, para beneficio personal.

q. Uso de la cuenta y contraseña de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.

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

s. Retirar de las instalaciones de las instituciones y entidades del Sector Defensa, computadores de escritorio, portátiles e información clasificada física o digital sin autorización, o abandonarla en lugares públicos o de fácil acceso.

t. Entregar, enseñar o divulgar información clasificada de las instituciones y entidades del Sector Defensa a personas o entidades no autorizadas.

u. Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de las instituciones y entidades del Sector Defensa o de terceras partes.

v. Ejecutar cualquier acción que difame, afecte la reputación o imagen de las instituciones y entidades del Sector Defensa, o de alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.

w. Realizar cambios no autorizados en la plataforma tecnológica de las instituciones y entidades del Sector Defensa.

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

y. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente directiva.

z. 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. INSTRUCCIONES GENERALES DE COORDINACIÓN

5.1. Revisión Independiente – Auditorías Internas

Cada institución y entidad del Sector Defensa es responsable de garantizar que se realicen revisiones periódicas al Sistema de Gestión de Seguridad de la Información, según el procedimiento de Auditorías Internas (Anexo R), para verificar su vigencia, su correcto funcionamiento y su efectividad

5.2. Gestión de Terceros

a. Cuando exista la necesidad de otorgar acceso de terceras partes a las instituciones y entidades del Sector Defensa deberá realizarse, siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:

- El tipo de acceso requerido (físico, lógico y a qué recurso)
- Los motivos para los cuales solicita el acceso
- El valor de la información
- Los controles empleados por la tercera parte

- La incidencia de este acceso en la seguridad de la información de las instituciones y entidades

b. En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones de las instituciones y entidades del Sector Defensa, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.

c. En ningún caso se otorgará acceso a terceros a la información, 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.

d. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la oficina de tecnología o la que haga sus veces, aprobarán y autorizarán el acceso y uso de la información.

e. 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 las instituciones y entidades del Sector Defensa

5.3. Acuerdos de Confidencialidad

Todos los funcionarios y terceros deben firmar la cláusula y/o acuerdo de confidencialidad que 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. 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.

5.4. Acuerdos de Intercambio de Información y Software

a. Todo funcionario y/o tercero es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

b. Los propietarios, de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo a la reglamentación vigente.

c. El intercambio de información y de software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen cláusulas de responsabilidad, deberes y derechos.

d. Los acuerdos de intercambio deben, en todo caso, velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo, deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.

e. Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realizará siguiendo el procedimiento establecido por la entidad que solicita la información.

f. El intercambio de información deberá contemplar las siguientes directrices:

- Uso de *web services*, para la publicación y consumo de información electrónica.
- Uso de canales cifrados.
- Respeto por los derechos de autor del software intercambiado.
- Términos y condiciones de la licencia bajo la cual se suministra el software.
- Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
- Informar al titular de los datos, el intercambio de estos con otras entidades.
- Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

5.5. Gestión de Activos de Información

Cada una de las instituciones y entidades del Sector Defensa tienen 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. Por lo tanto deben:

a. 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, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información.

b. Realizar la clasificación y control de activos de información con el objetivo de garantizar que los activos de información 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 de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información (Anexo H).

c. Realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.

d. Definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación de la información definido.

5.6. Uso Adecuado de los Activos de Información

Las instituciones y entidades que conforman el Sector Defensa podrán monitorear y supervisar la información, sistemas, servicios y equipos que sean de su propiedad, de acuerdo con lo establecido en esta política y la legislación vigente.

5.6.1 Internet:

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

1. 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.

2. Publicación, envío o adquisición de material sexualmente explícito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.

3. Publicación o envío de información confidencial hacia afuera de las instituciones y entidades del Sector Defensa sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.

4. Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados

5. Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.

6. Promover o mantener asuntos o negocios personales.

7. 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.

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

9. Uso de herramientas de mensajería instantánea no autorizadas por la oficina de tecnología, o la que haga sus veces.

10. 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 y 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.

5.6.2 Correo electrónico institucional o corporativo:

a. La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro de cada una de las instituciones y entidades que conforman el Sector Defensa.

b. Los mensajes y la información contenida en los buzones de correo institucional son de propiedad cada una de las instituciones y entidades que conforman el Sector Defensa. 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 el tráfico de la misma, se considera de interés del sector.

c. El tamaño de los buzones y mensajes de correo serán determinados por las oficinas de tecnología, o las que hagan sus veces, de las respectivas instituciones y entidades que conforman el Sector Defensa, conforme a las necesidades de cada usuario y previa autorización del jefe inmediato.

d. En cada institución y entidad se suministrará una cuenta de correo corporativa por cada oficina que lo requiera, la cual será utilizada para el envío masivo de correos institucionales.

e. No se considera aceptado el uso del correo electrónico corporativo para los siguientes fines:

1. Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, 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.

2. El envío de cualquier tipo de archivo que ponga en riesgo la seguridad de la información; en caso que sea necesario hacer un envío de este tipo de archivos deberá contar con la autorización correspondiente por parte de la oficina de tecnología, o la que haga sus veces.

3. El envío de información relacionada con la defensa y la seguridad nacional a otras entidades del Gobierno diferentes a las que conforman el Sector Defensa, sin la autorización previa del propietario de la información y de la oficina de tecnología, o la que haga sus veces.

f. Toda información que requiera ser transmitida fuera de cada institución y entidad del sector, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

g. Todo correo electrónico deberá respetar el estándar de formato e imagen corporativa definido para cada una de las instituciones y entidades del Sector Defensa y deberá contener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

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

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

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

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

5.6.3 Redes Inalámbricas:

a. Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a las redes institucionales.

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

c. El servicio de Internet en las Escuelas de Formación y Capacitación, deberá contar con mecanismos de autenticación de usuarios y deberá estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación.

d. El servicio de internet en las escuelas de formación, capacitación y en las instalaciones destinadas para el bienestar social, deben estar configuradas de forma independiente a la red operativa de la institución o entidad del Sector Defensa.

e. Se debe implementar infraestructura inalámbrica que permita configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas establecidas por defecto.

5.6.4 Segregación de Redes:

a. La plataforma tecnológica crítica de las instituciones y entidades del Sector Defensa que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

b. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere. La Oficina de Tecnología, o la que haga sus veces, es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

5.6.5 Computación en la Nube (Cloud Computing)

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

b. Ningún servicio de carácter operativo e institucional de las instituciones y entidades del Sector Defensa, deberán ser contratados en servicios en la nube públicos o híbridos.

c. Para el caso de las escuelas de formación y capacitación se podrá hacer uso de servicios en la nube públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada.

d. Las instituciones y entidades del Sector Defensa, podrán implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

5.6.6 Sistemas de Información de Acceso Público

a. La información pública producida por las instituciones y entidades del Sector Defensa, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

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

c. Las instituciones y entidades del Sector Defensa, deberán 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 los portales institucionales, o en cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina de Comunicaciones Estratégicas, o similares, y deberá estar debidamente rotulada según su nivel de clasificación.

5.6.7 Recursos tecnológicos:

a. La instalación de cualquier tipo de software en los equipos de cómputo de cada institución y entidad que conforma el Sector Defensa es responsabilidad exclusiva de sus Oficinas de Tecnología, o las que hagan sus veces, por tanto son los únicos autorizados para realizar esta labor.

b. Ningún activo de información debe ser instalado con la configuración establecida por defecto por el 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 las Oficinas de Tecnología, o las que hagan sus veces, de las correspondientes instituciones y entidades que conforman el Sector Defensa

d. 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 las Oficinas de Tecnología, o las que hagan sus veces.

e. Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación con la entidad del sector para la que estuviere prestando sus servicios.

f. De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

5.7. Clasificación de la Información

a. Toda la información deberá ser identificada, clasificada y documentada con base en los criterios de clasificación definidos en el Manual de Contrainteligencia (MACI) FF.MM2-6-Reservado y resolución número 03049 de 2012 DIPON "Manual del Sistema de Gestión de Seguridad de la Información".

b. Los propietarios de los activos de información son los responsables de establecer el nivel de clasificación de cada activo.

5.8. Concientización y Capacitación en Seguridad de la Información

a. Las instituciones y entidades que conforman el Sector Defensa, deben mantener un programa anual de concientización y capacitación para todos sus funcionarios así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades en sus instalaciones.

b. Todos los funcionarios y terceros al servicio de las instituciones y entidades que conforman el sector, 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.

5.9. Finalización de la Relación Laboral

Al momento de la desvinculación o de cambio de roles, todo funcionario y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados. Esto mediante el formato establecido en cada una de las instituciones y entidades del Sector.

5.10. Seguridad física y ambiental

a. La protección física se llevara a cabo mediante la creación de diversas barreras o medidas de control físicas, alrededor de las instituciones y entidades del Sector Defensa y de las instalaciones de procesamiento de información.

b. Las áreas protegidas se resguardaran mediante el empleo de controles de acceso físico a fin de permitir el acceso solo a personal autorizado.

c. Para la selección de las áreas protegidas 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 tomaran en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

d. Para incrementar la seguridad de las áreas protegidas se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

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

f. Se deberá garantizar la seguridad física del Centro de Datos incluyendo, entre otros, el sistema eléctrico, el sistema de protección contra incendios y el control de temperatura.

5.11. Acceso Físico

a. Se evaluarán las necesidades de capacitación e implementación de los procedimientos y controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de los activos de información.

b. Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y terceros autorizados evitar que las puertas se dejen abiertas.

c. Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por cada una de las instituciones y entidades que conforman el sector, mientras permanezcan dentro de sus instalaciones.

d. Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.

e. Es responsabilidad de todos los funcionarios y terceros acatar las normas de seguridad y mecanismos de control de acceso a las instituciones y entidades del Sector Defensa.

f. Los funcionarios y terceros, así como los visitantes, deberán tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones.

5.12. Trabajo en Áreas Protegidas

a. Todas las áreas que se hayan definido como protegidas y activos de información que la componen, mediante el procedimiento de control de acceso a área protegida, son considerados áreas seguras; por lo tanto deben ser protegidas de acceso no autorizado mediante controles y tecnologías de autenticación.

b. Todo acceso físico a las áreas protegidas deberá estar manejado según los lineamientos definidos por el procedimiento de Control de Acceso a Área protegida (Anexo I).

c. En las áreas seguras donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

1. No se deben consumir alimentos ni bebidas.
2. No se deben ingresar elementos inflamables.
3. No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
4. No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
5. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
6. 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.

5.13. Seguridad y Mantenimiento de los Equipos

a. Los equipos que hacen parte de la infraestructura tecnológica de las instituciones y entidades que conforman el Sector Defensa deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

b. Las instituciones y entidades que conforman el Sector Defensa adoptarán 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 terceros 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.

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 tales como máquinas de copiado, impresoras y máquinas de fax deberán estar ubicados en zonas de acceso restringido y se permitirá el uso únicamente a personal autorizado.

f. Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de las instituciones y entidades que conforman el Sector Defensa.

g. Las instituciones y entidades que conforman el Sector Defensa garantizarán 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.

5.14. Seguridad de los Equipos Fuera de las Instalaciones

a. Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones de cada una de las instituciones y entidades que conforman el Sector Defensa, deben velar por la protección de los mismos sin dejarlos desatendidos, comprometiendo la imagen o información del sector.

b. El propietario del activo, con el apoyo de la oficina de tecnología o la que haga sus veces, identificará mediante una metodología de análisis de riesgos que cada institución o entidad establezca, los riesgos potenciales que puede generar el retiro de equipos o medios de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

c. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información 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 (Anexo G) y se deberá poner la denuncia ante la autoridad competente, si aplica.

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

5.15. Traslado de Propiedad

a. El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica, debe ser autorizado por el propietario del activo previa solicitud del funcionario interesado. Si el activo está clasificado como relacionado con la defensa y la seguridad nacional, el retiro deberá estar autorizado también por el Ayudante General (o quién haga sus veces).

b. Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones de las instituciones y entidades del Sector Defensa, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.

c. Las instituciones y entidades que conforman el Sector Defensa proporcionarán los mecanismos y recursos necesarios para que en cada punto de acceso a sus instalaciones exista un puesto de revisión donde se inspeccione y se lleve el control de los equipos que son ingresados y retirados.

d. Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos sólo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a través del proceso de sanitización. Las Oficinas de Tecnología, o las que hagan sus veces, de las instituciones y entidades que conforman el Sector Defensa, generarán un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.

5.16. Documentación de Procedimientos Operativos

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, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

c. La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por el administrador de la aplicación, propietario del activo, Jefe de dependencia o el funcionario a quien se le hayan otorgado dichas funciones.

d. Los procedimientos operativos deben contener instrucciones para el manejo de los 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.

5.17. Control de Cambios Operativos

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de las Oficinas de Tecnología, o las que hagan sus veces, de las instituciones y entidades que conforman el Sector Defensa, 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 (Anexo J). Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

5.18. Segregación de Funciones

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 Oficinas de Tecnología, o las que hagan sus veces, con el fin de mantener actualizada dicha información acorde con la realidad de cada una de las instituciones y entidades que conforman el Sector Defensa.

5.19. Separación de Ambientes

a. Cada una de las instituciones y entidades que conforman el Sector Defensa proveerán 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. El paso de software y hardware, de un ambiente a otro, deberá ser controlado y gestionado de acuerdo con lo definido en el Procedimiento de Control de Cambios (Anexo J).

c. 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.

d. 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.

e. El ambiente del sistema de prueba debe emular el ambiente de producción lo más estrechamente posible.

f. No se permite la copia de información Ultra Secreta, Secreta, Reservada, Confidencial, Restringida o Exclusiva de Comando, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe contar con las respectivas autorizaciones y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y que se elimine de forma segura después de su uso.

g. 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.

h. Periódicamente se deberá verificar las versiones instaladas tanto en ambiente de pruebas como en producción y se confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de cada institución y entidad del sector.

5.20. Gestión de la Capacidad

a. Las Oficinas de Tecnología, o las que hagan sus veces, como áreas responsable de la administración de la plataforma tecnológica, deberán implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación, conforme a lo establecido en el Procedimiento Gestión de la Capacidad (Anexo K).

b. El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.

5.21. Protección contra Software Malicioso

a. Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en los procedimientos de Gestión de Vulnerabilidades Técnicas (Anexo L) y Control de Cambios (Anexo J).

b. 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.

c. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de las correspondientes Oficinas de Tecnología, o las que hagan sus veces, y deberán ser actualizados permanentemente.

d. 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.

e. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de las diferentes instituciones y entidades que conforman el Sector Defensa deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

f. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por el área competente.

g. Cada institución y entidad que conforma el Sector Defensa 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.

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

5.22. Copias de Respaldo

a. Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por las Oficinas de Tecnología, o las que hagan sus veces, y las dependencias responsables de la misma, contenida en la plataforma tecnológica de las instituciones y entidades del Sector Defensa, 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 (Anexo M).

b. Los medios de las copias de respaldo se almacenarán tanto localmente como 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.

c. Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares, establecidos según las necesidades y capacidades de cada una de las instituciones y entidades del Sector por sus correspondientes oficinas de tecnología, o las que hagan sus veces, con el fin de asegurar que son confiables en caso de emergencia. Estas copias serán retenidas por un periodo de tiempo determinado, de acuerdo a lo establecido en el procedimiento de Gestión de Copias de Respaldo (Anexo M).

d. Las Oficinas de Tecnología, o las que hagan sus veces, establecerán procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca de su traslado, frecuencia e identificación; así mismo, definirá conjuntamente con las dependencias usuarias los períodos de retención de dicha in formación.

e. Se debe disponer de los recursos necesarios para permitir la identificación relacionada 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.

5.23. Gestión de Medios Removibles

a. Se restringe la conexión no autorizada a la infraestructura tecnológica del Sector Defensa, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CD, DVD, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

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

c. Las instituciones y entidades que conforman el Sector Defensa definirán los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser 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, dando cumplimiento a los lineamientos establecidos en el procedimiento de Inventario y Clasificación de Activos de Información (Anexo H). Si un medio removible llegase a contener información con distintos niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.

e. Para los procesos de baja, de reutilización o de garantía de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. La destrucción segura se documentará mediante acta, registro fílmico y fotográfico.

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

5.24. Computación Móvil

a. Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se debe implementar controles de acceso y técnicas criptográficas para cifrar la información crítica almacenada en estos.

b. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser debidamente autorizada por la oficina de tecnología, o la que haga sus veces, previa verificación de que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura.

5.25. Gestión de Registros

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 que serán

verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento Monitoreo y Revisión de *"Logs"*.

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. El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

d. 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 tecnología, o la que haga sus veces, mediante el procedimiento de Gestión de Incidentes de Seguridad (Anexo G).

5.26. Control de Acceso

a. Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

b. El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el propietario de cada activo, según el procedimiento Gestión de Usuarios y Contraseñas (Anexo O).

c. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática del Sector Defensa deberá estar autorizado por la respectiva Oficina de Tecnología, o la que haga sus veces.

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

e. La creación, modificación y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática deberá seguir el procedimiento Gestión de Usuarios y Contraseñas (Anexo O).

f. Todo usuario que se cree para que un tercero ingrese a las redes de las instituciones y entidades del Sector Defensa, debe tener una fecha de vencimiento específica, la cual en ningún caso debe superar la fecha de terminación de sus obligaciones contractuales.

g. La asignación de privilegios en las aplicaciones para los diferentes usuarios estarán determinados por el procedimiento Gestión de Usuarios y Contraseñas (Anexo O). Estos privilegios deben revisarse a

intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

h. Los equipos de terceros que requieran acceder a la redes de datos de las diferentes instituciones y entidades que conforman el Sector Defensa deben cumplir un procedimiento de sanitización informática antes de concedérseles dicho acceso.

i. Los equipos de terceros que hayan sido autorizados para acceder de forma permanente a una o varias de las redes de datos institucionales, sólo podrán hacerlo una vez se haya cumplido con el formateo inicial de discos duros y/o medios de almacenamiento; posteriormente, deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba definido. Una vez culminadas estas labores se debe proceder a un formateo final para retirar estos equipos de las instalaciones.

c. Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de Tecnología, o la que haga sus veces, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura.

5.27. Administración de Contraseñas

a. La administración así como la asignación y entrega de las contraseñas a los usuarios deberá seguir el procedimiento Gestión de Usuarios y contraseñas (Anexo O).

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:

1. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.

2. Las contraseñas no deberán ser reveladas.

3. 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 Gestión de Usuarios y Contraseñas (Anexo O).

4. Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que una persona esté utilizando un usuario y contraseña que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad (Anexo G).

5.28. Bloqueo de Sesión, Escritorio y Pantalla Limpia

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 mismo usuario que la bloqueó.

c. Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la respectiva institución y entidad del sector.

d. 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.

e. 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.

5.29. Control de Versiones

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, de acuerdo con el procedimiento Control de Versiones (Anexo Q).

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 (Anexo G).

5.30. Controles Criptográficos

a. Las Oficinas de Tecnología, o las que hagan sus veces, de las instituciones y entidades que conforman el Sector Defensa, deben identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en

el procedimiento de Inventario y Clasificación de Activos de Información (Anexo H), tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

b. No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por las Oficinas de Tecnología, o las que hagan sus veces, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y terceros autorizados.

5.31. Gestión de Vulnerabilidades Técnicas

a. Las Oficinas de Tecnología, o las que hagan sus veces, se encargarán de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.

b. Las Oficinas de Tecnología, o las que hagan sus veces, serán responsables de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la institución o entidad.

c. No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la oficina de tecnología, o la que haga sus veces, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del Sector Defensa, 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. Se realizará, por parte del área competente, el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

f. Las Oficinas de Tecnología, o las que hagan sus veces, realizarán las revisiones de las alertas de seguridad definiendo, en caso de ser necesario, un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

5.32. Gestión de Incidentes de Seguridad de la Información

a. Los funcionarios y terceros 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 (Anexo G).

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

c. Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad (Anexo G) para cada una de las instituciones y entidades que conforman el Sector Defensa.

d. 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.

e. Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de seguridad de la información.

f. Los resultados de las investigaciones que involucren a los funcionarios del Sector Defensa deberán ser informados a las áreas de competencia.

g. Las instituciones y entidades que conforman el Sector Defensa deberán 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.

5.33. Seguridad de la Información en la Continuidad del Negocio

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. Las entidades que conforman el Sector Defensa deberán contar con un Plan de Continuidad del Negocio 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 Continuidad de Negocio.

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 Continuidad de Negocio.

5.34. Derechos de Propiedad Intelectual

a. Las instituciones y entidades que conforman el Sector Defensa cumplirán con la reglamentación vigente sobre 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 software a la medida, adquirido a terceras partes o desarrollado por funcionarios de las instituciones y entidades del Sector Defensa, serán de uso exclusivo de dicha entidad y la propiedad intelectual será de quien lo desarrolle.

6. 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.

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 las entidades que conforman el Sector Defensa, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros.

JUAN CARLOS PINZÓN BUENO
Ministro de Defensa Nacional

ANEXOS:

A. GLOSARIO.
B. FORMATO DE INVENTARIO DE ACTIVOS DE INFORMACION.
C. FORMATO ACUERDO DE CONFIDENCIALIDAD.
D. FORMATO AUTORIZACIÓN INGRESO / SALIDA EQUIPOS INSTITUCIONALES
E. FORMATO AUTORIZACIÓN INGRESO / SALIDA EQUIPOS ENTIDADES EXTERNAS
F. FORMATO REPORTE INCIDENTES DE SEGURIDAD
G. PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD
H. PROCEDIMIENTO DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN
I. PROCEDIMIENTO DE CONTROL DE ACCESO A ÁREA PROTEGIDA
J. PROCEDIMIENTO DE CONTROL DE CAMBIOS
K. PROCEDIMIENTO GESTIÓN DE LA CAPACIDAD
L. PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES TÉCNICAS
M. PROCEDIMIENTO GESTIÓN DE COPIAS DE RESPALDO
N. PROCEDIMIENTO MONITOREO Y REVISIÓN DE "LOGS".
O. PROCEDIMIENTO GESTIÓN DE USUARIOS Y CONTRASEÑAS.
P. PROCEDIMIENTO DE SANITIZACIÓN INFORMÁTICA
Q. PROCEDIMIENTO CONTROL DE VERSIONES
R. PROCEDIMIENTO AUDITORÍAS INTERNAS
S. PROCEDIMIENTO IDENTIFICACIÓN Y TRATAMIENTO DE RIESGOS

DISTRIBUCIÓN

Original	:	Ministerio de Defensa Nacional
Copia No.1	:	Comando General de las Fuerzas Militares
Copia No.2	:	Comando Ejército Nacional
Copia No.3	:	Comando Armada Nacional
Copia No.4	:	Comando Fuerza Aérea Colombiana
Copia No.5	:	Dirección General Policía Nacional
Copia No.6	:	Viceministerio para las Políticas y Asuntos Internacionales
Copia No.7	:	Viceministerio para la Estrategia y la Planeación
Copia No.8	:	Viceministerio del Grupo Social y Empresarial del Sector Defensa
Copia No.9	:	Secretaria General del Ministerio de Defensa Nacional
Copia No.10	:	Dirección General de Sanidad Militar
Copia No.11	:	Dirección Empresas del GSED
Copia No.12	:	Comando Conjunto Cibernético

Firmado digitalmente por :HUGO DE JESUS GARCIA DE VIVERO

Director de Logística