MANUAL
DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
DIGSA

SGSI
SISTEMA DE GESTIÓN
DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción de los cambios
1	Diciembre de 2020	Versión Inicial

CONTROL DE APROBACION

Aprobó:	CR. Luis Hernando Sandoval Pinzon Subdirector Técnico y de Gestión DIGSA	
Revisó:	GRADO. CS. Vivian Tatiana Alba Díaz Gestor de Calidad PROGTIC	CR. Carlos Darío Gonzalez Villamil Coordinador Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA
	SMSM. Edna del Pilar Martínez Páez Grupo Planeación Estratégica DIGSA Líder Área Sistemas Integrados de Gestión ARSIG	PD. Alexandra Martínez Vargas Coordinadora Grupo Planeación Estratégica DIGSA Representante de la Dirección
Elaboró:	PD. Diana Marcela Lopez Bejarano Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones DIGSA Área Seguridad de la Información	

Tabla de Contenido

1. Presentación

La política de Gobierno Digital es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas. Dentro de los elementos base que permiten el desarrollo de dicha política se encuentra el de Seguridad y Privacidad, el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Debido a los múltiples riesgos y amenazas que en la actualidad atentan contra la seguridad de la información, la protección y la privacidad de los datos, se hace indispensable que la Dirección General de Sanidad Militar implemente, mantenga y optimice de manera continua un Sistema de Gestión de Seguridad de la Información.

Para realizar este modelo se requiere elaborar una serie de procesos, políticas y procedimientos que conllevan al cumplimiento de los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones. Por esta razón el siguiente Manual de Políticas de Seguridad de la Información establece los lineamientos y políticas administrativas, técnicas y legales, las cuales deben ser adoptadas por todos los funcionarios, contratistas, proveedores, y todo personal externo que utilice los servicios de tecnologías de la información que ofrece la Dirección General de Sanidad Militar. El desarrollo de Políticas de Seguridad de la Información le permitirá a la DIGSA tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, permitiendo una gestión oportuna, efectiva y aprovechando de una manera eficiente los activos con que cuenta.

Las políticas de seguridad descritas en el presente manual, se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. Objetivo General

Establecer lineamientos de seguridad de alto nivel que permitan que los activos de información de propiedad de la DIGSA, sean accedidos sólo por las personas autorizadas que tienen necesidad legítima para la realización de las funciones propias de la DIGSA (confidencialidad), que no se realicen modificaciones sin autorización y se salvaguarde su exactitud y completitud (integridad), así como que sean accesibles y utilizables cuando éstos se requieran para el desarrollo de las actividades propias de la entidad (disponibilidad); alineados con la misión, visión, objetivos estratégicos y valores de la DIGSA.

3. Alcance

Las políticas de seguridad de la información dan cumplimiento a las disposiciones legales vigentes en materia de seguridad de la información, se enmarcan dentro de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia y en la norma internacional del Sistema de Gestión de Seguridad de la Información ISO 27001:2013.

Son aplicables para todos los aspectos administrativos, técnicos, tecnológicos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y proveedores que presten sus servicios o tengan algún tipo de vinculación con la Dirección General de Sanidad Militar y que accedan al uso de las plataformas y servicios tecnológicos que preste la DIGSA, con el fin de alcanzar un adecuado nivel de seguridad y protección de los activos de información.

4. Fundamento Normativo

- Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

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

- Ley 1341 de 2009. "Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales

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

- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". Decisión Andina 351 de 2015 "Régimen común sobre derecho de autor y derechos conexos".

- Decreto 1377 de 2013. "Por el cual se reglamenta parcialmente la Ley 1581 de 2012 sobre la protección de datos personales.

- Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea...", donde se encuentra como componente el Modelo de Seguridad y Privacidad de la Información.

- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- Decreto 1413 de 2017 "Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

- Norma Técnica Colombiana ISO27001:2013. Sistemas de Gestión de Seguridad de la Información

- Norma Técnica Colombiana ISO31000:2013. Gestión del Riesgo Principios y Directrices.

- Directiva Permanente Nro. DIR2014-18 "Políticas de Seguridad de la Información para el Sector Defensa"

- Directiva Permanente No. 154 /MDN-CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1 "Políticas de Seguridad de las Información para las Fuerzas Militares"

- Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital año 2018.

5. Definiciones

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

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

Análisis de riesgos: Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

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

Control: Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de

riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

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

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Incidente de seguridad de la información: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

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

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Privacidad: La capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos.

Procedimiento: Forma específica de llevar a cabo una actividad o un proceso.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario de activo de información: Identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

Responsable del tratamiento: Persona natural o jurídica, pública o privada. Que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de la DIGSA. Se expresa en términos de probabilidad y consecuencias.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

6. Acrónimos

AREIN:	Área de Seguridad de la Información
ARECO:	Área de Infraestructura Tecnológica, Redes y Comunicaciones
ARIBD:	Área administración del Sistema y Base de Datos
CCOCI:	Comando Conjunto Cibernético
COLCERT:	Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
CSIRT:	Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía.
DIGSA:	Dirección General de Sanidad Militar.
MSPI:	Modelo de Seguridad y Privacidad de la Información.
MINTIC:	Ministerio de Tecnologías de la Información y Comunicaciones.
SISAM:	Grupo Sistema Integral de Información – Tecnologías de la Información y la Comunicaciones
SGSI:	Sistema de Gestión de Seguridad de la Información.
SGSPI:	Sistema de Gestión de Seguridad y Privacidad de la Información
TIC:	Tecnologías de la Información y las Comunicaciones.

7. Compromiso de la Dirección

La Alta Dirección de la DIGSA está comprometida con el desarrollo y la implementación de políticas de Seguridad de la Información, así como de su mejora continua, mediante:

a) La autorización para la implementación de políticas de Seguridad de la Información en la DIGSA.

b) La revisión y aprobación de políticas de Seguridad de la Información.

c) El suministro de los recursos necesarios para una adecuada implementación de políticas de Seguridad de la Información y el DIGSA.

d) La divulgación sobre la importancia de cumplir las políticas de Seguridad de la Información para el logro de los objetivos de seguridad.

El compromiso de la Alta Dirección asegura la identificación, evaluación, tratamiento, monitoreo y control de los riesgos que puedan alterar la Seguridad de la Información; mediante la destinación de los recursos físicos, humanos y económicos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGSI en los procesos de la DIGSA.

8. Generalidades de las políticas de Seguridad de la Información

8.1 Organización de la Seguridad de la Información

La DIGSA mediante la Directiva Permanente No.154/CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1- Políticas de Seguridad de la Información para las Fuerzas, establece y difunde los criterios y comportamientos generales que deben seguir todos los funcionarios, contratistas, practicantes, y cualquier persona que tenga una relación con las Fuerzas Militares, 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, protegiendo adecuadamente la información, reduciendo los riesgos y optimizando el empleo de tecnologías de información.

8.2 Roles y Responsabilidades

Todos los funcionaros públicos, contratistas y terceros de la DIGSA, deben conocer y dar cumplimiento al modelo de seguridad y privacidad de la información establecido en la Entidad, así mismo la gestión de la Seguridad y Privacidad de la Información es un Sistema transversal a todos los procesos de la entidad (Estratégico, Misionales, Apoyo, Evaluación y Control), por tal motivo la DIGSA define y asigna los roles y responsabilidades para el cumplimiento del Sistema de Gestión de Seguridad y Privacidad de la Información-SGSPI, así:

a. Comité Técnico Comité Institucional de Gestión y Desempeño

El Comité Institucional de Gestión y Desempeño, acorde con lo definido en el Decreto 1499 de 2017, debe incluir todos los temas que atiendan la implementación y desarrollo de las políticas de gestión definidas en el MIPG, entre las que se encuentra la Política de Seguridad Digital.

b. Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones-SISAM

- Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información.
- Aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información de los activos de información tecnológicos y recursos informáticos de la DIGSA.
- Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de Seguridad de la Información.
- Incluir los controles de seguridad de la información en el diseño, desarrollo, instalación y mantenimiento de las aplicaciones bajo su responsabilidad.
- Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Gestionar la plataforma tecnológica que soporta los procesos de la entidad.
- Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.
- 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 software y de aplicaciones.
- Establecer y dar mantenimiento a los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

A través del Área de Seguridad de la Información se debe:

- Implementar el Modelo de Seguridad y Privacidad de la información-MSPI en la DIGSA de acuerdo a los lineamientos dados por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

- Establecer, documentar y actualizar las políticas y los procedimientos de Seguridad de la Información que apliquen para la plataforma de tecnologías de información administrada por el grupo SISAM.

- Validar y monitorear, de manera periódica, la implementación de los controles de seguridad establecidos.

- Con el apoyo del Comando Conjunto Cibernético-CCOCI, gestionar y monitorear las alertas e incidentes de seguridad de la información que se presenten en la infraestructura tecnológica de la DIGSA.

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

c. Grupo de Talento Humano[1]

- Comunicar los derechos y establecer las responsabilidades legales que adquiere cada funcionario, contratista o tercero, con relación al manejo y protección de los datos institucionales tanto al interior como fuera de las instalaciones.

- Incluir en los contratos cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad en el cumplimiento de las políticas de seguridad de la información de la Dirección General de Sanidad Militar. Lo anterior a través del documento de confidencialidad denominado "Acta de Compromiso de Reserva, Seguridad y Calidad de la Información Personal Militar – Civil Planta y Civil Vinculado por Contrato o Convenio", el cual deberá ser parte integral de los contratos.

- Garantizar que se realicen las verificaciones y controles de seguridad requeridos por la criticidad del empleo, tales como verificación de antecedentes judiciales, validación de certificados de estudios presentados, validación de referencias de comportamiento satisfactorio y validación de su hoja de vida.

- Definir claramente las funciones y tareas que desempeñará el funcionario en el cargo con el fin de establecer la responsabilidad en el manejo de la información, teniendo en cuenta la clasificación de la misma y el cumplimiento de las políticas de seguridad de la información.

- Elaborar y ejecutar programas de inducción y de re-inducción para los funcionarios asegurando que conozcan sus responsabilidades e 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 o contratista.

[1] NTC-ISO-IEC 27001 A.7

- Gestionar los aspectos de seguridad que se requieran durante el proceso de desvinculación laboral de cualquier empleado, y demás novedades de personal comunicando de forma oficial al Grupo Sistema Integral de Información-Tecnologías de la Información y las comunicaciones y demás grupos de la DIGSA, con el fin de que se tomen las medidas y procedimientos de inactivación de cuentas de usuario, accesos a sistemas de información entrega de hardware, software e información a su cargo, necesarios para evitar riesgos que atenten contra la seguridad de la información.

- Solicitar la devolución del carné o cualquier distintivo de autenticación que lo acredita como funcionario de la Dirección General de Sanidad Militar.

- Dar cumplimiento a los artículos establecidos en la Ley Estatutaria No. 1581 de 17 de octubre del 2012 por la cual de dictan disposiciones generales para la protección de datos personales.

d. Grupo de Asuntos legales

- Define, documenta y actualiza los requerimientos estatutarios, regulatorios y contractuales en materia de seguridad de la información, y establece los lineamientos de la entidad para satisfacer estos requerimientos.

- Asesora a la entidad en materia legal en lo relacionado a la seguridad de la información y establece las pautas legales que permitan cumplir con los requerimientos legales en esta materia.

e. Grupo Contratación

- Vela por la incorporación de las cláusulas en materia de seguridad de la información en los contratos, acuerdos u otra documentación que la entidad firme con contratistas y/o terceros. Por medio de los documentos denominados "Acta Compromiso de Reserva Externos" y "Acuerdo de Confidencialidad Sector Defensa – Anexo C", los cuales deberán reflejarse en los respectivos contratos.

f. Coordinadores de Grupo y/o supervisores de contratos de prestación de servicios

- Cuando un funcionario termine la relación laboral o contractual, el Coordinador de Grupo y/o Supervisor del Contrato, debe comunicar de manera oficial al Grupo de Talento Humano y al Grupo de Contratos, para que se realicen los trámites pertinentes de cancelación de cuentas de usuario.

- Cuando un funcionario sea trasladado de dependencia, el Coordinador de Grupo y/o supervisor deberán informar a los líderes funcionales y al Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, para retirar los accesos lógicos a los activos de información (herramientas tecnológicas ejemplo: Kactus, OnBase) a los cuales tenía acceso en la Dependencia.

- Cuando un funcionario termine su relación laboral y/o contractual, y/o sea trasladado de dependencia, el coordinador de grupo y/o supervisor deberán verificar la entrega de la información y hardware (equipo de escritorio-portátil) que tenía a su cargo.

- Cuando un funcionario termine su relación laboral y/o contractual, y/o sea trasladado de dependencia, el Coordinador de Grupo y/o Supervisor deberán informar al Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, para hacer limpieza de la información almacenada en las estaciones de trabajo antes de asignarse nuevamente dicho equipo.

- El Coordinador de Grupo y/o supervisor, deberá verificar que cuando un funcionario se desvincule o cambio de roles en la DIGS, haga entrega de todos los activos de información que le hayan sido asignados, mediante el procedimiento de desvinculación establecido por el Grupo de Talento Humano.

- El traslado entre Dependencias de la Dirección General de Sanidad Militar de todo activo informático, está bajo el control del Grupo Apoyo Administrativo. Cuando se requiera retirar de las instalaciones de la entidad activo informáticos, se deberá solicitar autorización al Grupo de Apoyo Administrativo, con el fin de registrar, controlar y hacer seguimiento a los mismos. El usuario que retire el activo será el responsable de la custodia, salvaguarda de la información que allí este almacenada.

- Los funcionarios y/o contratistas que tengan activos informáticos a su cargo, son responsables de la pérdida o daño que sufran, cuando lo anterior no se ocasione por el deterioro natural, por su uso normal o por otra causa justificada.

- Los Coordinadores de Grupo y/o lideres deberán 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.

8.3 Acciones que afectan la seguridad de la Información

a. Dejar los computadores encendidos en horas no laborales

b. Permitir que personas ajenas a la DIGSA 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 los documentos impresos que contengan información clasificada al terminar la jornada laboral.

e. No retirar de forma inmediata todos los documentos con información sensible que se envíen a la 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 la DIGSA para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.

g. Instalar software en la plataforma tecnológica de la DIGSA cuyo uso no esté autorizado por el Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones (SISAM) y que pueda atentar contra las leyes de derechos de autor o propiedad intelectual.

h. 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.

i. Guardar información clasificada en cualquier dispositivo de almacenamiento que no pertenezca a la DIGSA.

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

k. Ingresar a la red de datos de la DIGSA por cualquier servicio de acceso remoto sin la autorización del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

l. Usar servicios de internet en los equipos de la DIGSA, diferente al provisto por el Grupo SISAM.

m. Realizar actividades personales o utilización de los recursos tecnológicos de la DIGSA para beneficio personal.

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

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

p. Retirar de las instalaciones de la DIGSA computadores de escritorio, portátiles e información física o digital clasificada sin la debida autorización.

q. Entregar, enseñar o divulgar información clasificada de la DIGSA a personas o Entidades no autorizadas.

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

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

t. Realizar cambios no autorizados en la plataforma tecnológica de la DIGSA.

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

v. Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente política de seguridad de la información.

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

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

y. 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 caso.

9. Política General de Seguridad de la Información

La siguiente es la política de Seguridad de la Información establecida para la Dirección de Sanidad Militar, así:

"La DIGSA, como entidad encargada de asegurar la prestación del servicio de salud del personal afiliado y beneficiario de las Fuerzas Militares, reconoce la importancia de identificar y proteger sus activos de información frente a riesgos asociados, así como propender por los principios de seguridad de la información, relacionados con su confidencialidad, disponibilidad e integridad; comprometiéndose a establecer, implementar, mantener, evaluar, gestionar, proteger, preservar y mejorar continuamente su Sistema de Gestión de Seguridad de la Información - SGSI bajo los aspectos del ordenamiento legal, sus objetivos estratégicos y código de integridad".

La Alta Dirección de la DIGSA, deduciendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos; alineado con el ordenamiento jurídico y normativo en concordancia con la misión, visión, objetivos estratégicos y valores de la Entidad.

Para la DIGSA, la protección de la información busca la disminución del impacto generado sobre los activos de información por los riesgos identificados de manera sistemática; con el propósito de mantener un nivel aceptable de exposición que permita responder por la confidencialidad, disponibilidad e integridad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

10. Políticas específicas de seguridad de la información

La DIGSA considera la información como un activo fundamental para la Entidad, razón por la cual es necesario que se establezca un marco para asegurar que la información es protegida independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Las políticas específicas de Seguridad de la Información, constituyen una parte fundamental del SGSI de la DIGSA, se consideran la base para la implementación de los controles, procedimientos y estándares definidos y serán revisadas periódicamente o en caso de cambios relevantes en la Entidad que incidan en la Seguridad de la Información, con el fin de asegurar que sigan siendo adecuadas y ajustadas a las recomendaciones de la Guía de Seguridad y Privacidad de la Información establecida por MINTIC y la Norma NTC-ISO-IEC 27001.

La Seguridad de la Información es una prioridad para la DIGSA y por tanto es responsabilidad de todos los funcionarios, contratistas y/o terceros, velar por el cumplimiento de estas políticas.

A continuación, se presenta la descripción general de las políticas específicas de Seguridad de la Información relevantes para el cumplimiento de los objetivos y la implementación del SGSI de la DIGSA, las cuales serán gestionadas como parte de la implementación del SGSI, así:

10.1 Políticas de Gestión de Activos[2]

10.1..1 Control de Activos de Información (Hardware y Software)

a. La DIGSA 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, de acuerdo al procedimiento Gestión de Activos de Información de la DIGSA.

c. La entidad debe realizar la clasificación y control de los 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

[2] NTC-ISO-IEC 27001 A.8.1

niveles de protección y medidas de tratamiento de acuerdo al procedimiento de procedimiento Gestión de Activos de Información de la DIGSA.

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

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

10.1..2 Uso Adecuado de los Activos de Información (Hardware y Software)

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, teléfonos, entre otros) de todas y cada una de la Dirección General de Sanidad Militar-DIGSA, son activos de información que se proporcionan a los funcionarios y contratistas para cumplir con sus actividades laborales. La DIGSA se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en el presente manual de políticas de seguridad de la información y la legislación vigente.

10.1..3 Uso de Internet

El uso adecuado de la navegación de internet se deberá controlar, verificar y monitorear de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se consideran aceptables los siguientes usos:

a. Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

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

c. 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.

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

e. 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 Coordinador de Grupo junto con el diligenciamiento del formato Solicitud Recursos Informáticos DIGSA.

f. Promover o mantener asuntos o negocios personales.

g. 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.

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

i. Uso de herramientas de mensajería instantánea no autorizadas por el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

j. Emplear cuentas de correo externas no institucionales para el envío o recepción de información institucional.

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

l. El uso de internet no considerado dentro de las prohibiciones 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.

10.2 Clasificación de la Información

a. La Clasificación de la seguridad de la información es el nivel de seguridad asignado a una información contenida, manejada o registrada por cualquier medio, según su incidencia o importancia respecto de la seguridad nacional, institucional, operacional o personal.

b. Los Coordinadores de Grupo son los responsables de establecer el nivel de clasificación de cada activo de información.

c. Expedir la tarjeta de autorización de acceso a la información con base en los siguientes documentos: estudio de seguridad de personal, acto de posesión y funciones del cargo u obligaciones contractuales.

d. La autorización del acceso a información clasificada en el nivel asignado, no implica que se tenga derecho a conocer toda la información de dicha clasificación, se debe mantener el principio de la compartimentación.

e. Para obtener la autorización de acceso a la información clasificada, los funcionarios o contratistas deben acreditar el conocimiento de las políticas de seguridad de la información de la DIGSA.

10.3 Control de Medios Removibles

a. Se restringe la conexión no autorizada a la infraestructura tecnológica de la DIGSA, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, modems, 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. La DIGSA definirá 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 (ejemplo: token área financiera). Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el Coordinador de Grupo junto con el diligenciamiento del formato Solicitud Recursos Informáticos DIGSA.

d. 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; teniendo en cuenta el proceso que lo requiera. La destrucción segura se documentará mediante acta, registro fílmico y fotográfico.

10.3..1 Trabajo en Casa

Mediante Directiva Presidencial N° 2 del 12 de marzo de 2020 que trata sobre las" Medidas para atender la contingencia generada por el COVID-19, a partir del uso de tecnologías de la información y las telecomunicaciones – TIC". Se define, que como medida preventiva se pueda realizar trabajo en casa por medio del uso de las TIC, sin que constituya como modalidad de teletrabajo, descrito en el numeral 4 del artículo 6 de la Ley 1221 de 2008 "por el cual se establecen normas para promover y regular el teletrabajo". Por lo tanto, para el caso de la DIGSA se denomina "trabajo en casa". Esta actividad se realiza mediante conexión remota a los equipos de la Entidad, ya que la DIGSA no cuenta con la implementación de teletrabajo en términos definidos por la Ley 1221 de 2008.

Por lo anterior el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, determina las circunstancias y requisitos para la configuración de conexiones remotas a la plataforma tecnológica de la DIGSA; así mismo, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura. Cualquier funcionario, contratista o proveedor de la DIGSA, previamente autorizado por el Grupo de Tecnologías de la Información y las Comunicaciones (SISAM), que requiera tener acceso a la información de la Entidad desde redes externas, debe acceder remotamente mediante un proceso de autenticación y autorización de dirección IP pública; haciendo uso de conexiones seguras (https, VPN). La activación de la conexión remota debe ser debidamente solicitada, justificada y aprobada a través de un procedimiento formal y documentado. Lo anterior deberá

contemplar una solicitud previa, la cual debe ser justificada por el Coordinador de Grupo junto con el diligenciamiento del formato Solicitud Servicios Informáticos DIGSA

Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad.

El usuario con conexión remota se compromete a respetar la legislación en materia de protección de datos, las políticas de seguridad de la información de la DIGSA y a utilizar la información a la que tenga acceso, única y exclusivamente para cumplir con sus obligaciones para con la DIGSA.

10.4 Políticas de Control de Acceso[3]

10.4..1 Control de Acceso a los activos de Información

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. De igual forma, se propenderá por la autenticación mediante un único usuario a las diferentes aplicaciones y sistemas de información.

b. El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados, una vez diligenciado el formato solicitud de servicios informáticos DIGSA.

c. Las credenciales de acceso son de uso personal e intransferible.

d. Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la DIGSA, deberá estar autorizado por el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

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

f. Todo usuario que se cree para que un tercero ingrese o contratista, debe tener una fecha de vencimiento, 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 estará determinada por el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones y 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 laborar.

[3] NTC-ISO-IEC 27001 A.9

h. Los equipos de terceros que requieran acceder a las redes de datos de la DIGSA, deben cumplir un procedimiento de sanitización[4] informática antes de concedérseles dicho acceso.

i. Los equipos de contratistas y/o terceros que hayan sido autorizados para acceder de forma permanente a la red de datos de la DIGSA, solo podrán hacerlo una vez se haya cumplido con el procedimiento inicial de formateo inicial de discos duros y/o medios de almacenamiento y posteriormente deben permanecer dentro de las respectivas instalaciones hasta 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.

j. Los accesos a la red inalámbrica deberán ser autorizados por el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura de la DIGSA.

10.4..2 Control de la Administración de Contraseñas

a. La administración, asignación y entrega de las contraseñas a los usuarios deberá gestionarse con el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

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, así:

- Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas.
- Las contraseñas no se deberán registrar en papel, correo electrónico, archivos digitales
- Deberán tener como mínimo ocho (8) caracteres alfanuméricos sin repetición.
- Deben estar compuestas por: letras en mayúsculas, letras en minúsculas, números y símbolos especiales en cualquier combinación.
- Debe cambiarse obligatoriamente cada 60 días.

[4] 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 desclasificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.

- Después de tres (3) intentos no exitosos de ingreso de la contraseña el usuario se bloquea de manera inmediata y deberá esperar un tiempo determinado de cinco (5) minutos para volver a intentar, o solicitar el desbloqueo a través de la mesa de ayuda.

- Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que un funcionario que esté utilizando un usuario y contraseña que no le pertenece, teniendo en cuenta las políticas de seguridad de la información de la DIGSA, alertando sobre un posible incidente de seguridad.

10.4..3 Control de 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 solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueo.

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

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.

10.4..4 Control de Acceso a Terceros

a. 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 la DIGSA, se establecerán controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario a los permisos a otorgar.

b. 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.

c. El acceso de los terceros a la información o cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al Coordinador de Grupo. Este, junto con el Grupo Sistema Integral de Información-

Tecnologías de la Información y las Comunicaciones, aprobarán y autorizarán el acceso y uso de la información.

d. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplan 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 de información.
   - 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 auditoria por parte de la DIGSA.

10.5 Políticas de Seguridad Física y del Entorno[5]

a. Las áreas protegidas y centros de datos se resguardarán mediante el empleo de controles de acceso físico a fin de permitir el acceso solo al personal autorizado.

b. 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 de tomaran en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad de las instalaciones.

c. 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] NTC-ISO-IEC 27001 A.11

10.5..1 Control de Acceso Físico

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

b. Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación (carnet institucional) adoptado por la DIGSA, mientras permanezcan dentro de sus instalaciones.

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

d. 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.

h. El personal de vigilancia debe registrar en una bitácora el ingreso y retiro de todo equipo de cómputo (pc o portátil, mouse, teclado, cargador, etc), servidores, equipos activos de red o cualquier equipo electrónico; en caso de que estos equipos sean propiedad de la DIGSA deberán contar con autorización expresa del Grupo de Apoyo Administrativo y/o Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

i. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, debe controlar el ingreso a los centros de datos y centros de cableado de la DIGSA.

e. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, es responsable de mantener organizado e identificado el cableado en los racks de los centros de cableado y centro de datos.

f. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, debe mantener libre de objetos o elementos que no sean propios de la operación en el centro de datos y centros de cableado en la DIGSA.

10.5..2 Controles en Áreas Protegidas

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

a. No se debe consumir ni alimentos ni bebidas.

b. No se deben ingresar alimentos inflamables.

c. No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.

d. No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.

e. 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.

10.5..3 Controles de seguridad y Mantenimiento de los Equipos

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

b. La DIGSA 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 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 no autorizadas.

d. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, debe asegurar que la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se le 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 (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la DIGSA.

10.5..4 Seguridad de los Equipos Fuera de las Instalaciones

a. Los usuarios que requieran manipular los equipos fuera de las instalaciones de la DIGSA, deben velar por la protección de los mismos sin dejarlos desatendidos, comprometiendo la imagen o información institucional.

b. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la defensa y seguridad nacional, se deberá realizar

inmediatamente el respectivo reporte, teniendo en cuenta que puede ocasionar un incidente 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 DIGSA, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieran o que puedan poner en riesgo la información que contiene.

d. Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones de la DIGSA, deber ser debidamente identificado y registrado antes de conceder la autorización respectiva.

10.6 Políticas de Seguridad de las Operaciones[6]

10.6..1 Documentación de Procedimientos Operativos

a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de la 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 detallados 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 deber ser autorizada por el administrador de la aplicación, propietario del activo, coordinador de grupo 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 que hubiere lugar.

10.6..2 Control de Cambios Operativos

a. Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado y autorizado adecuadamente por parte del Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones, y

[6] NTC-ISO-IEC 27001 A.12

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 precedidos de la definición de requerimientos, especificaciones y controles. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

10.6..3 Control en la Segregación de Funciones

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.

10.6..4 Gestion de Capacidad

El Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones, como área responsable de la administración de la plataforma tecnológica de la DIGSA, deberá 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 Monitoreo Infraestructura Tecnológica de la DIGSA.

10.6..5 Control en la Separación de Ambientes

a. La DIGSA 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 propios o tercerizados, 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 propio o tercerizados, deberá ser controlado y gestionado.

c. Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción propios o tercerizados; 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 propio o tercerizado, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

e. El ambiente del sistema de pruebas propio o tercerizado, deberá emular el ambiente de producción lo más estrechamente posible.

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 propio o tercerizado y a cualquier usuario que no lo requiera para el desarrollo de su labor.

10.6..6 Protección contra Software Malicioso

a. Los sistemas operacionales y aplicaciones deberán actualizarse periódicamente.

b. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información propia y/o tercerizados, 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 propios o tercerizados, no deberán ser deshabilitados o desinstalados sin autorización del Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones 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 la DIGSA, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información institucional.

f. La DIGSA será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, pagina 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 institucional deberán ser revisados periódicamente, para verificar que no haya presencia de cogido malicioso.

10.6..7 Control de copias de Respaldo

a. Se debe asegurar que la información definida en conjunto con el Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones y las áreas responsables de la misma, y que se encuentra contenida en la plataforma tecnológica de la DIGSA, 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 de la DIGSA

b. 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.

c. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, establecerá los procedimientos explícitos de resguardo y recuperación de la información que incluya especificaciones acerca de sus traslado, frecuencia e identificación; así mismo, definirá conjuntamente con las dependencias los periodos de retención de dicha información.

d. 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.

10.6..8 Control de Registros (logs)

a. Tanto los sistemas de información de administración propia y/o tercerizados que manejan información crítica, como los dispositivos de procesamiento de red y seguridad informática, deberán generar registros de eventos 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.

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 al Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, teniendo en cuenta el procedimiento de Gestión de Incidentes de Seguridad de la DIGSA.

10.7 Políticas de Seguridad de Comunicaciones[7]

10.7..1 Control de 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.

[7] NTC-ISO-IEC 27001 A.13

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 Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones, será la responsable de validar a quién se le asignarán los servicios a través de redes inalámbricas.

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

10.7..2 Control de Computación en la Nube

La DIGSA podrá implementar servicios en la nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

10.7..3 Control de Intercambio de Información y Software

a. Todo funcionario o contratista 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 Coordinadores de Grupo y/o Área donde se encuentra la información que se requiere 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 y disponibilidad.

c. Los acuerdos de intercambio-confidencialidad deben 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.

d. 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.

- 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.

10.7..4 Control de Correo Electrónico Institucional

La asignación de una cuenta de correo electrónico de la Dirección General de Sanidad Militar, se suministra como herramienta de trabajo para cada uno de los funcionarios (personal de planta, prestación de servicios y otros terceros previa autorización) que la requieran para el desempeño de sus funciones; su uso se encuentra sujeto a las siguientes reglas:

1. La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas en la DIGSA.

2. Los mensajes y la información contenida en los buzones de correo institucional son de propiedad de la DIGSA. 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 consideran de la institución.

3. El tamaño de los buzones y mensajes de correo será determinado por el Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones.

4. Está prohibido el uso del correo electrónico institucional para los siguientes fines:

   a. Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no institucional 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 que promuevan actividades ilegales incluidos el lavado de activos.

   b. El envío de la información relacionada con la defensa y 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 Coordinador de Grupo y el Área de Sistema Integral de Información Tecnologías de la Información y las Comunicaciones.

   c. El envío de archivos adjuntos con extensiones .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 envío de este tipo de archivos deberá ser autorizado por el Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones.

   d. El envío masivo de mensajes corporativos deberá ser solicitado por el Coordinador de Grupo que lo requiera y debe contar con la aprobación del Grupo Sistema Integral de Información Tecnologías de la Información y las Comunicaciones.

5. Toda información que requiera ser transmitida fuera de la DIGSA, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar protegida en formatos no editables (PDF) y con mecanismos de seguridad (contraseñas). Solo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

6. Todo correo electrónico deberá respetar el estándar de formato e imagen institucional definido por la DIGSA y deberá contener al final del mensaje un texto en el que se contemplen mínimo los siguientes elementos:

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

   b. El mensaje sólo puede ser utilizado por la persona o dependencia a la cual está dirigido.

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

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

10.7..5 Acuerdos de Confidencialidad

Todos los funcionarios deben firmar el documento de confidencialidad denominado "Acta de Compromiso de Reserva, Seguridad y Calidad de la Información Personal Militar – Civil Planta y Civil Vinculado por Contrato o Convenio", el cual 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 donde se suscriban contratos con empresas que tengan acceso a la información y/o a los recursos de la DIGSA por medio de los documentos denominados "Acta Compromiso de Reserva Externos" y "Acuerdo de Confidencialidad Sector Defensa – Anexo C", los cuales deberán reflejarse en los respectivos contratos.

10.8 Políticas de Adquisición, Desarrollo y Mantenimiento de Sistemas[8]

1. La información pública producida por las Dependencias de la DIGSA, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.

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

[8] NTC-ISO-IEC 27001 A.14

3. La DIGSA 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 es responsable de la veracidad de la misma.

4. Toda la información publicada en el portal institucional o cualquier otro medio, deberá conta con la revisión y aprobación del Grupo de Planeación Estratégica Área Gestión del Cambio y Comunicaciones Estratégicas.

5. El Área de Tecnologías y Sistemas de Información, deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.

6. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones desarrollará y/o contratará el software requerido por la DIGSA; de manera coordinada con el Grupo que manifieste la necesidad del software.

7. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones establecerá las especificaciones técnicas, para la adquisición o contratación de sistemas de información, contemplando requerimientos de seguridad de la información.

8. Todo aplicativo informático o software debe ser aprobado por parte del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones

9. El Grupo Sistema Integral de Información-Tecnologías de la Información, será la única dependencia autorizada para realizar copia de seguridad del software original; cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

10. La instalación del software en los activos informáticos de la DIGSA, se realizará únicamente a través del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones.

11. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información de la DIGSA.

12. Para la adquisición y actualización de software, es necesario efectuar la solicitud al Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

13. El software que se adquiera a través de terceros, debe quedar licenciado a nombre de la Dirección General de Sanidad Militar. Se deben establecer los lineamientos para la supervisión y seguimiento a las actividades de desarrollo propio y/o tercerizado, los cuales

deben quedar inmersos en las cláusulas y/o especificaciones técnicas de los contratos a ejecutar por la DIGSA.

14. Se encuentra prohibido el uso e instalación de juegos en los computadores de la DIGSA.

15. Para el caso que se considere la tercerización del desarrollo de software, se establecerán los siguientes requerimientos:

    a. Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual.

    b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

    c. Procedimientos de certificación de la calidad y supervisión del trabajo llevado a cabo por el proveedor, que incluya la verificación del cumplimiento de los requerimientos de seguridad del software establecidos.

10.9 Política de Relación con Proveedores[9]

a. En los casos en que se requiera entregar información a proveedores, o que producto de la prestación del servicio deban acceder a la información y/o recursos de la DIGSA, se deben suscribir los documentos de confidencialidad y no divulgación de la información entre la DIGSA y los proveedores denominado "Acuerdo de Confidencialidad Sector Defensa – Anexo C" y el documento denominado "Acta Compromiso de Reserva Externos", los cuales deberán reflejarse en los respectivos contratos.

   La aplicación de los acuerdos de confidencialidad de la información con proveedores son responsabilidad de cada Dependencia de la DISGSA.

b. Se deberá divulgar las políticas y procedimientos de seguridad de la información de la DIGSA a los proveedores, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de acuerdo con las políticas y procedimientos de seguridad de la información.

c. Se deberá evaluar y aprobar de manera formal los accesos a la información de la DIGSA requeridos por terceras partes.

d. Se deberá establecer y monitorear las condiciones de conexión para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la DIGSA.

e. Se deberá establecer y monitorear las condiciones de seguridad física y ambiental de los terceros que prestan servicio a la DIGSA en sus propias instalaciones.

[9] NTC-ISO-IEC 27001 A.15

f. Se deberá monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de Confidencialidad de parte de los terceros proveedores de servicios.

10.10 Política de Gestión de Incidentes de Seguridad de la Información[10]

a. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, con el apoyo del Comando Conjunto Cibernético-CCOCI, se encargarán de identificar las vulnerabilidades técnicas de la infraestructura tecnológica de la DIGSA.

b. No se permite a los usuarios de los activos de información, sin la autorización expresa del Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos de las Fuerzas Militares, o la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.

c. Los administradores de las plataformas y sistemas de información propios y/o tercerizados, serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.

d. El Área de Seguridad de la Información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades y/o recomendaciones enviadas por el CCOCI, y que sean subsanadas por el Área de Infraestructura, Redes y Comunicaciones de la DIGSA, y/o terceros a través del supervisor.

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.

f. 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 Gestión de Incidentes de la DIGSA.

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

b. Se deberá establecer y mantener actualizado un directorio de las Entidades que puedan brindar respuesta y apoyo en caso de un incidente en la DIGSA.

c. Los resultados de las investigaciones que involucren a los funcionarios de la DIGSA, deberán ser informados a las áreas de competencia.

[10] NTC-ISO-IEC 27001 A.16

10.11 Política de Continuidad de Seguridad de la información[11]

La DIGSA debe contar con un Plan de Continuidad que asegure que la operación de los procesos críticos, podrán ser restaurados dentro de escalas de tiempo razonables, ante la ocurrencia de eventos no previstos o desastres naturales. Dicho plan deberá tener establecido la priorización para las fases de recuperación, los pasos a seguir cuando existan situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir y los procesos alternos que permitan continuar con el proceso de manera temporal.

10.12 Nivel de Cumplimiento[12]

El cumplimiento de las Políticas de Seguridad y Privacidad de la Información aplicarán para todos los servidores públicos, contratistas, proveedores y terceras partes que interactúen con los activos de información de propiedad de la entidad o en calidad de responsable, custodio o usuario. Si los parámetros aquí descritos se infringen la Dirección General de Sanidad Militar se reservará el derecho de tomar las medidas correctivas pertinentes las cuales pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

10.12.1 Derechos de Propiedad Intelectual

a. La DIGSA cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementará 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 cuente 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 la entidad, será de uso exclusivo de la DIGSA.

[11] NTC-ISO-IEC 27001 A.17
[12] NTC-ISO-IEC 27001 A.18

10.12.2 Privacidad y Protección de Información de Datos Personales

a. La DIGSA propenderá por la protección de los datos personales de los funcionarios, usuarios, proveedores y terceros de los cuales reciba y administre información en cumplimiento a la Ley 1581 de 2012.

b. Se establecerán los términos, condiciones y finalidades para las cuales la DIGSA, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla, hayan suministrado datos personales.

c. El Grupo Sistema Integral de Información-Tecnologías de la Información y las Comunicaciones, definirá e identificará los controles necesarios para proteger los datos personales almacenados en bases de datos o cualquier otro repositorio y se compromete a evitar su divulgación, alteración o eliminación sin la autorización requerida.

d. Todos los usuarios deben mantener reserva absoluta con respecto a la información de la DIGSA o de sus funcionarios que manejen información relevante o de importancia debido a sus funciones.

e. Se debe verificar la identidad de las personas, a quienes se les entregue información por teléfono, correo electrónico o certificado, entre otros.

11. Administración de las Políticas de la DIGSA

Las políticas de Seguridad de la Información se deben preservar en el tiempo y están sujetas a una revisión anual; en el evento de cambios estructurales que afecten a la Dirección General de Sanidad Militar, se debe asegurar que éstas se ajusten siempre a las necesidades del negocio.

La fecha de vigencia de las políticas de Seguridad de la Información será a partir de su aprobación por parte de la Alta Dirección.

Ante la necesidad de un cambio en las políticas de Seguridad de la Información y con el fin de contribuir a un mejoramiento continuo de las mismas, se deben comunicar los cambios realizados a todos los usuarios internos, externos, terceros y a quienes de manera directa o indirecta apliquen.

12. Bibliografía

Ministerio de las Tecnologías de la Información y Comunicaciones (2018). Manual de Gobierno Digital. Bogotá.

Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Modelo de Seguridad y Privacidad de la Información versión 3.0.2. Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. Política General de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones. Recuperado de https://www.mintic.gov.co/portal/604/articles62124_Politica_Seguridad_Privacidad_Informacion.pdf

Ministerio de las Tecnologías de la Información y Comunicaciones, Fortalecimiento de la Gestión TI en el Estado, https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Ministerio de Defensa Nacional (2014). Directiva Permanente DIR 2014-18. Políticas de Seguridad de la Información para el Sector Defensa. Bogotá

Ministerio de Defensa Nacional – Comando General de las Fuerzas Militares (2014). Directiva Permanente No. 154 /MDN-CGFM-JEMC-SEMCO-JEIMC-DIRCO-23.1. Políticas de Seguridad de la Información para las Fuerzas Militares. Bogotá

ISO/IEC/27001(2013). Sistema de Gestión de Seguridad de la Información. Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC, Bogotá D.C.