FUERZAS MILITARES DE COLOMBIA
ARMADA NACIONAL

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA

MANUAL
ARC T4-8.1.1
PÚBLICO

MANUAL DE SEGURIDAD DE LA INFORMACIÓN ARMADA NACIONAL

(MAN. SEG. INF. ARC)

PRIMERA EDICIÓN

2018

COPIA 001/100

FUERZAS MILITARES DE COLOMBIA
ARMADA NACIONAL

ARMADA NACIONAL
REPÚBLICA DE COLOMBIA
Protegemos el azul de la bandera

MANUAL
ARC T4-8.1.1
PÚBLICO

MANUAL DE SEGURIDAD DE LA INFORMACIÓN ARMADA NACIONAL

(MAN. SEG. INF. ARC)

PRIMERA EDICIÓN

2018

Gerente del Proyecto
Capitán de Navío DIANA MILENA ÁVILA HERNÁNDEZ

Comité Técnico Estructurador
Teniente de Corbeta JENNY ALEXANDRA VARGAS VARGAS
Asesor de Defensa 02 MARÍA BELÉN SICACHÁ RUÍZ

Comité de Validación
Vicealmirante BENJAMÍN CALLE MEZA
Contralmirante ANDRÉS VÁSQUEZ VILLEGAS
Contralmirante CAMILO HERNANDO GÓMEZ BECERRA
Capitán de Navío ÁLVARO JOSÉ CERMEÑO PETRO
Capitán de Navío NELSON MAURICIO QUEVEDO LEÓN
Capitán de Fragata MARCELA AGUILAR DEL VALLE
Capitán de Corbeta GIOVANNY MOJICA GONZÁLEZ

Dirección de Doctrina Naval
Capitán de Navío GERMÁN ALEXANDER SCOVINO GARZÓN
Suboficial Jefe JHONNY FRANCO SALCEDO

Diseño, diagramación e impresión
Fenix Media Group S.A.S

República de Colombia
Armada Nacional
Manual de Seguridad de la Información de la Armada Nacional, primera edición
2018
Dirección de Doctrina Naval
Bogotá, D.C. – Colombia
2018.

MINISTERIO DE DEFENSA NACIONAL

ARMADA NACIONAL

DISPOSICIÓN NÚMERO 06 **DEL**

(16 MAR 2018)

Por la cual se aprueba el "Manual de Seguridad de la Información Armada Nacional", primera edición 2018.

EL COMANDANTE DE LA ARMADA NACIONAL

En ejercicio de sus facultades legales y en especial las que le confieren los ordinales c y d del artículo 26 del Decreto No. 1605 del 8 de agosto de 1988 "Reglamento de Publicaciones Militares".

D I S P O N E:

ARTÍCULO 1°. Apruébese el "**MANUAL DE SEGURIDAD DE LA INFORMACIÓN ARMADA NACIONAL**", primera edición 2018, elaborado por el Comando de la Armada Nacional, el cual se identificará así:

MANUAL
ARC T4-8.1.1
PÚBLICO

PARÁGRAFO.- Las observaciones a que dé lugar la aplicación del Manual en referencia, deben ser presentadas al Comando de la Armada Nacional, con el fin de estudiarlas y tenerlas en cuenta para posteriores ediciones, conforme a lo establecido por el Reglamento de Publicaciones Militares.

ARTÍCULO 2°. El Comando de la Armada Nacional, dispondrá la edición del Manual aprobado en virtud de la presente disposición.

ARTÍCULO 3°. La presente disposición, rige a partir de la fecha de su expedición y deroga todas las disposiciones contrarias sobre la materia.

COMUNÍQUESE Y CÚMPLASE
Dada en Bogotá D.C. a los 16 MAR 2018

Almirante **ERNESTO DURÁN GONZÁLEZ**
Comandante Armada Nacional

CONTENIDO

CONTROL DE CAMBIOS 7
INTRODUCCIÓN 8

CAPÍTULO I 1-1

1. GENERALIDADES **1-1**
1.1. OBJETIVO Y ALCANCE **1-1**
1.1.1. Objetivo **1-1**
1.1.2. Alcance **1-1**
1.2. RESPONSABILIDAD DE LA DOCTRINA **1-1**
1.3. NORMAS Y DOCUMENTOS DE REFERENCIA **1-2**
1.4. TÉRMINOS Y DEFINICIONES **1-3**

CAPÍTULO II 2-1

2. MARCO REFERENCIAL Y MARCO JURÍDICO **2-1**
2.1. ANTECEDENTES **2-1**
2.2. MARCO JURÍDICO **2-2**
2.2.1. Alcance **2-2**
2.2.2. Ley 594 de 2000 ..... **2-2**
2.2.3. Ley 527 de 1999 ..... **2-2**
2.2.4. Ley 1221 de 2008 ..... **2-2**
2.2.5. Ley 1273 de 2009 ..... **2-2**
2.2.6. Ley 1581 de 2012 ..... **2-6**
2.2.7. Decreto 1377 de 2013 ..... **2-6**
2.2.8. Ley 1712 de 2014 ..... **2-7**

CAPÍTULO III 3-1

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN **3-1**
3.1. OBJETO Y CAMPO DE APLICACIÓN **3-1**
3.2. ESTRUCTURA DEL MANUAL **3-1**
3.3. CONTEXTO DE LA ORGANIZACIÓN **3-1**
3.3.1. Enfoque Basado en Procesos **3-2**
3.3.2. Alcance del SGSI **3-2**
3.4. LIDERAZGO **3-2**
3.4.1. Liderazgo y Compromiso de la Dirección **3-2**
3.4.2. Compatibilidad con Otros Procesos **3-2**

3.5. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 3-3
3.5.1. Evaluación de Riesgos de Seguridad de la Información 3-3
3.5.2. Tratamiento de Riesgos de la Seguridad de la Información 3-3
3.6. SOPORTE 3-4
3.6.1. Provisión de Recursos 3-4
3.6.2. Programas de Formación y Planes de Sensibilización 3-4
3.6.3. Toma de Conciencia 3-4
3.6.4. Comunicación 3-4
3.6.5. Información Documentada 3-4
3.7. OPERACIÓN DEL SGSI 3-5
3.8. CONTROLES 3-5
3.9. DECLARACIÓN DE APLICABILIDAD 3-5
3.10. EVALUACIÓN DEL DESEMPEÑO 3-5
3.10.1. Auditoría Interna 3-6
3.10.2. Revisión por la Dirección 3-6
3.11. MEJORA 3-6
3.11.1. No Conformidades de Seguridad de la Información 3-6
3.11.2. Mejora Continua 3-7

CAPÍTULO IV 4-1

4. OBJETIVOS DE CONTROL Y CONTROLES 4-1
4.1. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN 4-1
4.1.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información 4-1
4.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 4-5
4.2.1. Organización Interna 4-5
4.2.2. Dispositivos Móviles y Teletrabajo 4-24
4.3. SEGURIDAD DE LOS RECURSOS HUMANOS 4-26
4.3.1. Antes de Asumir el Empleo 4-26
4.3.2. Durante la Ejecución del Empleo 4-26
4.3.3. Terminación o Cambio de Empleo 4-28
4.4. GESTIÓN DE ACTIVOS 4-28
4.4.1. Responsabilidad por los Activos 4-28
4.4.2. Clasificación de la Información 4-43
4.4.3. MANEJO DE MEDIOS 4-44
4.5. CONTROL DE ACCESO 4-46
4.5.1. Requisitos del Negocio para Control de Acceso 4-46
4.5.2. Gestión de Acceso de Usuarios 4-51

4.5.3. Responsabilidades de los Usuarios **4-52**
4.5.4. Control de Acceso a Sistemas y Aplicaciones **4-54**
4.6. CRIPTOGRAFÍA **4-55**
4.6.1. Controles Criptográficos **4-55**
4.7. SEGURIDAD FÍSICA Y DEL ENTORNO **4-56**
4.7.1. Áreas Seguras **4-56**
4.7.2. Equipos **4-61**
4.8. SEGURIDAD DE LAS OPERACIONES **4-66**
4.8.1. Procedimientos Operacionales y Responsabilidades **4-66**
4.8.2. Protección Contra Códigos Maliciosos **4-69**
4.8.3. Copias de Respaldo **4-71**
4.8.4. Registro y Seguimiento **4-72**
4.8.5. Control de Software Operacional **4-73**
4.8.6. Gestión de Vulnerabilidad Técnica **4-74**
4.8.7. Consideraciones sobre Auditorías de Sistemas de Información **4-75**
4.9. SEGURIDAD DE LAS COMUNICACIONES **4-76**
4.9.1. Gestión de la Seguridad de las Redes **4-76**
4.9.2. Transferencia de Información **4-77**
4.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS **4-79**
4.10.1. Requisitos de Seguridad de los Sistemas de Información **4-79**
4.10.2. Seguridad en los Procesos de Desarrollo y Soporte **4-82**
4.10.3. Datos de Prueba **4-83**
4.11. RELACIÓN CON LOS PROVEEDORES **4-84**
4.11.1. Seguridad de la Información en las Relaciones con los Proveedores **4-84**
4.11.2. Gestión de la Prestación de Servicios con los Proveedores **4-86**
4.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN **4-87**
4.12.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información **4-87**
4.13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO **4-90**
4.13.1. Continuidad de Seguridad de la Información **4-90**
4.13.2. Redundancias **4-91**
4.14. CUMPLIMIENTO **4-92**
4.14.1. Cumplimiento de Requisitos Legales y Contractuales **4-92**
4.14.2. Revisiones de Seguridad de la Información **4-93**

REFERENCIAS BIBLIOGRÁFICAS **4-95**

CONTROL DE CAMBIOS

El control de cambios del presente Manual, se llevará a cabo por parte de la Dirección de Doctrina de la Armada Nacional, que garantizará su actualización permanente y distribución correspondiente a las Unidades de la Institución.

Esta parte se utilizará para incorporar las modificaciones al Manual, dando a conocer en qué parte específica del contenido se generó un cambio, la fecha, quién lo propone, la descripción y finalmente la versión.

Es pertinente recordar que los cambios sugeridos se hacen a través de la Jefatura responsable del proceso y siguiendo el procedimiento doctrinal que culmina con la firma del acto administrativo por parte del señor Comandante de la Armada Nacional.

VERSIÓN	FECHA	PÁGINA	PROPONENTE	DESCRIPCIÓN

INTRODUCCIÓN

El manual de seguridad de la información de la Armada Nacional, se constituye en una guía dentro de la implementación del sistema de gestión de seguridad de la información, el cual permitirá generar los cambios necesarios acordes a los avances tecnológicos y al mismo tiempo soportará la información de los procesos, como pilares de la gestión institucional. Debido a estos cambios, se incrementa el nivel de riesgos que hace necesario un constante mejoramiento en los sistemas de seguridad de la información en la Armada Nacional; para ello es primordial que se busque garantizar la protección de los activos de información institucionales, tanto de manera física o digital, enfocándonos en los pilares fundamentales que son: Confidencialidad, integridad y disponibilidad, minimizando así cualquier tipo de materialización del riesgo.

En el desarrollo de la estrategia se ha revisado el enfoque basado en procesos de la organización y se han definido los procedimientos documentados del Sistema de Gestión de Seguridad de la Información. De igual manera se han descrito los lineamientos para el manejo de un Sistema de Gestión de Seguridad de la Información (SGSI) en la institución basados en la norma Internacional ISO 2700:2013 la cual aplica la gestión de riesgos y brinda confianza a las partes interesadas en los riesgos gestionándolos de forma adecuada.

Por último la Armada Nacional ha reconocido la información como un activo vital por tanto en la política de seguridad de la información se establecen los controles necesarios a través del uso e implementación de estándares internacionales, con la participación del Alto Mando quienes lideran e integran la gestión asegurando que el SGSI logre los resultados previstos promoviendo la mejora continua.

CAPÍTULO I

1. GENERALIDADES

1.1. OBJETIVO Y ALCANCE

1.1.1. Objetivo

Establecer la política de seguridad de la información para el uso adecuado de los activos de información de la Armada Nacional, estableciendo una cultura y manejo de buenas prácticas para la aplicación y administración de controles del plan de mitigación de los riesgos.

1.1.2. Alcance

Este documento presenta los aspectos claves para la implementación del Sistema de Gestión de Seguridad de la Información en la Armada Nacional conforme a lo estipulado en la norma NTC – ISO/IEC 27001:2013. Por tal motivo se define un alcance para el sistema, la organización para un modelo de gestión y los aspectos para el establecimiento, implementación, operación y seguimiento del SGSI.

El alcance del Sistema de Gestión de Seguridad de la Información de la Armada Nacional de Colombia aplica a todos los activos de información que manejan todos los procesos de la Armada Nacional, son de obligatorio cumplimiento por parte de todos los funcionarios, contratistas y terceras partes que presten sus servicios a la Armada Nacional.

1.2. RESPONSABILIDAD DE LA DOCTRINA

La Dirección de Doctrina de la Armada Nacional es la responsable por la modificación y aprobación de los cambios que requiere el Manual: Dichos cambios deben ser presentados a la Dirección de Doctrina de la Armada Nacional en forma directa por la Jefatura de Operaciones Logística o por parte de cualquier miembro de la Institución o a través de ese conducto.

1.3. NORMAS Y DOCUMENTOS DE REFERENCIA

a. Constitución Política de Colombia de 1991.

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 "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".

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." vigente hasta el 4 de febrero de 2018.

j. Ley 1266 de 2008 "Por la cual se dictan disposiciones generales de habeas data y se regula el manejo de información".

k. Ley 1221 de 2008 "Teletrabajo".

l. Ley 1273 de 2009 "Protección de la información y de los Datos".

m. 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.

n. 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".

o. Decreto 1747 de 2000 "Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales".

p. Reglamento de Régimen Interno de la Armada Nacional.

q. Documento CONPES 3701 de julio del 2011 "Lineamientos de política para ciberseguridad y ciberdefensa".

r. DIR2014-18 Ministerio de Defensa del 19 de junio de 2014 "Políticas de seguridad de la información para el Sector Defensa".

s. Circular No. 233 MDN-CGFM-CARMAR-AYGAR-JAGCA-95.5 del 12 de diciembre de 2014 "Programa de Gestión Documental - PGD".

t. Directiva Permanente 001/MDN-CGFM-CARMA-SECAR-JINA-DICOI-23.1 del 12 de enero de 2017 "Directrices de Seguridad y Manejo de la Información Clasificada, Pública Reservada y Pública Clasificada de la Armada Nacional".

u. Manual de Contrainteligencia FF.MM. 2-6 Reservado.

v. Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la República de Colombia.

w. La ISO/IEC 27000, es referenciada parcial o total en el documento y es indispensable para su aplicación.

x. Norma Técnica Colombiana NTC – ISO/IEC 27005:2011 "Gestión del Riesgo de Seguridad de la Información".

y. Norma Técnica Colombiana NTC – ISO/IEC 31001:2011 "Gestión del Riesgo".

z. Norma Técnica Colombiana NTC – ISO/IEC 27001:2013 "Sistemas de Gestión de Seguridad de la Información - Requisitos".

aa. Ley 1862 de 2017 "Normas de Conducta del Militar Colombiano y se expide el Código Disciplinario Militar".

ab. Las demás normas vigentes aplicables.

1.4. TÉRMINOS Y DEFINICIONES

a. Activo de información: Cualquier bien que tiene valor para la organización [ISO/IEC 13335], por tanto debe protegerse. Puede ser información física como digital, entre los que podemos relacionar bases de datos, documentación, manuales, software, hardware, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado, también activos intangibles como la imagen y la reputación.

b. Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos en la seguridad de la información. [ISO/IEC Guide 73].

c. Ciberterrorismo: Ataque cibernético que emplea redes de ordenadores o comunicación para causar suficiente destrucción o interrupción para intimidar a una sociedad.

d. Confidencialidad: La propiedad vinculada con la seguridad de la información por la que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados. [ISO 13335-1].

e. Declaración de aplicabilidad: Declaración documentada que describe los objetivos de control y los controles que son

relevantes para el Sistema de Gestión de la Seguridad de la Información o SGSI de la organización y aplicables al mismo. Los controles del Sistema de Gestión de Seguridad de la Información o SGSI se basan en los resultados de la evaluación de riesgos de seguridad de la información (requisitos legales o reglamentarios, obligaciones contractuales y las necesidades de la organización en materia de seguridad de la información).

f. Delito Informático: Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos.

g. Disponibilidad: Vinculado con la seguridad de la información se refiere a la propiedad de ser accesible y utilizable por una entidad autorizada. [ISO 13335-1].

h. Evaluación de riesgos: El proceso general de análisis y estimación de los riesgos en la seguridad de la información. [ISO Guide 73].

i. Evento de seguridad de la información: La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información. [ISO/IEC TR 18044].

j. Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos de la seguridad de la información. [ISO/IEC Guide 73].

k. Incidente de seguridad de la información: Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información. (ISO 18044).

l. Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos. [ISO/IEC 13335-1].

m. Nube: Es un servicio de hospedaje que se presta a través de internet que se puede utilizar para enviar correo electrónico, editar documentos, ver películas o TV, escuchar música, jugar o almacenar imágenes y otros archivos. Las nubes pueden ser privadas, públicas o híbridas. Nube pública es la que vende servicios en Internet a cualquier usuario. Las nubes privadas son una red o centro de datos que pertenece a una organización y que ofrece servicios de hosting a un número limitado de personas. Las nubes híbridas combinan nubes públicas y privadas, enlazadas mediante tecnología que permite compartir datos y aplicaciones entre ellas.

n. Particionamiento: Es la acción de hacer la división o el repartimiento del disco duro.

o. Seguridad de la Información: La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio (ISO 17799).

p. Sistema de Gestión de la Seguridad de la Información (SGSI): La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión de la seguridad de la información o SGSI incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. Puede seguir los requisitos de la norma ISO 27001.

q. Tratamiento de riesgos de seguridad de la información: El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos de la seguridad de la información. [ISO/IEC Guide 73].

r. Web Service: Es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Permiten la interoperabilidad entre plataformas de distintos fabricantes por medio de protocolos estándar y abiertos.

CAPÍTULO II

2. MARCO REFERENCIAL Y MARCO JURÍDICO

2.1. ANTECEDENTES

La tecnología informática en el ámbito institucional de las Fuerzas Militares de Colombia, ha evolucionado desde un campo de computación personal y aislado, hasta campos avanzados de integración e interoperabilidad interinstitucional, con una amplia tendencia a la adquisición de equipos de tecnología abierta; por lo cual, nuevamente se observa una heterogeneidad de equipos y sistemas, que si bien mejoran la cobertura computacional y el rendimiento en la producción y oportunidad de la información, también incrementa el nivel de riesgos en la seguridad.

La disponibilidad creciente de herramientas informáticas en internet de libre uso, que explotan las vulnerabilidades de los diferentes sistemas de computación y que no requieren de niveles de conocimientos técnicos altos por parte de los atacantes; así como también, el creciente índice de delitos informáticos, acceso abusivo a los sistemas informáticos, fuga de información, ciberterrorismo y crimen informático, a nivel nacional y transnacional, amenazan y colocan en grave riesgo la seguridad informática y comprometen la Seguridad y Defensa del Estado; por lo cual, se requiere la implementación de controles proactivos y reactivos, para inferir en la probabilidad e impacto de los ataques y amenazas que pudiesen materializar los riesgos identificados.

Los diferentes casos de infiltración de sistemas, fuga de información, pérdida o robo de equipos de cómputo y ataques a las redes y sistemas de las Fuerzas Militares que se reportan continuamente, permiten demostrar la posesión y accesibilidad de las diferentes organizaciones al margen de la ley y de delincuentes comunes, a tecnologías de información con las cuales pueden llevar a cabo actividades ilícitas contra los recursos informáticos, afectando la confidencialidad, integridad y disponibilidad de los mismos, así como la imagen institucional.

2.2. MARCO JURÍDICO

2.2.1. Alcance

La presente Doctrina se enmarca dentro de los lineamientos y cumplimiento de las normas constitucionales sobre la materia, en especial lo establecido en la Ley 527 de 1999, Ley 1273 de 2009, Ley 1581 de 2012, Decreto 1377 de 2013 y Ley 1712 de 2014 y regirá para todas las Jefaturas, Comandos y Unidades Mayores y Menores de la Armada Nacional.

2.2.2. Ley 594 de 2000

Por medio de la cual se dicta la ley general de archivos y se dictan otras.

2.2.3. Ley 527 de 1999

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.

2.2.4. Ley 1221 de 2008

Tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).

2.2.5. Ley 1273 de 2009

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "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".

Artículo 1. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPÍTULO PRIMERO

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se

aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPÍTULO SEGUNDO

De las atentados informáticos y otras infracciones.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un

tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Articulo 58. CIRCUNSTANCIAS DE MAYOR PUNIBILIDAD. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

2.2.6. Ley 1581 de 2012

Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

2.2.7. Decreto 1377 de 2013

Este decreto se generó con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 donde se reglamenta aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de

información, las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales, este último tema referido a la rendición de cuentas.

2.2.8. Ley 1712 de 2014

El objeto de esta ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

CAPÍTULO III

3. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para la Armada Nacional y están influenciados por las necesidades y objetivos de la institución, los requisitos de seguridad, los procesos institucionales y estructura de gestión total de la información, teniendo en cuenta la seguridad de la información en el diseño de procesos, sistemas de información y controles.

3.1. OBJETO Y CAMPO DE APLICACIÓN

Este manual presenta los requisitos básicos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.

3.2. ESTRUCTURA DEL MANUAL

Este documento de política se divide en dos partes, y guarda la siguiente estructura:

Dos capítulos introductorios de conceptos generales, el presente Capítulo III Sistema de Gestión de Seguridad de la Información establecimiento de la evaluación y tratamiento de los riesgos y el capítulo IV objetivos de control y controles donde se definen los catorce dominios, 35 objetivos de control y 114 controles de acuerdo a lo estipulado en la norma ISO27001 Versión 2013.

3.3. CONTEXTO DE LA ORGANIZACIÓN

La Armada Nacional debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información.

La identificación, valoración y administración del riesgo se realiza determinando las causas y efectos, con base en el contexto interno, externo y del proceso dentro de la

Armada Nacional, que puede afectar el logro de los objetivos y la misión Institucional.

3.3.1. Enfoque Basado en Procesos

El Sistema de Gestión de Seguridad de la Información, tendrá un enfoque basado en procesos. Se incorpora a la organización mediante la adopción de un modelo PHVA que define las etapas de establecimiento, implementación, operación, seguimiento, mantenimiento y mejora del sistema frente a la seguridad de la información.

3.3.2. Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información de la Armada Nacional de Colombia, aplica a todos los activos de información que manejan todos los procesos de la Armada Nacional, son de obligatorio cumplimiento por parte del personal militar y no uniformados, contratistas y terceras partes, que presten sus servicios a la Armada Nacional.

3.4. LIDERAZGO

3.4.1. Liderazgo y Compromiso de la Dirección

La línea de mando de la Armada Nacional está comprometida con la Seguridad de la información al adoptar integralmente los principios de esta, enunciados en la norma ISO 27001:2013, los compromisos se encuentran establecidos en los Roles y Responsabilidades para la Seguridad de la Información en el Capítulo IV de éste manual.

3.4.2. Compatibilidad con Otros Procesos

El Sistema de Gestión de Seguridad de la Información definido en la norma ISO 27001 se encuentra alineado con la NTC-ISO 9001:2015, con el fin de apoyar la implementación y operación, consistente e integrada y garantiza el coexistir con otros sistemas de gestión relacionados que se vayan adoptando en la Armada Nacional.

3.5. PLANIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las etapas definidas para el desarrollo y la implementación del Sistema de Gestión de Seguridad de la Información son:

a. Fase de Diagnóstico donde se pretende identificar el estado actual de la Armada Nacional, con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, se realiza a través del diligenciamiento de la herramienta de diagnóstico proporcionado por la estrategia de gobierno en línea.

b. Fase de Planificación, donde se define la política de seguridad de la información y los procedimientos, se establecen los roles y responsabilidades, gestión de activos y riesgos y plan de comunicaciones.

c. Fase de Implementación, documentos con el plan de tratamiento de riesgos y la declaración de aplicabilidad e indicadores de seguridad de la información.

d. Fase de evaluación de desempeño.

3.5.1. Evaluación de Riesgos de Seguridad de la Información

La Armada Nacional establece una metodología para la Administración y Gestión del Riesgo, fundamentada y alineada con el Departamento Administrativo de la Función Pública (DAFP), Modelo Estándar de Control Interno (MECI), Estatuto Anticorrupción y la NTC-ISO 31000:2011.

Los riesgos de seguridad de la información están enmarcados en este sistema y estructuran para cada uno de los procesos de la Armada Nacional.

3.5.2. Tratamiento de Riesgos de la Seguridad de la Información

Después de efectuar los análisis de riesgos el comité de seguridad de la información junto con cada una de las áreas involucradas debe efectuar un plan de tratamiento de riesgos, para los riesgos considerados como críticos en los activos bajo su responsabilidad.

Los planes de tratamiento de riesgos deben ser registrados a través del Sistema de Administración de Riesgos de la Armada Nacional, de acuerdo al procedimiento de identificación y tratamiento de riesgos.

3.6. SOPORTE

3.6.1. Provisión de Recursos

El Responsable de Seguridad de la Información en cada uno de los procesos, debe gestionar todos los recursos necesarios para que la implementación de los controles se realice con base en el plan de tratamiento de riesgos definidos.

3.6.2. Programas de Formación y Planes de Sensibilización

Los programas de formación y sensibilización se definirán, revisarán y ejecutarán de acuerdo a las necesidades del Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información.

3.6.3. Toma de Conciencia

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de: la política de la seguridad de la información, su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información.

3.6.4. Comunicación

Las acciones de mejora se deben comunicar a todas las partes interesadas, con un nivel de detalle apropiado a las circunstancias, en donde sea pertinente llegar a acuerdos sobre los cursos de acción.

3.6.5. Información Documentada

El Sistema de Gestión de la Seguridad de la Información de la Armada Nacional incluye la información documentada a través del Sistema de Suite Visión Empresarial, con los estándares establecidos para el manejo de documentación de la institución, garantizando de esta manera que la información se pueda actualizar fácilmente y esté disponible cuando se requiera.

3.7. OPERACIÓN DEL SGSI

El Responsable y Administrador de Seguridad de la Información con el apoyo de los responsables de los procesos Institucionales, es quien coordina y da dirección a la Operación del Sistema de Gestión de Seguridad de la Información en la Armada Nacional, a través de la realización de las diferentes actividades de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema, que se encuentran relacionados en el plan de trabajo implementación del sistema de gestión de seguridad de la información.

3.8. CONTROLES

El Manual de Seguridad de la Información de la Armada Nacional esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología pueden consultar los procedimientos a través de la suite visión empresarial de la Armada Nacional (suiteve).

3.9. 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 la entidad, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros, puede ser consultada a través de la suite visión empresarial de la Armada Nacional (suiteve).

3.10. EVALUACIÓN DEL DESEMPEÑO

En la definición del Modelo PHVA, la fase de seguimiento y revisión hacen parte de las etapas de Verificar, donde se establecen los aspectos a ser desarrollados por los

responsables del sistema de gestión de seguridad de la información (SGSI) en todos los niveles, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema vs. la política, objetivos y experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones.

La Armada Nacional debe revisar el SGSI a intervalos planificados para asegurarse de su convivencia, adecuación, eficacia y mejora continua.

3.10.1. Auditoría Interna

La Dirección de Inspecciones de la Armada Nacional desarrollará las auditorías internas a intervalos planificados, a fin de proporcionar información del Sistema de Gestión de Seguridad de la Información.

a. Se debe planificar, establecer, implementar y mantener uno o varios programas de auditoría.

b. Definir criterios y alcance.

c. Seleccionar los auditores.

d. Asegurarse de que los resultados de las auditorías se informen de acuerdo a lo establecido en el procedimiento de inspecciones código EVALIND-PT-001-IGAR-V01, de la Inspección General de la Armada Nacional.

3.10.2. Revisión por la Dirección

La Armada Nacional efectuará las actualizaciones a que haya lugar del SGSI a intervalos planificados, a fin de asegurar su convivencia, adecuación, eficacia y mejora continua.

3.11. MEJORA

3.11.1. No Conformidades de Seguridad de la Información

La Armada Nacional mantendrá registros de aquellos eventos o comportamientos que van en contra de lo establecido en los requerimientos para la implementación, operación y mantenimiento del SGSI.

3.11.2. Mejora Continua

La Armada Nacional debe mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.

CAPÍTULO IV

4. OBJETIVOS DE CONTROL Y CONTROLES

4.1. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

4.1.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información

OBJETIVO:

Brindar orientación y apoyo en la implementación de la seguridad de la información de acuerdo con los requisitos de la Armada Nacional y con las leyes y reglamentos, vigentes.

POLÍTICAS:

a. Políticas Generales para la seguridad de la información

La Armada Nacional de Colombia, se compromete a preservar la confidencialidad, integridad y disponibilidad de la información misional de acuerdo a las disposiciones legales, técnicas y a sus responsabilidades contra amenazas internas y externas.

La información es un activo principal imprescindible para la Institución, para la protección de los activos de información, la implementación del SGSI y el apoyo, generación y publicación de sus políticas, procedimientos e instructivos, como herramienta fundamental para la continuidad del negocio, implementando buenas prácticas en la gestión de riesgos, mediante el fortalecimiento de la capacidad Institucional y la toma de decisiones eficientes y seguras.

b. Objetivos de la Política de Seguridad de la Información

La Armada Nacional, para el cumplimiento de su misión, visión, objetivos estratégicos, y apegado a

los valores corporativos, establece la función de seguridad de la información en la entidad, con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los colombianos y funcionarios, en la Armada Nacional.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información y comunicaciones.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios y terceros, que tengan relación con la Armada Nacional y la ciudadanía en general.
- Garantizar la continuidad del negocio frente a incidentes de seguridad.

c. Visión General

En la Armada Nacional es de vital importancia impartir las instrucciones para la actualización, desarrollo,aplicación,cumplimiento y supervisión de las políticas de seguridad de la información que deben seguir el personal militar y no uniformado, contratistas y cualquier persona que tenga relación con la Institución o que tenga acceso a sus activos de información, se aplica a todos los procesos, con el fin de proteger la información. El compromiso con el Sistema de Gestión de Seguridad de la Información es el de establecer un marco de confianza en el ejercicio de los deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión institucionales.

d. Propósito

Preservar los principios de confidencialidad, integridad y disponibilidad de la información para fortalecer la continuidad de las actividades operacionales, administrativas y logísticas, protegiendo adecuadamente la información, reduciendo los riesgos, optimizando el empleo de las tecnologías de información.

e. Políticas Específicas de Seguridad de la Información

La Armada Nacional ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

La Armada Nacional protegerá la información generada, procesada o resguardada por los procesos y activos de información que hacen parte de los mismos.

La Armada Nacional protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

La Armada Nacional protegerá su información de las amenazas originadas por parte del personal interno y externo.

La Armada Nacional protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La Armada Nacional controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

La Armada Nacional implementará control de acceso a la información, sistemas y recursos de red.

La Armada Nacional garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La Armada Nacional garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.

La Armada Nacional garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La Armada Nacional garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

f. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de las políticas.

g. Revisión de las Políticas para Seguridad de la Información

Las políticas de seguridad de la información se revisarán periódicamente mínimo una vez al año, o antes, en caso de producirse cambios tecnológicos, impacto de incidentes de seguridad, auditorias y cambios en la estructura organizacional.

4.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.2.1. Organización Interna

OBJETIVO:

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la institución.

POLÍTICAS:

a. Roles y Responsabilidades para Seguridad de la Información

- **Roles para Seguridad de la Información**
  - **CEO (Comandante)**

    El CEO (Chief Executive Officer). Es el COMANDANTE DE LA ARMADA NACIONAL, el cargo más alto dentro del organigrama de la organización. Es el responsable final de las acciones que se lleven a cabo dentro de la institución, de su desempeño y su eficiencia.

    El CEO tiene una importante relación con el CIO, debido a que las estrategias de la institución están estrechamente ligadas al ámbito de las tecnologías de la información.

  - **CIO**

    El CIO (Chief Information Officer), es el Director de Tecnologías de Información y Comunicaciones. Reporta al CEO, y se encarga básicamente que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados.

  - **Comité de Dirección del Sistema de Gestión de Seguridad de la Información (CDSGSI)**

    Está conformado por los encargados de los procesos de la Armada Nacional.

  - **Comité de Gestión del Sistema**

de Gestión de Seguridad de la Información

Por cada proceso de la Armada Nacional los dueños de los procesos y jefes de jefatura designarán al personal que participará dentro de este comité, su objetivo es: asegurar que exista la dirección y apoyo gerencial para establecer, implementar y monitorear las estrategias de Seguridad de la Información que requiera la entidad. La División de Informática de la Armada Nacional será la secretaría técnica del comité, responsable de convocar y dinamizar el funcionamiento de este comité.

- **Responsable de Seguridad de la Información**

  Supervisa el cumplimiento de la Política de Seguridad de la Información y el presente manual y asesora en materia de seguridad de la información a las dependencias y unidades de la Armada Nacional que así lo requieran.

- **Administrador de Seguridad**

  Asesora al Responsable de Seguridad de la Información en cuanto a Seguridad de la información.

- **Oficial de Seguridad de la Información**

  Se encarga de hacer cumplir la Política de Seguridad de la Información y el presente manual y asesora en materia de Seguridad de la Información en las respectivas Escuelas de Formación, Bases, y Brigadas, quienes deben mantener el contacto con el OSGSI de la Armada Nacional quien coordina con JINA. El OSI de cada Unidad debe ser un militar activo preferiblemente con el perfil de ingeniero o tecnólogo en sistemas, electrónico y telecomunicaciones.

- **Vigía de Seguridad de la Información**

  Se encarga de hacer cumplir la Política de Seguridad de la Información y el presente

manual y asesora en materia de Seguridad de la Información en las respectivas en los respectivos Batallones, Capitanías de Puerto, Unidades Terrestres y a Flote, quienes mantendrán contacto con el OSI de cada Fuerza, Base o Brigada, con el OSGSI de la Armada Nacional quien coordina JINA. El Vigía de Seguridad de la Información de cada Unidad debe ser un militar activo, preferiblemente con el perfil de ingeniero o tecnólogo de sistemas, electrónico, telecomunicaciones, o con habilidades y competencias en el área de sistemas o comunicaciones, quienes deberán fortalecer día a día sus conocimientos en este campo ya sea de manera autodidacta o con apoyo educativo de la Institución.

- **Dirección de Inspecciones de la Armada Nacional**

  Realiza la Auditoría al Sistema de Gestión de Seguridad de la Información.

- **Custodio**

  Es el responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentren bajo su administración.

- **Usuario o propietario**

  Verifica la integridad de la información institucional y vela porque se mantenga la disponibilidad y confiabilidad de la misma.

- **Deberes y Responsabilidades para la Protección de la Información de la Armada Nacional**

  Las responsabilidades de seguridad de la información están definidas y asignadas de acuerdo a la clasificación dada a la información.

- **CEO (Comandante)**

  Su función principal es la de supervisar y velar porque la estrategia definida en la institución cumpla con la consecución de los objetivos de la organización, además de sembrar los principios y pilares básicos a seguir dentro de la Armada Nacional.

- **CIO (Director de Tecnologías de Información y Comunicaciones)**

  Se encarga de mejorar los procesos de tecnologías de la información de la organización, gestionar el riesgo y la continuidad de negocio a nivel de tecnología, controlar el coste en infraestructura de tecnologías de la información, alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos.

- **Líderes de Procesos Institucionales o Jefes de Jefatura**

  Conformar el Comité de Dirección del Sistema de Gestión de Seguridad de la Información (CDSGSI), quienes tendrán las máximas responsabilidades y aprobarán las decisiones de alto nivel relativas al sistema y participan activamente en las reuniones que sean convocadas.

  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.

  Designar al personal que participará en el CSGSI que maneja el Sistema Administrador del Riesgo (SAR).

- **Responsable de Seguridad de la Información (OSGSI)**
  - Generar e implementar políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información.
  - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de la implantación de las medidas de seguridad.
  - Garantizar la seguridad y privacidad de los datos.
  - Supervisar la administración del control de acceso a la información.
  - Supervisar el cumplimiento normativo de la seguridad de la información.
  - Supervisar la arquitectura de seguridad de la información de la Armada Nacional.
  - Asegurar el buen funcionamiento del proceso de seguridad de la información de la Unidad. Éste debe ser el punto de referencia para todos los procesos de seguridad, teniendo la capacidad de guiar y asesorar a los usuarios de la Unidad sobre cómo desarrollar procedimientos para la protección y manejo de los activos de información.
  - Apoyar a los OSI ante incidentes de seguridad mediante un plan de respuesta, con el fin de atender rápidamente este tipo de eventualidades.
  - Coordinar la realización periódica de revistas a las prácticas de seguridad informática e información.
  - Realizar verificación a los activos de información para prevenir el impacto de los riesgos derivados de la posible pérdida de la integridad, confidencialidad y disponibilidad de la información.
  - Difundir el directorio consolidado de los OSI de las unidades de la Armada Nacional.

- Supervisar que la información que requiera ser transportada, solo podrá realizarse en medios de almacenamiento cifrados, previa autorización del Jefe de la dependencia y visto bueno del OSI de la Unidad.
- Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las redes de datos y a la información de las diferentes unidades de la Armada Nacional.
- Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad, en el desarrollo de los planes de recuperación de desastres y planes de continuidad de tecnología.
- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la Armada Nacional. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de la información.

– **Comité de Gestión del Sistema de Seguridad de la Información**

- Asignar responsables, tareas, actividades y toma de decisiones en cuanto a seguridad se refiere, respaldado por el Comandante, siempre buscando la mejora continua del SGSI.
- Definir, estructurar, recomendar, hacer seguimiento y mejorar el SGSI de la Institución.
- Revisar, aprobar y actualizar las políticas y estándares del SGSI.
- Evaluar la efectividad de las medidas tomadas.
- Elaborar un plan de formación y de sensibilización para el SGSI.

- Presupuestar los recursos necesarios para el SGSI.
- Planificar auditorías internas periódicas del SGSI.
- Planificar un análisis y evaluación de riesgos de la información para la Armada Nacional, mínimo una vez al año.
- Implementar, difundir, evaluar, sancionar y validar jurídicamente las medidas de seguridad.
- Verificar el estado del plan de tratamiento de riesgos.
- Reportar al Comandante sobre eventos e incidentes de seguridad.
- Reunirse cuando se requiera, con la finalidad de verificar, evaluar y tener control del cumplimiento de las responsabilidades asignadas.

– **Administrador de Seguridad**

- Asesorar al Responsable de Seguridad de la Información de la institución.
- Proponer, documentar e implementar las políticas, normas y procedimientos de seguridad informática.
- Promover el cumplimiento de las políticas de seguridad de la información para los funcionarios y terceros, cuando aplique.
- Definir controles de seguridad y accesos a las redes locales y a la red de transmisión de datos de la armada nacional, con el fin de garantizar la seguridad perimetral, integridad de los datos almacenados en la infraestructura tecnológica de la Armada Nacional.
- Proyectar los planes de contingencia, mantenimiento y seguridad requeridos para salvaguardar y mantener el correcto funcionamiento de las redes de comunicación de datos de la Armada.
- Aplicar conocimientos, habilidades,

herramientas y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

- Identificar la brecha entre el modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del modelo de seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Encarrilar el proyecto hacia el cumplimiento de la implementación del modelo de seguridad y privacidad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Capacitar en las políticas de Seguridad de Información impartidas por la Armada Nacional al personal antes de asumir un cargo en la Institución, efectuando las coordinaciones necesarias con los OSI o Gestores de S.I. quienes replicarán lo pertinente en sus Unidades.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.

- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.
- Apoyar al Responsable de Seguridad de la información en la gestión de riesgos de seguridad sobre la gestión de TI y de información de la Armada Nacional.

– **Propietarios de la Información y/o líderes de los Procesos**
  - Implementar las políticas de SGSI a la información digital y física que reposa en el archivo central, de igual manera incluir dentro de sus charlas de sensibilización el adecuado manejo para el cumplimiento de las Políticas de Seguridad de la Información.
  - Estructurar el plan de continuidad para el archivo central de acuerdo a los lineamientos de la normatividad vigente.
  - Clasificar los activos de información tanto físicos como digitales 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.
  - Definir el protocolo para la recuperación de los activos físicos, de información y sistemas críticos en caso de ocurrencia de un incidente informático o en caso de desastre, e identificar el impacto que ocasiona el estar fuera de servicio por un lapso de tiempo determinado.

- Definir el plan de continuidad y de recuperación en caso de desastre para el proceso en el adecuado manejo de la información en coordinación con el OSGSI.
- Coordinar con el OSI de la Unidad y el OSGSI de la Armada Nacional 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.
- Comunicar los requerimientos de seguridad de la información al área correspondiente, los cuales deben estar avalados por el OSI de la Unidad.
- Determinar y autorizar los privilegios necesarios de acceso a los activos de información, de acuerdo al cargo desempeñado.
- Comunicar al área correspondiente sus requerimientos en capacitación sobre seguridad de información.
- Revisar los registros y reportes de auditoría para asegurar el cumplimiento con las restricciones de seguridad en 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.
- 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.

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

– **Oficial de Seguridad de la Información Unidades (OSI)**

- Asegurar el buen funcionamiento del proceso de seguridad de la información de la Unidad, debe ser el punto de referencia para todos los procesos, teniendo la capacidad de guiar y asesorar a los usuarios de la Unidad sobre cómo desarrollar procedimientos para la protección y manejo de los activos de información.
- Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales, de igual forma poner en conocimiento del OSGSI de la Armada Nacional quien coordina con JINA; con el fin de efectuarse el correspondiente análisis y recomendaciones para neutralizar futuros incidentes similares.
- Coordinar la realización periódica de revistas a las prácticas de seguridad informática e información, las cuales deben ser reportadas al OSGSI de la Armada Nacional, con copia a JINA.
- Proponer y coordinar la realización de un análisis formal de riesgos en seguridad de la información que abarque la unidad a la cual pertenece.
- Emitir respuesta oportuna en coordinación con el área de Contrainteligencia de la unidad para dar cumplimiento al Plan de Contrainteligencia anual, con respecto a temas de seguridad informática y de la información.

- Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
- Capacitar en las políticas de Seguridad de Información impartidas por la Armada Nacional en su unidad al personal antes de asumir un cargo en la Institución.
- Realizar verificación a los activos de información para prevenir el impacto de los riesgos derivados de la posible pérdida de la integridad, confidencialidad y disponibilidad de la información.
- Prevenir la pérdida, daño, robo o puesta en riesgo de los activos y la interrupción de los servicios informáticos de la Armada Nacional para garantizar la confiabilidad, integridad y disponibilidad de la información.
- Realizar revistas de verificación aleatorias a los activos documentales, informáticos y dispositivos de almacenamiento, para detectar el retiro no autorizado de información, en caso de hallar alguna novedad deberá reportar de forma inmediata a la JINA y al OSGSI de la Armada Nacional, relacionando las acciones inicialmente tomadas.
- Supervisar que los equipos de la infraestructura tecnológica de las unidades y dependencias de la Armada Nacional estén ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.
- Verificar que los funcionarios, contratistas y terceros velen 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.

- Verificar que los equipos y máquinas de copiado, impresoras y máquinas de fax estén ubicados en zonas de acceso restringido y se permita su uso a personal autorizado.
- Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las redes de datos y a la información de las diferentes unidades de la Armada Nacional.
- Coordinar con los administradores de los activos informáticos de las unidades, para 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.
- Controlar que los activos informáticos personales de los miembros de la institución que residen a bordo de la Unidad y los alumnos de las escuelas de formación, sean sometidos a las mismas condiciones de seguridad y reserva de la información y sólo puedan ingresar a las áreas de bienestar social, alojamientos, viviendas fiscales y aulas de estudio; de igual forma el propietario del activo deberá firmar la declaración de aceptación y compromiso de cumplimiento de las políticas de seguridad de la información de la Institución, además registrar estos activos, en una minuta de ingreso y salida de la Unidad.

- Verificar cambios en direccionamiento IP y cargos de personal en los meses de julio y enero de cada año con el fin de actualizar los permisos establecidos en los formatos de seguridad de la información.
- Coordinar con la maestría de armas de su unidad para que se dé cumplimiento al visto bueno del OSI dentro de los ceses de traslado y definitivo del personal, a fin que sean cerrados los servicios informáticos que ya no se requieran a los usuarios.

– **Vigía de Seguridad de la Información Unidades (VIGIA)**

- Asegurar el buen funcionamiento del proceso de seguridad de la información de la Unidad, debe ser el punto de referencia para todos los procesos, teniendo la capacidad de guiar y asesorar a los usuarios de la Unidad sobre cómo desarrollar procedimientos para la protección y manejo de los activos de información.
- Atender y responder inmediatamente las notificaciones de sospecha de un incidente de seguridad o de incidentes reales, de igual forma poner en conocimiento del OSI de la unidad, OSGSI de la Armada Nacional y JINA; con el fin de efectuarse el correspondiente análisis y recomendaciones para neutralizar futuros incidentes similares.
- Coordinar la realización periódica de revistas a las prácticas de seguridad informática e información, las cuales deben ser reportadas al OSGSI de la Armada Nacional, con copia a JINA.
- Proponer y coordinar la realización de un análisis formal de riesgos en seguridad de la información que abarque la unidad a la cual pertenece.

- Emitir respuesta oportuna en coordinación con el área de Contrainteligencia de la unidad para dar cumplimiento al Plan de Contrainteligencia anual, con respecto a temas de seguridad informática y de la información.
- Participar en la resolución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.
- Capacitar en las políticas de Seguridad de Información impartidas por la Armada Nacional en su unidad al personal antes de asumir un cargo en la Institución.
- Realizar verificación a los activos de información para prevenir el impacto de los riesgos derivados de la posible pérdida de la integridad, confidencialidad y disponibilidad de la información.
- Prevenir la pérdida, daño, robo o puesta en riesgo de los activos y la interrupción de los servicios informáticos de la Armada Nacional para garantizar la confiabilidad, integridad y disponibilidad de la información.
- Realizar revistas de verificación aleatorias a los activos documentales, informáticos y dispositivos de almacenamiento, para detectar el retiro no autorizado de información, en caso de hallar alguna novedad deberá reportar de forma inmediata a la JINA y al OSGSI de la Armada Nacional, relacionando las acciones inicialmente tomadas.
- Supervisar que los equipos de la infraestructura tecnológica de las

unidades y dependencias de la Armada Nacional estén ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

- Verificar que los funcionarios, contratistas y terceros velen 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.
- Verificar que los equipos y máquinas de copiado, impresoras y máquinas de fax estén ubicados en zonas de acceso restringido y se permita su uso solo a personal autorizado.
- Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las redes de datos y a la información de las diferentes unidades de la Armada Nacional.
- Coordinar con los administradores de los activos informáticos de las unidades, para 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.
- Controlar que los activos informáticos personales de los miembros de la institución que residen a bordo de la Unidad y los alumnos de las escuelas de formación, sean sometidos a las mismas condiciones de seguridad y reserva de la información y sólo puedan ingresar a las áreas de bienestar social, alojamientos, viviendas fiscales y aulas de estudio; de igual forma el propietario del activo deberá

firmar la declaración de aceptación y compromiso de cumplimiento de las políticas de seguridad de la información de la Institución, además registrar estos activos, en una minuta de ingreso y salida de la Unidad.

- **Custodio de información**
  - Administrar accesos a nivel de red (sistema operativo).
  - Administrar accesos a nivel de bases de datos.
  - Administrar los accesos a archivos físicos de información almacenada en medios magnéticos (diskettes, cintas), ópticos (cd's) o impresa.
  - Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas (service packs, fixes, etc.).
  - Desarrollar procedimientos de autorización y autenticación.
  - Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.
  - Investigar brechas e incidentes de seguridad.
  - Entrenar a los empleados en aspectos de seguridad de información en nuevas tecnologías o sistemas implantados bajo su custodia.
  - Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.
- **División de Informática**
  - Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
  - Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes

sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.

- Realizar el monitoreo a las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la Institución.
- Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del Estado Colombiano.

– **Responsables de la Seguridad de la Información**

- Organismos y dependencias de Contrainteligencia orgánicos de las unidades a Flote y en Tierra de la Armada Nacional, que orientan y controlan el cumplimiento de las medidas para la seguridad de la información que se procesa, difunde y almacena en todas las dependencias de la Armada Nacional.
- Los funcionarios de la Armada Nacional son los directos responsable de la protección de la información que procesan, difunden y almacenan teniendo en cuenta las funciones de su cargo.
- El Comité de Seguridad de la Unidad emite normas de seguridad interna y verifica el cumplimiento de las políticas de seguridad establecidas por el mando; éste comité deberá ser conformado por el Comandante de la Unidad, oficial de operaciones, oficial de inteligencia, jefe de contrainteligencia,

oficial de seguridad, oficial de seguridad informática y suboficial custodio.

b. Separación de Deberes

Todas las personas que tengan acceso a la infraestructura tecnológica o a sistemas de información de la Armada Nacional, deben contar con una definición clara de los roles y funciones de los cargos que tienen relación, para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información. La definición de separación de deberes debe estar previamente aprobada por la DITIC o quien haga sus veces, en coordinación con el Jefe de área de la dependencia.

La separación de deberes sobre la infraestructura tecnológica y sobre los sistemas de información deben ser revisados periódicamente por DITIC o quien haga sus veces, con el fin de mantener actualizada dicha información, acorde con la realidad de cada una de las unidades de la Armada Nacional y DIMAR.

La separación de deberes sobre la infraestructura tecnológica y sistemas de información, deberán cumplir con los esquemas de seguridad robustos, que manejen usuarios, perfiles y responsabilidades.

c. Contacto con las Autoridades

La Armada Nacional mantendrá los contactos apropiados con las autoridades pertinentes, en caso de encontrar violación a la presente política de seguridad de la información de acuerdo al procedimiento de Gestión de Incidentes de Seguridad como el Comando Conjunto Cibernético (CCOC) y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT).

d. Contacto con Grupos de Interés Especial

Se mantendrán los contactos apropiados con los grupos de interés especial (Policía, Bomberos, Defensa Civil) u otros foros de seguridad especializados y asociaciones profesionales para

que puedan ser contactados de manera oportuna en el caso de que se presente un incidente de seguridad de la información.

e. Seguridad de la Información en la Gestión de Proyectos

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. Se debe tener en cuenta:

- Los gerentes de proyectos deben velar por que se incluya la seguridad de la información en cada proyecto.
- En el acta de constitución se realizará la valoración de los riesgos de seguridad de la información certificando que se lleve a cabo en una etapa temprana del proyecto para identificar los controles necesarios. Asegurando así que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.

4.2.2. Dispositivos Móviles y Teletrabajo

OBJETIVO:

Garantizar la seguridad de teletrabajo y el uso de dispositivos móviles.

POLÍTICAS:

a. Política para Dispositivos Móviles

Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, tabletas, smartphone, entre otros, se deben implementar controles de acceso como pin, contraseñas o patrones, técnicas criptográficas para cifrar la información crítica almacenada en estos y software antivirus.

Se deben revisar los permisos que se le suministran a las aplicaciones cuando se instalan en los dispositivos móviles e instalarlas desde sitios de confianza.

Mantener siempre actualizadas las aplicaciones y el sistema operativo de los dispositivos móviles.

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

Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o mecanismo que se defina para su protección, dentro o fuera de las Unidades y dependencias de la Armada Nacional.

b. Teletrabajo

La Armada Nacional autorizará las actividades de teletrabajo según sus necesidades, condiciones de trabajo, roles y perfiles del personal militar y no uniformado, contratistas y terceros. Las actividades de teletrabajo sólo se podrán desarrollar una vez sea autorizado por la División de Informática y se establezca controles de seguridad alineados con este Manual de Seguridad de la Información, cumpliendo con los parámetros de la Ley 1221 de 2008 "Teletrabajo" y frente al respectivo análisis de riesgo, cuando se requiera tener acceso a la información de la Institución desde redes externas, podrá acceder remotamente mediante un proceso de autenticación y uso de conexiones seguras como VPN (Redes Privadas Virtuales) establecidas en la Institución. Lo anterior asegurando el cumplimiento de requisitos de seguridad de los equipos desde los que se desea acceder como un firewall, un antivirus, instalar actualizaciones necesarias, implementar contraseñas de bloqueo y realizar mantenimientos regulares.

Antes de llevar a cabo cualquier actividad de teletrabajo, se definirán las actividades a desarrollar, la información a acceder, el horario y se realizará mediante Formato Solicitud de Acceso Remoto a Servicios Informáticos.

Cuando se trabaje en un equipo de cómputo externo debe utilizarse cifrado para la protección

de la información, antivirus para la protección contra malware y realizar un borrado seguro de la información.

Los equipos de cómputo desde donde se realice el teletrabajo deben tener instalado software legal.

4.3. SEGURIDAD DE LOS RECURSOS HUMANOS

4.3.1. Antes de Asumir el Empleo

OBJETIVO:

Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

POLÍTICAS:

a. Selección

Las verificaciones de los antecedentes de todos los candidatos a un empleo en la Armada Nacional se deben llevar a cabo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

b. Términos y Condiciones de Empleo

Los acuerdos contractuales con empleados y contratistas, deben establecer los niveles de responsabilidades y las de la Armada Nacional en cuanto a la seguridad de la información.

4.3.2. Durante la Ejecución del Empleo

OBJETIVO:

Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades en el cumplimiento de las políticas de seguridad de la información de la Institución y las cumplan.

POLÍTICAS:

a. Responsabilidades de la Dirección

La Armada Nacional debe exigir a todos los empleados y contratistas la aplicación de la

seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

b. Toma de Conciencia, Educación y Formación en la Seguridad de la Información

Todos los funcionarios y terceros al servicio de las Jefaturas, Comandos de Fuerza, Escuelas de Formación, Unidades de la Armada Nacional y contratistas, deben recibir formación y actualizaciones regulares sobre las políticas de seguridad de la información y procedimientos pertinentes para su cargo; durante el proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas con el fin de mantener la concientización de los funcionarios sobre la importancia de la seguridad de la información.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación, Unidades de la Armada Nacional, 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.

La concientización de seguridad implica el conocimiento, por parte de todo el personal que accede a información clasificada, de las obligaciones básicas y del deber de reserva que adquieren, derivadas del acceso a este tipo de información, así como de las responsabilidades penales y disciplinarias que son aplicables en caso de incumplimiento.

c. Proceso Disciplinario

Contra aquellos funcionarios que cometan una violación a la seguridad de la información, se deberá adelantar un proceso disciplinario, que debe comunicarse; las acciones emprendidas, serán conforme al reglamento de régimen disciplinario, de las Fuerzas Militares para el personal uniformado y el código único disciplinario, para el personal civil.

4.3.3. Terminación o Cambio de Empleo

OBJETIVO:

Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

POLÍTICAS:

a. Terminación o Cambio de Responsabilidades de Empleo

Asegurar que los empleados, contratistas o terceros realicen un cambio de empleo de una manera ordenada. La salida de un empleado, contratista o tercero será supervisada y se revisará que todo el equipo y retiro de los accesos a sistemas de información, se cumplan correctamente. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

4.4. GESTIÓN DE ACTIVOS

4.4.1. Responsabilidad por los Activos

OBJETIVO:

Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

POLÍTICAS:

a. Inventario de los Activos

Se deben identificar los activos de información, sus respectivos propietarios y su ubicación, a fin de elaborar y mantener un inventario actualizado mínimo cada año, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información y mediante formato Registro de Activos de Información Críticos Sistema Gestión de Seguridad de la Información alineado con la Ley 1712 de 2014 Ley de Transparencia.

b. Propiedad de los Activos

Cada una de las unidades y dependencias de la Armada Nacional 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.

c. Uso Aceptable de los Activos

Las normas para el uso aceptable de la información y de los activos de información y las instalaciones de procesamiento de información están identificadas en el presente documento y deben cumplirse de forma obligatoria por todos los funcionarios de la Institución.

Cada usuario debe firmar un acta de responsabilidad y custodia sobre los activos informáticos que le sean asignados y el compromiso de cumplimiento de las Políticas de Seguridad Informática e Información y promesa de reserva sobre los mismos.

La información de inteligencia, contrainteligencia, operaciones, proyectos y planes especiales de la Jefatura, Base Naval, Brigada, Batallón y Unidades Especiales, se considera clasificada; la clasificación de la información deberá obedecer a lo ordenado en la normatividad vigente por lo tanto debe ser almacenada única y exclusivamente en dispositivos informáticos institucionales, implementando las medidas de seguridad adecuadas, tales como protección con software de cifrado.

La instalación de cualquier tipo de software en los equipos de cómputo de cada Jefatura, Comando de Fuerza, Escuela de Formación, Unidad de la Armada Nacional, es responsabilidad exclusiva de la Dirección de Tecnología de Información y Comunicaciones o quien haga sus veces en estas dependencias, por tanto, son ellos los únicos autorizados para realizar esta labor.

Ningún activo informático adquirido y que sea configurable, debe ser instalado con la

configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador; se debe realizar la configuración adecuada de seguridad a través del administrador de los activos informáticos de cada Unidad.

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 deben ser realizados únicamente por DITIC o quien haga sus veces.

Los usuarios de los activos informáticos 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 efectuadas por DITIC o quien haga sus veces.

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.

Los requerimientos o necesidades de recursos tecnológicos de las dependencias de la Armada Nacional deben ser avalados por DITIC o quien haga sus veces.

Los recursos tecnológicos asignados a los funcionarios, contratistas y demás terceros autorizados, tienen el único propósito de contribuir a la realización de sus actividades laborales e institucionales y deben tener las restricciones adecuadas a su cargo.

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

Sobre los equipos más críticos de la red se deben configurar políticas de arranque a través de contraseña de setup (inicio).

Se prohíbe la instalación de software diferente

al instalado y autorizado por los funcionarios de las dependencias de informática de las Unidades.

El usuario debe cancelar todas las sesiones activas antes de dejar el equipo desatendido. El equipo debe tener configurada la opción de protector de pantalla con contraseña, con un tiempo mínimo de activación.

Los equipos que almacenan información clasificada o sensible, no deben tener acceso a internet.

En los equipos de cómputo se debe visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador.

Los equipos de los usuarios que requieran acceso a internet deben estar autorizados previamente mediante formato establecido.

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

Ningún servicio de carácter operativo o administrativo de las Jefaturas, Comandos de Fuerza, Escuelas de Formación, unidades de la Armada Nacional, deben contratarse en servicios en la nube públicos o híbridos

Para el caso de las Escuelas de Formación y Capacitación, se podrá hacer uso de servicios en la nube públicos o híbridos, siempre y cuando no se vea comprometida la seguridad institucional y la información clasificada.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación, unidades de la Armada Nacional, podrán desarrollar e implementar servicios en la nube privados o híbridos, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de controles adecuados.

Los usuarios no deben subir información de terceros que violen el derecho a la intimidad

o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Para la protección de medios que contienen información durante el transporte, verifique que se contemple:

- El uso de un transporte o servicio de mensajería sean confiable.
- Un procedimiento para verificar la identificación de los servicios de mensajería.
- El embalaje debe proteger el contenido contra cualquier daño físico que pudiera presentarse durante el tránsito, y de acuerdo con las especificaciones de los fabricantes, por ejemplo, protección contra factores ambientales que puedan reducir la eficacia de la restauración del medio, tal como exposición al calor, humedad o campos electromagnéticos.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, según el caso, 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, sin embargo, en ningún caso se considerarán aceptables los siguientes usos:

- **INTERNET**

  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:

  - Navegar en sitios de contenido sexualmente explícito, discriminatorio, que

implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.

- Realizar cualquier actividad tipificada como delito informático o delitos sexuales a través de los activos informáticos institucionales.
- Publicar, enviar o adquirir material sexualmente explícito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.
- Publicar o enviar información confidencial fuera de las unidades y dependencias de la Armada Nacional, sin la aplicación previa de los controles para salvaguardarla y sin la autorización de los propietarios respectivos.
- Utilizar otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados.
- Publicar anuncios comerciales o material publicitario en internet 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.
- Promover o mantener asuntos o negocios personales.
- Descargar, instalar y utilizar 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.
- Navegar en las cuentas de correo de carácter personal, no institucional o en redes sociales, sin justificación.
- Uso de herramientas de mensajería instantánea no autorizadas por DINFO o la que haga sus veces.
- Emplear cuentas de correo externas, no institucionales, para el envío o recepción de información institucional.

- 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 sin violar la intimidad del usuario.
- 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.
- Dado el caso que por la naturaleza del cargo se requieran accesos especiales, estos deben ser solicitados mediante Formato Solicitud de Acceso Internet Institucional. Este formato será actualizado por el usuario cuando se realice cambio en la dirección IP o en el cargo.

• **CORREO ELECTRÓNICO INSTITUCIONAL**

- La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro de cada una de las Unidades y dependencias de la Armada Nacional, la misma debe solicitarse mediante Formato de Solicitud Cuenta de Correo Institucional.
- Los mensajes y la información contenida en los buzones de correo institucional son de propiedad de las unidades y dependencias de la Armada Nacional. 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 interés de la Armada Nacional.
- El correo institucional de cada funcionario se creará con la característica nombre. apellido@armada.mil.co, en caso que el

usuario ya exista se creará como nombre. apellido.primera inicial del segundo apellido @armada.mil.co, en caso de existir un homónimo se siguen tomando las siguientes letras del segundo apellido.

- En los casos que sean comunicaciones, servicios de guardia o inteligencia, se creará la cuenta con la sigla de la Unidad o dependencia seguida por el dominio @ armada.mil.co. Para legalizar este proceso debe llenarse el formato de autorización de correo electrónico y oficio dirigido a la División de Informática solicitando dicha cuenta, la cual hará parte a partir de su creación, de los activos de información de la dependencia y debe ser entregada en acta de relevo o libros de minuta.
- Se pueden habilitar alias de cuentas de correo sobre las cuentas personales, esta debe ser administrada con absoluta responsabilidad por la persona nombrada, se creará la cuenta con la sigla de la Unidad, dependencia o cargo, seguida por el dominio @armada.mil.co. La solicitud se debe realizar a DINFO mediante el correo electrónico soporte.bogota@armada.mil.co. En caso de relevo del cargo, traslado o baja, se debe informar quien asume la responsabilidad sobre este alias o si se requiere su eliminación; cabe aclarar que éste alias hará parte desde su creación, de los activos de información de la dependencia y debe ser entregada en acta de relevo o libros de minuta.
- Un correo, con información clasificada o sensible se debe transmitir por medio de las dependencias de inteligencia o contrainteligencia de cada Unidad, ya que ellos cuentan con el correo Cobra que tiene mecanismos de cifrado.
- Todo el personal de la Armada Nacional debe tener asignada una cuenta de correo electrónico institucional "@armada.mil.co", el cual es el único medio autorizado

para el trámite de información institucional.

- El tamaño de los buzones es de 5 Gigabytes y mensajes de correo adjuntos es de 42 Megabytes. En caso que se requiera mayor capacidad de almacenamiento para el correo electrónico institucional, por necesidades de cada usuario, éste deberá solicitarlo a DINFO mediante correo electrónico a la cuenta soporte.bogota@armada.mil.co.
- Es responsabilidad de cada usuario tener copias de respaldo (backups) de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas generándolo a través de zimbra de acuerdo al procedimiento establecido o también utilizando un gestor de correo electrónico (zimbra store o Outlook) que permita mantener copia local de los mensajes recibidos.
- Es responsabilidad del propietario de la cuenta mantener el buzón por debajo de su capacidad para evitar que se sature, implementando prácticas de buen uso, tales como lectura regular de los mensajes, eliminación de mensajes antiguos y vaciar la papelera.
- Existen listas de correo goficiales@armada.mil.co, gsuboficiales@armada.mil.co, gciviles@armada.mil.co y gimp@armada.mil.co que se utilizan para envío correo electrónico masivo a nivel nacional y gbogota@armada.mil.co para envío correo electrónico masivo a nivel Bogotá, el uso de estas listas solo es para envío de información de interés general institucional, se tienen solo algunas cuentas permitidas como la administración de correo, maestría de armas Bogotá, División de Administración de Personal y otras dependencias autorizadas por el señor Segundo Comandante de la Armada Nacional, ningún funcionario puede enviar información a esas listas. Los usuarios que

reenvíen información de respuesta a las listas y no al correo que se solicita enviar información, será bloqueada su cuenta un tiempo que oscilara entre dos a cinco días y si reincide, la cuenta se bloqueará hasta por cinco días.

- Cuando se requiera realizar la recuperación de contraseñas el usuario debe realizar lo requerido en el Procedimiento para Gestión de Usuarios y Contraseñas.
- No está autorizada la utilización de correos comerciales para transmitir información de carácter institucional.
- La División de Informática de la Armada Nacional o cualquier otra dependencia no solicita información de usuario y contraseña a través del correo electrónico, por tanto, los usuarios nunca deben responder o acceder a links donde se solicite dicha información.
- No se considera aceptado el uso del correo electrónico institucional para los siguientes fines:
  - Utilizar sistemas y servicios de la Institución con mensajes, imágenes o contenidos que sean violatorios al derecho a la intimidad de cualquier persona.
  - Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, discriminatorio, sexista, pornográfico, publicitario no institucional, mensajes que atenten contra la seguridad y defensa de la nación, 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.
  - El envío de cualquier tipo de archivo

que ponga en riesgo la seguridad y reserva 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 DITIC, o la que haga sus veces.

- El envío de información relacionada con la defensa y la seguridad nacional a otras entidades del Gobierno diferentes a las que conforman la Armada Nacional, sin la autorización previa del propietario de la información y de la DITIC, o la que haga sus veces.
- Toda información que requiera ser transmitida fuera de cada Jefatura, Comando de Fuerza, Escuela de Formación y Unidad de la Armada Nacional, que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. Sólo podrá ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- Todo correo electrónico deberá respetar el estándar de formato e imagen institucional definido para cada una de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deberá contener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:
- El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
- El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
- En caso de que el mensaje sea recibido

por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

- Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.
- Todo el personal de la Armada Nacional deberá configurar su correo electrónico Institucional de tal manera que en la firma de su correo quede claramente identificado, de acuerdo al Manual de Comunicación Institucional Doctrina ARC T10 – 1.1 Público:
  - Grado completo no abreviado.
  - Nombres y apellidos completos.
  - Cargo completo y no abreviado.
  - Dependencia, Unidad y Jefatura a la que pertenece completa y no abreviada.
  - Datos de Contacto.
  - Dirección Oficina.
  - Teléfono Oficina con extensión, si la tiene.
  - Celular institucional, si lo tiene.
  - Ciudad y país.
  - Correo institucional.

d. Medidas que Atentan contra la Seguridad de la Información

- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a las unidades y dependencias de la Armada Nacional, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
- No clasificar o etiquetar la información.
- No guardar bajo llave documentos impresos que contengan información clasificada, al terminar la jornada laboral.
- No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.

- Reutilizar papel que contenga información sensible, 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.
- Hacer uso de la red de datos de las unidades y entidades de la Armada Nacional, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
- Instalar software en la plataforma tecnológica de las unidades y dependencias de la Armada Nacional, cuyo uso no esté autorizado por la DITIC o quien haga sus veces, atentando contra las leyes de derechos de autor o propiedad intelectual.
- Destruir la documentación institucional sin seguir los parámetros y normatividad vigente establecida para el proceso de gestión documental.
- Descuidar información clasificada de las unidades y dependencias de la Armada Nacional, sin las medidas apropiadas de seguridad que garanticen su protección.
- No cumplir protocolos para mantener la reserva de la información clasificada o que tenga reserva.
- Enviar información no pública por correo físico, copia impresa o electrónica sin la debida autorización o sin la utilización de los protocolos establecidos para la divulgación.
- Almacenar y mantener información clasificada en dispositivo de almacenamiento de cualquier tipo que no sean de propiedad de las respectivas unidades y dependencias de la Armada Nacional.
- Conectar computadores portátiles u otros dispositivos electrónicos personales a la red de datos de las unidades y dependencias de la Armada Nacional, sin la debida autorización.
- Ingresar a la red de datos de las unidades y dependencias de la Armada Nacional por

cualquier servicio de acceso remoto, sin la autorización de la DITIC o la que haga sus veces.

- Usar servicios de internet en los equipos de la Institución, diferente al provisto por la DITIC o la que haga sus veces.
- Promover o mantener actividades personales utilizando los recursos tecnológicos de las unidades y dependencias de la Armada Nacional para beneficio personal.
- Uso de la cuenta y contraseña de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.
- 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.
- Retirar de las instalaciones de las unidades y dependencias de la Armada Nacional, computadores de escritorio, portátiles e información clasificada física o digital sin autorización o abandonarla en lugares públicos o de fácil acceso.
- Entregar, enseñar o divulgar información clasificada de las unidades y dependencias de la Armada Nacional a personas o entidades no autorizadas.
- Llevar a cabo actividades ilegales o intentar acceso no autorizado a la plataforma tecnológica de las unidades y dependencias de la Armada Nacional o de terceras partes.
- Ejecutar cualquier acción que difame, afecte la reputación o imagen de las unidades y dependencias de la Armada Nacional o de alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
- Realizar cambios no autorizados en la plataforma tecnológica de las unidades y dependencias de la Armada Nacional.
- Determinar, otorgar y autorizar todos los privilegios de acceso a sus activos de información.

- Ejecutar acciones para eludir o modificar los controles establecidos en la presente directiva.
- Desconocer la cultura organizacional relacionada con conciencia en la seguridad de la información, su buen uso, control y protección derivando en malas prácticas que dejan como resultado fuga de información sensible con riesgos de impacto para la Institución.
- Ubicar los equipos que hacen parte de la infraestructura tecnológica de las unidades y dependencias de la Armada Nacional en lugares donde no estén protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.
- Transportar información en medios de almacenamiento sin las medidas de seguridad adecuadas y sin previa autorización del Jefe de la dependencia y el OSI de la Unidad.
- Prestar a personas ajenas o no autorizadas los equipos institucionales asignados.
- Almacenar las contraseñas de acceso a los diferentes sistemas de información en medios o formatos no protegidos.
- Desproteger los recursos asignados por las unidades o dependencias de la Armada Nacional, no guardar el secreto de las contraseñas de acceso, no cambiarla periódicamente y no notificar al OSI de la Unidad cualquier novedad o incidente informático.
- Ubicar equipos tales como máquinas de copiado, impresoras y máquinas de fax en zonas sin control o de libre acceso.
- Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

e. Devolución de los Activos

Todos los empleados y contratistas deberán devolver todos los activos de información de la Armada Nacional en su poder a la terminación de su vinculación laboral, el formato de cese definitivo es utilizado como medio de control.

4.4.2. Clasificación de la Información

OBJETIVO:

Asegurar que la información recibe un nivel apropiado de protección, acorde a su importancia en la Armada Nacional.

POLÍTICAS:

a. Clasificación de la Información

Los responsables de la información deben realizar la clasificación y control de activos de información con el objetivo de garantizar que reciban un apropiado nivel de protección, clasificación de la información e identificación de su sensibilidad, criticidad, definiendo los niveles de protección y medidas de tratamiento conforme al procedimiento de Inventario y Clasificación de Activos de Información.

La clasificación de información de que trata la Ley 1621 de 2013 (ultrasecreto, secreto, confidencial y restringido) está orientada a proteger la información de Inteligencia y Contrainteligencia, así como los agentes, métodos, medios y fuentes. Por lo tanto, dicha clasificación aplica ÚNICA y EXCLUSIVAMENTE para la documentación originada por Unidades y dependencias que cumplan funciones de Inteligencia y Contrainteligencia.

Las Unidades o dependencias de la Armada Nacional que NO tengan función de inteligencia o contrainteligencia deben aplicar los criterios contenidos en la Ley 1712 de 2014 artículos 6 y 19 y su correspondiente Decreto Reglamentario; en consecuencia, la información que deba gozar de reserva será denominada como "Documentación Pública Reservada" conforme

a lo publicado mediante Directiva Permanente 001/MDN-CGFM-CARMA-SECAR-JINA-DICOI-23.1 del 12 de enero de 2017.

La clasificación debe realizarse evaluando las características en las cuales se basa la seguridad de la información: Confidencialidad, integridad y disponibilidad.

La clasificación de los activos debe revisarse mínimo cada año, cuando sea identificado algún riesgo o cuando haya cambios en la estructura del proceso.

b. Etiquetado de la Información

Los procedimientos para el etiquetado de la información serán aplicados de acuerdo con el esquema de clasificación de la información aprobada por la entidad, lo anterior teniendo en cuenta las tablas de retención documental aprobadas para las diferentes áreas.

c. Manejo de Activos

Se aplicará los procedimientos Inventario y Clasificación de Activos de Información, para el manejo de activos de conformidad con el esquema de clasificación de la información aprobada por la Armada Nacional y presentada en este documento.

4.4.3. MANEJO DE MEDIOS

OBJETIVO:

Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

POLÍTICAS:

a. Gestión de Medios de Soporte Removibles

Se encuentra restringida la conexión a la infraestructura tecnológica (servidores, computadores, impresoras, scanner y demás dispositivos de tecnologías de la información) de la Armada Nacional de cualquier elemento de almacenamiento como dispositivos personales

USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, smartphone, tabletas, módems, memorias SD o de almacenamiento, entre otros dispositivos no institucionales. Las excepciones especiales serán autorizadas por la Dirección de Informatica.

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 mediante algún mecanismo de cifrado que garantice su integridad y confidencialidad.

Las unidades de la Armada Nacional 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 mediante formato de Excepción de Instalación Software de Seguridad.

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. 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.

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

En la Armada Nacional todos los medios removibles de almacenamiento de información como USB, discos duros externos, módems, CD, DVD, deben estar identificados con el logo, label o caratula institucional.

b. Disposición de los Medios

En la Armada Nacional se debe disponer en forma segura de los medios cuando ya no se requieran, empleando procedimientos formales.

Los equipos de cómputo asignados, deben ser devueltos a los Departamento de Telemática de las Unidades, una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación laboral con la Armada Nacional.

Los equipos de contratistas y terceros que hayan sido autorizados para acceder a las instalaciones militares, sólo podrán ser retirados al finalizar el contrato o labores para las cuales estaban definidos, previa revista de sanitización que incluirá entre otras tareas el borrado seguro de la información a través del proceso de verificación de equipos. DITIC o quien haga sus veces, generará el paz y salvo o constancia de dicho procedimiento, que deberá ser realizado al momento del retiro del equipo, de las instalaciones físicas correspondientes.

c. Transferencia de los Medios Físicos

Los medios que contienen información se deberán proteger contra accesos no autorizados, uso indebido o corrupción durante el transporte.

4.5. CONTROL DE ACCESO

4.5.1. Requisitos del Negocio para Control de Acceso

OBJETIVO:

Limitar el acceso no autorizado a la información y/o a las instalaciones de personal a los recintos de procesamiento de información de la Armada Nacional.

POLÍTICAS:

a. Política de Control de Acceso

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. Esto se manejará conforme al procedimiento autorización de ingreso a los servicios de los recursos informáticos y de comunicaciones.

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.

Para el acceso a sistemas de información y base de datos se debe diligenciar el formato solicitud uso sistemas de información y/o base de datos.

Los administradores deben identificar y eliminar o deshabilitar periódicamente las identificaciones de usuarios redundantes y que no sean asignados a otros usuarios.

En las aplicaciones se debe suministrar menús para controlar el acceso a las funciones de los sistemas y limitar la información contenida en los elementos de salida.

En los sistemas de información no se debe visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente.

En los activos de información evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado.

En los sistemas de información se debe validar la información de ingreso solamente al completar todos los datos de entrada, ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.

En los sistemas de información se debe proteger contra intentos de ingreso mediante fuerza bruta.

En los sistemas de información se debe llevar un registro con los intentos exitosos y fallidos.

No se debe visualizar una contraseña que se esté ingresando en texto claro.

A través de la red no se debe transmitir contraseñas en texto claro.

Terminar sesiones después de un período de inactividad definido, especialmente en lugares de alto riesgo, tales como áreas públicas o externas por fuera de la gestión de seguridad de la Institución o en dispositivos móviles.

Restringir los tiempos de conexión con el fin de brindar seguridad adicional en aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

Llevar un registro de las contraseñas usadas previamente, e impedir su reúso.

Las librerías de fuentes de programas no se deben mantener en los sistemas operativos.

Para gestionar los códigos fuente y las librerías de los programas, se debería hacer de acuerdo con los procedimientos establecidos.

El personal de soporte debe tener acceso restringido a las librerías de los programas fuentes aplicaciones.

La actualización de las librerías de las fuentes de aplicaciones y elementos asociados, y la entrega de los programas fuentes sólo se deben hacer una vez que se haya recibido autorización apropiada.

Los listados de programas se deben mantener en un entorno seguro.

Se debe conservar un registro de auditoría de todos los accesos a las librerías de programas fuente.

Se debe mantener y copiar las bibliotecas de los programas fuentes a través de procedimientos estrictos de control de cambios.

La creación, modificación y baja de usuarios en la infraestructura de procesamiento de información,

comunicaciones y seguridad informática deben seguir el procedimiento gestión de usuarios y contraseñas.

A los usuarios se les debe suministrar una autentificación secreta temporal segura, que se obligue a cambiar, al usarla por primera vez.

Todo usuario que se cree, para que un tercero ingrese a las redes de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y Unidades de la Armada Nacional, deben tener una fecha de vencimiento específica, la cual, en ningún caso, debe superar la fecha de terminación de sus obligaciones contractuales.

b. Acceso a Redes y a Servicios en Red

Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática de la Armada Nacional deberá estar autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones a través de la División de Informática de la Armada Nacional o quien haga sus veces, acuerdo lo estipulado en el formato solicitud de acceso remoto a servicios informáticos.

Todas las conexiones remotas deben ser autenticadas y seguras, antes y durante el acceso y su tráfico debe estar cifrado.

Los equipos de terceros que requieran acceder a las redes de datos de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deben cumplir un procedimiento de sanitización informática antes de concedérseles dicho acceso.

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 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 labores para las cuales estaba definido.

Una vez culminadas estas labores se procedera a un formateo final para retirar los equipos de las instalaciones.

Los accesos a la redes inalámbricas deben ser autorizados por los Departamentos de Telemáticas o quien haga sus veces y deberán contar con la verificación previa del OSI, quien debe determinar si se cumplen con las condiciones de seguridad, establecidas en los mecanismos de control para proteger la infraestructura. En ningún caso se podrán dejar configuraciones y contraseñas por defecto.

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.

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

El OSI o el que haga sus veces será el responsable de validar a quien le serán asignados los servicios a través de redes inalámbricas.

El servicio de Internet en las escuelas de formación y capacitación, deberá contar con mecanismos de autenticación de usuarios y estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación por fuera de la red administrativa de la unidad.

4.5.2. Gestión de Acceso de Usuarios

OBJETIVO:

Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

POLÍTICAS:

a. Registro y Cancelación del Registro de Usuarios

La asignación de privilegios en las aplicaciones, para los diferentes usuarios, está determinado por el procedimiento gestión de usuarios y contraseñas. 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.

b. Suministro de Acceso de Usuarios

Los derechos de acceso de los usuarios se deben revisar en intervalos regulares y modificar o reasignar estos derechos cuando se presenten cambios en el perfil de usuario, por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

c. Gestión de Derechos de Acceso Privilegiado

Los privilegios de administrador de cualquier equipo de cómputo, deben ser asignados exclusivamente al administrador del sistema. En ningún caso se deben asignar estos privilegios de acceso al usuario del equipo.

d. Gestión de Información de Autenticación Secreta de Usuarios

La asignación de la información secreta de autenticación, se deben controlar a través de un proceso de gestión formal de acuerdo a la clasificación dada a los activos por parte de los responsables.

e. Revisión de los Derechos de Acceso de Usuarios

Los propietarios de los activos deben revisar los

derechos de acceso de los usuarios, a intervalos regulares.

f. Retiro o Ajuste de los Derechos de Acceso

Los derechos de acceso de todos los funcionarios y de usuarios externos a la información y a las instalaciones de procesamiento de información de la Armada Nacional se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

4.5.3. Responsabilidades de los Usuarios

OBJETIVO:

Todos los usuarios de la Armada Nacional responderán por las acciones y/o omisiones efectuadas con sus cuentas que puedan atentar con la salvaguarda de la información de autenticación.

POLÍTICAS:

a. Uso de la Información de Autenticación Secreta

El usuario debe proteger los recursos asignados por la Unidad o dependencia, guardar el secreto de su contraseña, no prestar su clave de usuario bajo ninguna circunstancia, cambiar su contraseña periódicamente y notificar al OSI de la Unidad, cualquier novedad o incidente informático, que observe en el funcionamiento de su cuenta y en la aplicación de las Políticas de Seguridad de la Información.

Cada administrador de los sistemas de información debe asegurar que la información de autenticación secreta, configurada por defecto desde fábrica, se modifica después de la instalación de los sistemas o software.

Los usuarios deben propender por una administración responsable de sus contraseñas personales, evitando que sean almacenadas en formatos no protegidos.

La administración, así como la asignación y entrega de las contraseñas a los usuarios deberá seguir el procedimiento Gestión de Usuarios y Contraseñas.

Los usuarios deberán aplicar las siguientes recomendaciones para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

- Las contraseñas son de uso personal y por ningún motivo se deben prestar a otros usuarios.
- Las contraseñas no deberán ser reveladas por ningún motivo.
- 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.
- Es deber de cualquier funcionario y tercero reportar cualquier sospecha que una persona esté empleando un usuario y contraseña que no le pertenece, de acuerdo con el procedimiento de gestión de incidentes de seguridad.
- La longitud mínima de las contraseñas debe ser de 8 dígitos y contener mínimo una mayúscula, una minúscula, un número y un carácter especial.
- Las contraseñas no deben estar basadas en temas que puedan adivinarse fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono, fechas de nacimiento, etc.).
- Las contraseñas deben estar libres de caracteres completamente numéricos o alfabéticos idénticos, consecutivos.

En caso que un tercero deba por razones del servicio conocer una contraseña, la misma deberá ser cambiada dentro de las veinticuatro (24) horas siguientes.

4.5.4. Control de Acceso a Sistemas y Aplicaciones

OBJETIVO:

Evitar el acceso no autorizado a sistemas y aplicaciones.

POLÍTICAS:

a. Restricción de Acceso a la Información

El acceso a la información y a las funciones de los sistemas de las aplicaciones se restringe de acuerdo con la política de control de acceso.

b. Procedimiento de Ingreso Seguro

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro de acuerdo al Procedimiento para ingreso seguro a los sistemas de información.

c. Sistemas de Gestión de Contraseñas

El funcionario debe recibir un usuario y una contraseña para acceder a los recursos informáticos de la Institución, ésta contraseña es de cambio obligatorio en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8 (ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación.

Por seguridad se recomienda el cambio de dichas claves con una periodicidad de 90 (noventa) días.

Después de 3 (tres) intentos no exitosos de digitar la contraseña el usuario será bloqueado de manera inmediata y debe solicitar el desbloqueo a través de la mesa de servicios a DINFO.

d. Uso de Programas Utilitarios Privilegiados

Se restringe y controla estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.

e. Control de Acceso a Códigos Fuente de Programas

El acceso a código fuente de los programas es limitado, únicamente los ingenieros del grupo de soporte podrán contar con acceso a esta información y harán uso de la misma.

4.6. CRIPTOGRAFÍA

4.6.1. Controles Criptográficos

OBJETIVO:

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

POLÍTICAS:

a. Política sobre el Uso de Controles Criptográficos

La Jefatura de Inteligencia Naval debe 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, tanto cuando se encuentra almacenada como cuando es transmitida o procesada la información, teniendo en cuenta la clasificación y sensibilidad de la misma.

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

b. Gestión de Llaves

La Jefatura de Inteligencia Naval desarrolla e implementa la política sobre uso, protección y duración de las claves criptográficas.

4.7. SEGURIDAD FÍSICA Y DEL ENTORNO

4.7.1. Áreas Seguras

OBJETIVO:

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de la información de la Armada Nacional.

POLÍTICAS:

a. Perímetro de Seguridad Física

Todas las áreas que se hayan definido como restringidas 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 protegidos los accesos no autorizados mediante controles y tecnologías de autenticación de acuerdo a lo estipulado en el Procedimiento para Acceso a Áreas Seguras.

Se consideran áreas restringidas los centros de operaciones, centros de fusión de información de inteligencia, centro de operaciones de seguridad e infraestructura (COPEI), Compañía de Acción Integral (COPAI), estaciones de radio, centros de datos y todos aquellos que manejen o contengan información sensible; además se prohíbe:

- Uso de redes inalámbricas.
- Ingreso de teléfonos celulares, dispositivos de almacenamiento, smartphone, tabletas, equipos de cómputo personal o cualquier equipo tecnológico no autorizado.

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

- No consumir alimentos ni bebidas.
- No ingresar elementos inflamables.
- No permitir el acceso de personal ajeno, sin que esté acompañado por un funcionario durante el tiempo que dure su visita.

- No almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
- No permitir la toma de fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
- No permitir el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida, para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos (aire acondicionado de alta precisión) y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

b. Controles de Acceso Físicos

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.

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.

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 Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, mientras permanezcan dentro de sus instalaciones.

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

Es responsabilidad de todos los funcionarios y terceros acatar las normas de seguridad y

mecanismos de control de acceso a las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional.

Los funcionarios y terceros, así como los visitantes, deben 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.

Los servicios de procesamiento de información sensible o crítica deben estar ubicados en áreas restringidas, protegidas por perímetros de seguridad definidos, con barreras y controles de ingreso adecuados. Dichas áreas deben estar protegidas físicamente contra accesos no autorizados, daño e interferencia. La protección suministrada debe estar acorde con los riesgos identificados.

Las áreas protegidas se resguardan mediante el empleo de controles de acceso físico y registro, los cuales serán determinados por el OSI a fin de permitir el acceso sólo a personal autorizado.

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

c. Seguridad de Oficinas Recintos e Instalaciones

Las instalaciones claves deben estar ubicadas estratégicamente en zonas con acceso restringido al público.

Debe definirse donde sea aplicable, que las edificaciones sean discretas y den un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información.

Es necesario establecer que las instalaciones estén configuradas para evitar que las actividades o información confidenciales, sean

visibles y/o audibles desde el exterior. El blindaje electromagnético también debe ser el apropiado.

Los directorios y guías telefónicas internas, que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.

d. Protección contra Amenazas Externas y Ambientales

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 tomarán en cuenta las disposiciones y normas establecidas (estándares) en materia de sanidad y seguridad.

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

Las unidades de la Armada Nacional deben acoger los lineamientos a que haya lugar de acuerdo a la normatividad ambiental vigente para el Manejo de Residuos de Aparatos Eléctricos y Electrónicos (RAEE), de forma que se prevenga y reduzca el impacto ambiental.

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

- Sistema Alarma
- Sistema Eléctrico
- Sistema de protección contra incendios
- Control de temperatura
- Sistema CCTV
- Minuta de ingreso de personal ajeno.

e. Trabajo en Áreas Seguras

Todo acceso físico a las áreas protegidas debe estar manejado según los lineamientos definidos por el procedimiento de Control de Acceso a Áreas Seguras.

f. Áreas de Despacho y Carga

Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado, adicionalmente se debe cumplir con los siguientes parámetros:

- Deben existir registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.
- Establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado.
- Definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.
- Establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas.
- Definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.
- Establecer que el material que ingresa se registra de acuerdo con los procedimientos establecidos al entrar al sitio.
- Definir que los despachos entrantes y salientes están separados físicamente, en donde sea posible.

- Establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.

4.7.2. Equipos

OBJETIVO:

Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la Armada Nacional.

POLÍTICAS:

a. Ubicación y Protección de los Equipos

Los equipos que hacen parte de la infraestructura tecnológica de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, 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.

Los equipos tales como máquinas de copiado, impresoras y máquinas de fax deben estar ubicados en zonas de acceso restringido y deben contar con control de código para su uso.

b. Servicios de Suministro

Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos.

c. Seguridad del Cableado

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

En las unidades de la Armada Nacional todo el sistema de cableado estructurado deberá contemplar que esté dentro de la norma TIA/EIA 606, que proporciona una guía para la ejecución de la administración de un buen sistema de cableado.

d. Mantenimiento de Equipos

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 deben ser prestados a personas ajenas o no autorizadas.

Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, se 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.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, 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.

Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, deben estar presenten en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos e inspeccionar para asegurarse que no ha sido alterado y que su funcionamiento es adecuado.

Solo el personal de mantenimiento designado por la División de Informática de la Armada Nacional o quien haga sus veces, está autorizado para llevar a cabo reparaciones y el servicio a los equipos.

La Armada Nacional debe llevar un registro de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo que se realice sobre los activos informáticos de la Institución.

e. Retiro de Activos

Todo el personal que por cumplimiento de sus funciones institucionales necesite retirar un equipo, medio de almacenamiento, información o software de las instalaciones de la Unidad militar, deben ser debidamente identificados y registrados antes de conceder la autorización respectiva.

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) de acuerdo al formato Autorización Ingreso/Salida Equipos de Cómputo y Accesorios Institucionales al complejo militar y formato Autorización Ingreso /Salida de Equipos de Cómputo y/o Accesorios al complejo militar para las dependencias ubicadas en el complejo militar CAN en los formatos autorizados por CGFM y en las demás unidades los publicados en la Suite Visión Empresarial Armada Nacional.

Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, proporcionarán los mecanismos y recursos necesarios para que en cada punto de acceso a las instalaciones exista un puesto de revisión de

activos informáticos, donde se inspeccione y se lleve el control de los equipos que son ingresados y retirados previamente con supervisión y visto bueno del OSI.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, 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.

f. Seguridad de Equipos y Activos Fuera de las Instalaciones

Si por razones de trabajo los funcionarios que tengan a su cargo un equipo de cómputo necesitan llevarlo a sitios fuera de las instalaciones deben estar previamente autorizados por el Jefe de la dependencia, la información sensible o clasificada que contengan debe estar cifrada en el disco duro o borrada en forma segura.

Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deben velar por la protección de los mismos sin dejarlos desatendidos.

El propietario del activo, con el apoyo de DITIC, o quien haga sus veces, identificará mediante una metodología de análisis de riesgos que cada Jefatura, Comando de Fuerza, Escuela de formación y unidad de la Armada Nacional, 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.

En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información clasificada y que esté además relacionada con la defensa y la seguridad nacional, el responsable del equipo deberá ponerlo en conocimiento de DITIC y debe realizar inmediatamente el

respectivo reporte de incidente de seguridad (TELM-PT-010-JOLA), así como realizar la correspondiente denuncia ante la autoridad competente, si el caso lo amerita.

Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deberán contener únicamente la información estricta y necesaria para el cumplimiento de su misión, así mismo, se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene, adicionalmente la información debe estar cifrada.

g. Disposición Segura o Reutilización de Equipos

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.

Cuando el activo de información sea dado de baja se retira el disco duro y se realiza el borrado seguro a la información para prevenir la pérdida de confidencialidad en la División de Informática o quien haga sus veces en las unidades. Posteriormente se realizará la destrucción segura y se documentará mediante acta, registro fílmico y fotográfico, teniendo en cuenta el Procedimiento de Baja de Equipos Informáticos.

Para la reasignación de los equipos de cómputo se entregarán a la División de Informática para realizar el borrado seguro de la información y configuración de los mismos.

Para la garantía en equipos de cómputo se realiza el backup de la información y el borrado seguro, se procede a la entrega del disco duro a la empresa encargada de realizar el soporte y respectiva garantía cuando aplique.

Para la renovación de equipos de cómputo se realiza el particionamiento y configuración respectiva del disco duro de acuerdo a la lista de chequeo y se entrega a la dependencia.

h. Equipos de Usuario Desatendidos

En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.

Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

i. Política de Escritorio Limpio y Pantalla Limpia

Todas las estaciones de trabajo deben emplear únicamente el papel tapiz y el protector de pantalla establecido por la unidad o dependencia de la Armada Nacional.

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.

4.8. SEGURIDAD DE LAS OPERACIONES

4.8.1. Procedimientos Operacionales y Responsabilidades

OBJETIVO:

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información.

POLÍTICAS:

a. Procedimientos de Operación Documentados

Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.

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 formatos siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

Los procedimientos operativos deben quedar debidamente documentados, teniendo en cuenta el procesamiento y manejo de la información, manuales para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

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.

b. Gestión de Cambios

Todo cambio que se realice sobre los sistemas de información y la infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de la DITIC, o las que hagan sus veces, de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, conforme al Procedimiento de Gestión de Cambios; debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

c. Gestión de Capacidad

La DITIC o quien haga sus veces, como área responsable de la administración de la plataforma tecnológica, debe 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 y Procedimiento para la Renovación y Reasignación de Equipos Informáticos de la Armada Nacional.

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

d. Separación de los Ambientes de Desarrollo, Pruebas y Operación

Cada una de las unidades de la Armada Nacional proveerán los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica 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.

El paso de software y hardware, de un ambiente a otro, deberá ser controlado y gestionado de acuerdo con lo definido en el procedimiento para gestión de cambios.

Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción con el fin de evitar problemas de disponibilidad, confidencialidad e integridad de la información.

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

No se permite la copia de información Ultrasecreta, Secreta, Confidencial, Restringida, Exclusiva de Comando, de solo Conocimiento

y de uso Exclusivo, desde el ambiente de producción al ambiente de pruebas. En caso 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.

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

Periódicamente se podrán 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 las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional.

4.8.2. Protección Contra Códigos Maliciosos

OBJETIVO:

Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

POLÍTICAS:

a. Controles Contra Códigos Maliciosos

Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en los procedimientos de Gestión de Vulnerabilidades y Gestión de Cambios.

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 prevenga el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin la correspondiente autorización de DITIC y deberá ser actualizado en forma permanentemente.

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

Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de las Jefaturas, Comandos de Fuerza, Escuelas de Formación, unidades de la Armada Nacional y DIMAR, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

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

Cada Jefatura, Comando de Fuerza, Escuela de Formación, Unidad de la Armada Nacional, deberá mantener actualizado al personal 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.

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

4.8.3. Copias de Respaldo

OBJETIVO:

Proteger la información contra la pérdida de datos.

POLÍTICAS:

a. Respaldo de Información

La información con cierto nivel de clasificación debe asegurarse en conjunto por la DITIC o quien haga sus veces y la dependencia responsable de la misma, en la plataforma tecnológica de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, y periódicamente deberá ser 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 formato para Gestión de Copias de Respaldo.

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.

Se deberá establecer un Plan de Backup y Restauración de Copias de Seguridad de la Información que serán probados a intervalos regulares, establecidos según las necesidades y capacidades de cada una de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, por sus correspondientes DITIC o quien haga 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.

DITIC a través de DINFO o las que hagan sus veces de las correspondientes dependencias y unidades de la Armada Nacional, establecerá el procedimiento de resguardo y recuperación de la información que incluyan especificaciones del traslado, frecuencia, identificación; así mismo, definirá conjuntamente con las dependencias usuarias los periodos de retención de dicha información en el formato control de backups.

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.

Se debe hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una Política de Copias de Respaldo aceptada.

4.8.4. Registro y Seguimiento

OBJETIVO:

Registrar eventos y generar evidencia.

POLÍTICAS:

a. Registro de Eventos

Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deben 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" y formato monitoreo de seguridad.

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 a la Armada Nacional.

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

Todo evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a DITIC o quien haga sus veces, mediante el procedimiento de gestión de incidentes de seguridad.

Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

b. Protección de la Información de Registro

Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

c. Registros del Administrador y del Operador

Las actividades del administrador y del operador del sistema se registran y los registros se protegen y revisan con regularidad.

d. Sincronización de Relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Armada Nacional se deben sincronizar con el servidor NTP (servidor para sincronización de los relojes) autorizado por la División de Informática.

4.8.5. Control de Software Operacional

OBJETIVO:

Asegurar la integridad de los sistemas operacionales.

POLÍTICAS:

a. Instalación de Software en Sistemas Operativos

La Armada Nacional maneja el procedimiento de control de software para controlar la instalación de software en sistemas operativos.

Al actualizar el software operacional, aplicaciones y bibliotecas de programas solo la llevará a cabo administradores funcionales entrenados, con la autorización apropiada por la División de Informática de la Armada Nacional.

Los sistemas operacionales sólo deben contener códigos ejecutables aprobados, no el código de desarrollo o compiladores.

Las aplicaciones y el software de sistema operativo solo se deben implementar después de pruebas extensas y exitosas; y se debe llevar a cabo en sistemas separados.

4.8.6. Gestión de Vulnerabilidad Técnica

OBJETIVO:

Prevenir el aprovechamiento de las vulnerabilidades técnicas.

POLÍTICAS:

a. Gestión de las Vulnerabilidades Técnicas

La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan en la Armada Nacional, se obtendrán en el momento oportuno; se evalúa la exposición de la Armada Nacional a estas vulnerabilidades, y se toman las medidas requeridas para tratar el riesgo asociado.

DITIC a través de DINFO, se encargarán de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y definirá las herramientas o servicios necesarios por medio del Procedimiento de Gestión de Vulnerabilidades.

DITIC a través de DINFO, será el responsable 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.

No se permite a los usuarios de los activos informáticos, realizar o participar por iniciativa

propia o de terceros, en pruebas de acceso o ataques (activos o pasivos) a los activos informáticos de la Armada Nacional, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad, ataques a otros equipos o sistemas externos.

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

Se realizará, por parte del área competente, el seguimiento y verificación para las correcciones de las vulnerabilidades identificadas.

DITIC a través de DINFO, realizará 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 institucional.

b. Restricciones sobre la Instalación de Software

Se deben establecer e implementar reglas para la instalación de software por parte de los usuarios. Los funcionarios son responsables por la instalación y utilización de software no autorizado en sus equipos de cómputo y en las plataformas tecnológicas que soportan los sistemas de información de la Armada Nacional.

4.8.7. Consideraciones sobre Auditorías de Sistemas de Información

OBJETIVO:

Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

POLÍTICAS:

a. Controles de Auditoría de Sistemas de Información

La Armada Nacional, apoyada en la Dirección de Inspecciones de la Armada Nacional, a través del

procedimiento de Auditoría Interna verificará el cumplimiento de los requisitos de la norma ISO aplicables, la normatividad legal vigente, y los requisitos propios de la organización, los requisitos internos del proceso y procedimientos. Estás deberán ser acordadas y planificadas para reducir al mínimo las interrupciones en los procesos.

Se deben establecer a través de la Dirección de Inspecciones de la Armada Nacional o la que haga sus veces en cada Unidad, controles que permitan realizar auditorías, supervisión de las actividades por los técnicos responsables de la infraestructura de red y sus sistemas de información.

El alcance de las pruebas técnicas de auditoría se debe acordar y controlar, las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.

4.9. SEGURIDAD DE LAS COMUNICACIONES

4.9.1. Gestión de la Seguridad de las Redes

OBJETIVO:

Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

POLÍTICAS:

a. Controles de Redes

La Armada Nacional debe gestionar y controlar para proteger la información en sistemas y aplicaciones.

b. Seguridad de los Servicios de Red

Los mecanismos de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de la red, deben ser identificados e incluidos en los acuerdos de servicios de red de acuerdo al Procedimiento de Aseguramiento de Servicios en la Red, ya sea que los servicios se presten internamente o se contraten externamente.

c. Separación en las Redes

La plataforma tecnológica crítica de las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, 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.

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

4.9.2. Transferencia de Información

OBJETIVO:

Mantener la seguridad de la información transferida dentro de la Institución y con cualquier entidad externa.

POLÍTICAS:

a. Políticas y Procedimientos de Transferencia de Información

Las políticas formales de transferencia, procedimientos y controles deben estar en posición de proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

b. Acuerdos sobre Transferencia de Información

Todo funcionario o tercero es responsable por proteger la confidencialidad e integridad de la información de la Armada Nacional 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.

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 y disponibilidad de acuerdo a la reglamentación vigente.

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, teniendo en cuenta la Guía de Uso de Interoperabilidad Gobierno en Línea y Guía de Uso del Lenguaje Común de Intercambio de Información.

Los protocolos 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.

Cuando la información sea solicitada por autoridad judicial o administrativa competente, la entrega se realizará siguiendo el Procedimiento de Transferencia de información establecido por la Armada Nacional para la entrega de la información solicitada.

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.

c. Mensajería Electrónica

La Armada Nacional debe proteger adecuadamente la información incluida en la mensajería electrónica.

d. Acuerdos de Confidencialidad o de no Divulgación

Todos los funcionarios y terceros deben firmar la cláusula o acuerdo de confidencialidad que debe ser parte integral de los contratos, empleando la promesa de reserva 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 o a los recursos a personas o entidades externas, de acuerdo al Formato Acuerdo de Confidencialidad Armada Nacional.

4.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

4.10.1. Requisitos de Seguridad de los Sistemas de Información

OBJETIVO:

Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

POLÍTICAS:

a. Análisis y Especificación de Requisitos de Seguridad de la Información

Los requisitos relacionados con la seguridad de la información serán incluidos en los requerimientos para los nuevos sistemas de información o mejoras a los sistemas de información existentes de acuerdo al Procedimiento para el Desarrollo de Software en la Armada Nacional.

Los requerimientos de seguridad de la información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura.

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 para el Control de Cambios en Aplicaciones de Software de la Armada Nacional y formato de Control de Cambios.

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

Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado mediante formato solicitud uso sistemas de información y/o base de datos.

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.

b. Seguridad de los Servicios de las Aplicaciones en Redes Públicas

La información pública producida por las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional, de acuerdo con los parámetros y normatividad vigente e impartida por el Grupo de Comunicaciones Estratégicas de la Institución.

Todo portal institucional deberá contener la política de privacidad y uso, así como, seguir un procedimiento de desarrollo y ciclo de vida del software, emitido por DITIC, con el fin de garantizar la seguridad del mismo y crear un estándar para los distintos portales institucionales.

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, deberán garantizar el derecho de Habeas Data y la Ley de transparencia 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.

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.

La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

c. Protección de Transacciones de los Servicios de las Aplicaciones

La información de la Armada Nacional involucrada en las transacciones de servicios de

aplicaciones deberá ser protegida para prevenir la transmisión incompleta, mal enrutamiento, alteración de mensaje no autorizado, la divulgación no autorizada, la duplicación o la reproducción de mensajes no autorizados.

4.10.2. Seguridad en los Procesos de Desarrollo y Soporte

OBJETIVO:

Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

POLÍTICAS:

a. Política de Desarrollo Seguro

Se establecerán y aplicarán reglas para el desarrollo de software y de sistemas en la Armada Nacional.

b. Procedimientos de Control de Cambios en Sistemas

Los cambios a los sistemas dentro del ciclo de vida de desarrollo en la Armada Nacional se deben controlar mediante el uso de procedimiento de Control de Cambios en Aplicaciones de Software en la Armada Nacional.

c. Revisión Técnica de las Aplicaciones después de Cambios en la Plataforma de la Operación

Cuando se cambien las plataformas de operación, se debe revisar las aplicaciones críticas de la Armada Nacional, y ponerlas a prueba, para asegurar que no haya impacto adverso en las operaciones o seguridad de la información.

Se debe asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo, para permitir las pruebas y revisiones apropiadas antes de la implementación.

d. Restricciones en los Cambios a los Paquetes de Software

La Armada Nacional debe desalentar las

modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios serán controlados estrictamente.

e. Principios de Construcción de los Sistemas Seguros

Se aplicarán, documentarán y mantendrán los principios de construcción de sistemas seguros a todas las actividades de implementación de sistemas de información de acuerdo al Procedimiento para el desarrollo de software en la Armada Nacional.

f. Ambiente de Desarrollo Seguro

La Armada Nacional establece y protege adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de software.

g. Desarrollo Contratado Externamente

La Armada Nacional debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

h. Pruebas de Seguridad de Sistemas

Las pruebas de funcionalidad de la seguridad se deben llevar a cabo durante el desarrollo del sistema.

i. Prueba de Aceptación de Sistemas

Para los sistemas de información nuevos, actualizaciones y nuevas versiones, la Armada Nacional establece programas de prueba para aceptación y criterios de aceptación.

4.10.3. Datos de Prueba

OBJETIVO:

Asegurar la protección de los datos usados para pruebas.

POLÍTICAS:

a. Protección de Datos de Prueba

Los datos de prueba que se utilicen en la Armada Nacional serán seleccionados, protegidos y controlados cuidadosamente.

En la Armada Nacional la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.

Se debe establecer que el copiado y uso de la información operacional debe realizar una grabación en el log para suministrar un rastro de auditoría.

4.11. RELACIÓN CON LOS PROVEEDORES

4.11.1. Seguridad de la Información en las Relaciones con los Proveedores

OBJETIVO:

Asegurar la protección de los activos de la Armada Nacional que sean accesibles a los proveedores.

POLÍTICAS:

a. Política de Seguridad de la Información para las Relaciones con Proveedores

Cuando exista la necesidad de trabajar con partes externas y se requiera acceso a la información, datos de la institución, a sus plataformas tecnológicas, sistemas de información, procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte externa, se debe realizar una evaluación de riesgos para determinar las implicaciones para la seguridad de la información de la Armada Nacional y los requisitos de control.

Se deberá diligenciar el documento de aceptación, conocimiento y cumplimiento de las Políticas de Seguridad de la Información para la Armada Nacional, la promesa de reserva, Formato de acuerdo de confidencialidad previa realización de los estudios de seguridad pertinentes tanto a

la empresa como a los funcionarios o empleados de las terceras partes involucradas.

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

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 defina las condiciones para la conexión o el acceso.

El acceso de terceros a la información, datos y sistemas de la institución, no se debe brindar hasta haber implementado los controles apropiados y cuando es viable firmar un contrato que defina los términos y las condiciones para la conexión o el acceso y el acuerdo de trabajo, además de firmar la promesa de reserva.

b. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores

Se deben tener en cuenta las responsabilidades derivadas de las leyes nacionales y debe haber restricciones contra la copia y la revelación no autorizada de información institucional.

Se deberá explicar al funcionario, el contratista o usuario de tercera parte sobre las acciones de carácter legal, administrativo, penal, disciplinario o civil, a que puede estar sujeto, si viola u omite el cumplimiento de las normas de seguridad o la violación de la reserva establecida en la institución.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de

sistemas de información, redes 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, conozcan 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 unidades y dependencias de la Armada Nacional.

c. Cadena de Suministro de Tecnología de Información y Comunicación

La Armada Nacional debe incluir en sus acuerdos con los proveedores requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

4.11.2. Gestión de la Prestación de Servicios con los Proveedores

OBJETIVO:

Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

POLÍTICAS:

a. Seguimiento y Revisión de los Servicios de los Proveedores

Cada servicio con proveedor deberá tener un supervisor encargado de revisar y auditar la prestación de servicios de proveedores.

b. Gestión de Cambios en los Servicios de Proveedores

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de la información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

4.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.12.1. Gestión de Incidentes y Mejoras en la Seguridad de la Información

OBJETIVO:

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

POLÍTICAS:

a. Responsabilidades y Procedimientos

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la información.

Se debe establecer y mantener actualizado un directorio de los encargados de la Gestión de Incidentes de Seguridad de la Unidad, el cual consolidará el OSI y remitirá lo pertinente al OSGSI.

El OSGSI deberá difundir el directorio consolidado de los OSI de las unidades de la Armada Nacional.

Se debe llevar un registro físico 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 y las acciones tomadas de acuerdo al formato gestión de incidentes de seguridad de la información.

Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de gestión de incidentes de seguridad para cada una de las unidades de la Armada Nacional.

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.

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

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

Las unidades de la Armada Nacional 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.

En caso de presentarse una investigación, el OSGSI, OSI, CSIRT con apoyo del asesor jurídico de la Unidad deberá realizar seguimiento a los avances de la misma. De igual forma debe coordinar y 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.

b. Reporte de Eventos de Seguridad de la Información

Los funcionarios y terceros deberán informar al OSI de la Unidad cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y/o disponibilidad de la información, quien lo evaluará e informará al OSGSI de la Armada Nacional de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

c. Reporte de Debilidades de Seguridad de la Información

Los funcionarios y terceros deberán informar al OSI de la Unidad cualquier debilidad de seguridad de la información observada o sospecha de la misma en los sistemas y servicios, quien lo evaluará e informará al OSGSI de la Armada Nacional de acuerdo al con el procedimiento de Gestión de Incidentes de Seguridad.

d. Evaluación de Eventos de Seguridad de la Información y Decisiones Sobre Ellos

Los eventos de seguridad de la información los evalúa el OSI de la Unidad e informará al OSGSI de la Armada Nacional de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

Todos los incidentes informáticos deben ser reportados y se deberá adelantar un análisis con un informe escrito y detallado que identifique el incidente, los resultados, acciones tomadas y recomendaciones, el cual debe ser enviado al OSGSI de la Armada Nacional quien coordina con JINA.

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

e. Respuesta a Incidentes de Seguridad de la Información

La Armada Nacional da respuesta a los incidentes

de seguridad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

f. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

Los conocimientos adquiridos en la Armada Nacional a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

g. Recolección de Evidencia

La Armada Nacional debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.

4.13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

4.13.1. Continuidad de Seguridad de la Información

OBJETIVO:

La continuidad de seguridad de la información se deberá incluir en los sistemas de gestión de continuidad del negocio de la Armada Nacional.

POLÍTICAS:

a. Planificación de la Continuidad de la Seguridad de la Información

La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso del Alto Mando.

Las unidades y dependencias que conforman la Armada Nacional deberán contar con un Plan de Continuidad que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales como sismos, terremotos, tsunami, etc.

Para la Armada Nacional su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades, estarán incorporados y definidos en el Plan de Continuidad Tecnológica de la Armada Nacional.

Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados.

b. Implementación de la Continuidad de la Seguridad de la Información

La Armada Nacional debe seguir una estrategia de recuperación alineada con los objetivos, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante cualquier contingencia de acuerdo a los lineamientos del Plan de Continuidad Tecnológica de la Armada Nacional.

La Armada Nacional deberá establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

c. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información

La Armada Nacional debe verificar la información de continuidad de los controles de seguridad establecidos y aplicados a intervalos regulares con el fin de asegurarse que son válidos y eficaces en situaciones adversas.

4.13.2. Redundancias

OBJETIVO:

Asegurar la disponibilidad de instalaciones de procesamiento de información.

POLÍTICAS:

a. Disponibilidad de Instalaciones de Procesamiento de Información

Las instalaciones para el procesamiento de

información deben cumplir con los lineamientos de la Norma Técnica TIA 942 que rige los centros de datos a nivel Mundial.

4.14. CUMPLIMIENTO

4.14.1. Cumplimiento de Requisitos Legales y Contractuales

OBJETIVO:

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

POLÍTICAS:

a. Identificación de la Legislación Aplicable y de los Requisitos Contractuales

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la Armada Nacional para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la Institución.

b. Derechos de Propiedad Intelectual

Las Jefaturas, Comandos de Fuerza, Escuelas de Formación y unidades de la Armada Nacional, cumplirán con la reglamentación vigente sobre propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.

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

Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de

preservar los derechos morales e intelectuales de las obras o referencias citadas.

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

El software a la medida, adquirido a terceras partes que correspondan a desarrollos a la medida al igual que los desarrollos que tenga participación de funcionarios de la Armada Nacional, deben quedar registrados ante la Dirección Nacional de Derechos de Autor (DNDA) y el registro quedará a nombre de la Armada Nacional.

c. Protección de Registros

Los registros en los sistemas de información se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los registros legislativos, reglamentación contractual y comercial.

d. Privacidad y Protección de Datos Personales

Cuando sea aplicable, se debe asegurar la privacidad y protección de la información de datos personales, como exige la legislación y la reglamentación pertinentes.

e. Reglamentación de Controles Criptográficos

Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y la reglamentación, pertinentes.

4.14.2. Revisiones de Seguridad de la Información

OBJETIVO:

Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos Institucionales.

POLÍTICAS:

a. Revisión Independiente de la Seguridad de la Información

El enfoque de la organización para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

b. Cumplimiento con las Políticas y Normas de Seguridad

Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

c. Revisión del Cumplimiento Técnico

Los sistemas de información de la Armada Nacional se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

FUENTES BIBLIOGRÁFICAS

1. ISO 27001:2013.

FUENTES DOCUMENTALES Y JURÍDICAS

1. Constitución Política de Colombia.
2. Ley 527 de 1999.
3. Ley 1221 de 2008 "Teletrabajo".
4. Ley 1273 de 2009.
5. Ley 1581 de 2012.
6. Decreto 1377 de 2013.
7. Ley 1712 de 2014.

FUENTES INSTITUCIONALES

1. DIR2014-18 Ministerio de Defensa del 19 de junio de 2014 "Políticas de seguridad de la información para el sector defensa".
2. CIRCULAR 233 MDN-CGFM-CARMAR-AYGAR-JAGCA-95.5 del 12 de diciembre de 2014.
3. Directiva Permanente 001/MDN-CGFM-CARMA-SECAR-JINA-DICOI-23.1 del 12 de enero de 2017.

FUENTES ELECTRÓNICAS

1. Sistema de Gestión de Seguridad de la Información. https://www.incibe.es/
2. Sistema de Gestión de Seguridad de la Información iso 27001. http://www.iso27000.es/
3. Leyes relacionadas con seguridad de la información. http://www.secretariasenado.gov.co


ARMADA REPÚBLICA DE COLOMBIA
JEFATURA DE FORMACIÓN, INSTRUCCIÓN Y EDUCACIÓN NAVAL
DIRECCIÓN DE DOCTRINA