Ministerio de Defensa Nacional

Dirección General Marítima
Autoridad Marítima Colombiana

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

Contenido

1. JUSTIFICACIÓN DE LA POLÍTICA

La Política de Seguridad y Privacidad de la Información tiene como objetivo principal establecer reglas generales sobre el uso de la información, activos de información, sistemas informáticos y de comunicaciones por parte de los usuarios, administradores o terceros que tengan acceso a ellos y de esta manera, proteger los recursos de información de la Dirección General Marítima - DIMAR y la tecnología utilizada para su procesamiento, frente a las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información a partir de los lineamientos definidos por la norma ISO 27001:2013 y las directrices nacionales definidas por el Modelo de Seguridad y Privacidad de la Información - MSPI.

La Política de Seguridad y Privacidad de la Información establece controles, que regulan de manera efectiva el acceso de los usuarios a los sistemas a nivel de aplicación, sistema operativo, base de datos, red acceso físico y acceso remoto, orientados a adoptar las mejores prácticas sobre seguridad de la información.

2. DECLARACIÓN DE LA POLÍTICA

La Dirección General Marítima, entendiendo que la información es uno de sus activos más valiosos y de mayor importancia, se ha comprometido con la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión, visión, estrategias y necesidades de la Dirección y orientado al cumplimiento de estándares internacionales como ISO 27000:2013 y las directrices nacionales definidas en el Modelo de Seguridad y Privacidad de la Información - MSPI.

Para la Dirección General Marítima, la protección y el buen uso de la información busca la disminución del impacto generado por amenazas y riesgos a los que está expuesta, comprometiéndose así a mantener un nivel de exposición de los activos de información, que permita responder por la confidencialidad, integridad y la disponibilidad de los activos de información.

3. ALCANCE DE LA POLÍTICA

La Dirección General Marítima protegerá todos los activos de información, especialmente la información física y electrónica que almacene, produzca y gestione a través de la implementación de controles físicos y lógicos, realizando una efectiva gestión de riesgos y un proceso de mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la Entidad.

La Política de Seguridad y Privacidad de la Información es el eje principal del Sistema de Gestión de Seguridad de la Información -SGSI, proporcionando los lineamientos generales requeridos para implementar un modelo de seguridad de la información confiable y flexible y definiendo el marco básico que guiará la implementación de cualquier directriz, proceso, procedimiento, estándar o acción, relacionados con la seguridad de la información.

La DIMAR en el marco de la presente Política de Seguridad y Privacidad de la Información implementará controles de forma transversal a todos los procesos de la Entidad buscando

permear el quehacer de funcionarios, contratistas, operadores tecnológicos (en el caso que los haya) y demás partes interesadas, teniendo en cuenta que la seguridad de la información es fundamental para cumplir la misionalidad de la Entidad.

4. LINEAMIENTOS ASOCIADOS A LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

4.1 RESPONSABILIDAD Y AUTORIDAD

La DIMAR, para la implementación de la dimensión de arquitectura organizacional en lo que respecta a los sistemas de información y la infraestructura tecnológica y de acuerdo con las normatividades definidas por el gobierno central, deberá crear un Comité de Seguridad de la Información y Gobierno Digital el cual tendrá las siguientes funciones:

- Aprobar los lineamientos y metodologías relacionadas con la seguridad de la información y gobierno digital.
- Coordinar la implementación de los modelos de gobierno digital y de seguridad de la información.
- Revisar el avance en la implementación de los modelos de gobierno digital y de seguridad de información.
- Aprobar lineamientos, metodologías y prácticas al interior de la Dirección para la implementación de las estrategias demarcadas en los modelos descritos.
- Diseñar las estrategias para la apropiación de los modelos de gobierno digital y de seguridad de la información.
- Mantener el modelo de gobierno digital y de seguridad de la información.

El Comité de Seguridad de la Información y Gobierno Digital propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de la presente política.

Todo el personal de la Entidad es responsable de la implementación y cumplimiento de la Política de Seguridad de la Información dentro de sus dependencias.

El comité de Gestión y Desempeño Institucional aprobará esta política y es responsable de la autorización de sus modificaciones a la par con la Dirección de la Entidad.

4.1.1. Responsabilidad del Coordinador del Grupo de Informática y Comunicaciones CGRUINCO

- Controlar la existencia de documentación actualizada relacionada con los servicios de comunicación y las operaciones que deben ser administrados y gestionados por GRUINCO como parte de su quehacer diario.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y verificar su correcta implementación, asignando responsabilidades y gestionando un comité de cambios.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento de información.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

- Verificar el control de la realización de las copias de respaldo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo de GRUINCO, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de documentos para comunicar las fallas en el procesamiento de la información, sistemas de información y/o comunicaciones, que permita tomar medidas correctivas.
- Gestionar la implementación de los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar documentos para la administración de medios informáticos de almacenamiento, como cintas, discos, USB y la eliminación segura de los mismos.
- Definir y verificar el cumplimiento de los controles establecidos en el gobierno de Office 365.

4.1.2. Responsabilidades de los funcionarios

- Reportar con diligencia, prontitud y responsabilidad presuntas violaciones de seguridad a través de su jefe de dependencia y al Grupo de Informática y Comunicaciones, el cual debe proporcionar las herramientas informáticas para contrarrestar el incidente.
- Entregar la información almacenada en dispositivos personales que sean utilizados por los servidores públicos, proveedores y contratistas para adelantar sus funciones en la DIMAR, teniendo en cuenta que la información almacenada, procesada y generada a través de estos medios, se considera propiedad de la Entidad y el uso inadecuado de estos puede conllevar a las sanciones disciplinarias y legales correspondientes.
- Los servidores, contratistas y proveedores de la DIMAR tienen la obligación de conocer y cumplir lo establecido en la "Política de Seguridad y Privacidad de la Información" y en el "Manual de Seguridad y Privacidad de la Información" y propender por la integridad, disponibilidad y confidencialidad de esta, so pena que la Entidad tome las medidas disciplinarias, legales y administrativas correspondientes.
- Los servidores y contratistas de la DIMAR deben almacenar la información de la entidad únicamente en los medios designados por la Entidad, tales como: servidor de archivos, almacenamiento en la nube, medios magnéticos, entre otros. Una vez finalizada la vinculación con la Dirección, se deberá entregar toda la información procesada dentro de los equipos a cargo, al jefe inmediato o al supervisor del contrato y hacer entrega del inventario correspondiente al jefe inmediato.
- Los servidores, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la Entidad, tales como escritorios remotos y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros. Los dispositivos móviles de propiedad de la Entidad son de estricto uso para el cumplimiento de la misionalidad de la misma y por ende se deben gestionar desde GRUINCO.
- Las credenciales de acceso a la red y a recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los servidores y

contratistas de la DIMAR no deben revelar éstas a terceros ni utilizar claves ajenas. Todo funcionario y contratista será responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

- Todos los funcionarios y contratistas de la DIMAR son responsables de hacer un uso adecuado del internet y cumplir con las políticas para tal fin.
- Los funcionarios y contratistas deben adelantar los procesos correspondientes para retirar de las sedes de la DIMAR, dispositivos informáticos o que contengan información de la Entidad, contando con los vistos buenos de los responsables de la misma y los jefes inmediatos correspondientes.
- Todos los funcionarios y contratistas de la Entidad deben asistir a las diferentes capacitaciones, socializaciones y transferencias de conocimiento cuyo tema sea seguridad de la información, en pro de garantizar la confidencialidad, integridad y disponibilidad de los activos de la DIMAR.

4.2 ORGANIZACIÓN DE LA SEGURIDAD

4.2.1. Consideraciones generales

- Todo personal de la DIMAR cualquiera sea su situación contractual, debe dar cumplimiento a la política y lineamientos de seguridad de la información.
- El líder de la seguridad de la información será el encargado de impulsar la implementación de la presente Política.
- El Comité de Seguridad de la Información y Gobierno Digital tendrá a cargo el seguimiento de las actividades relativas a la seguridad de la información.
- El líder de la seguridad de la información tendrá a cargo el asistir al personal de la DIMAR en materia de seguridad de la información y coordinará la interacción con entidades especializadas. Así mismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la DIMAR y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.
- La Subdirección Administrativa y Financiera – SUBAFIN cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.
- La Subdirección Administrativa y Financiera – SUBAFIN, las Intendencias Regionales, y el líder de seguridad de la información definirán un acuerdo de confidencialidad, el cual debe ser firmado y cumplido por todas las personas que tengan acceso a información o activos de información de la DIMAR.

4.2.2. Procesamiento de la información

- Es responsabilidad del Director, Subdirectores, Jefes de Área, Coordinadores o Jefes de oficina, simultáneamente con el Coordinador del Grupo de Informática y Comunicaciones - CGRUINCO, autorizar o no, el uso de nuevos recursos de procesamiento de información y propender que se cumplan todas las políticas y requerimientos de seguridad pertinentes.

- Es responsabilidad del Coordinador del Grupo de Informática y Comunicaciones y del responsable del área al que se destinen los recursos tecnológicos, autorizar o no el uso de recursos personales de procesamiento de información en el lugar de trabajo, previa evaluación de cada caso por el personal de apoyo.

4.2.3. Asesoramiento especializado

- El líder de la seguridad de la información será el encargado de coordinar los conocimientos y las experiencias disponibles en la Entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad de la información.
- El líder de la seguridad de la información podrá obtener asesoramiento de entidades especializadas con el objeto de optimizar su gestión en seguridad de la información de la DIMAR.
- El líder de la seguridad de la información debe garantizar que se establezcan los acuerdos de confidencialidad a los que haya lugar, previo al intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias con aquellas organizaciones especializadas en temas relativos a la seguridad de la información.

4.2.4. Revisión independiente

El Grupo de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información y Gobierno Digital, debe realizar revisiones independientes sobre la vigencia e implementación de la Política de Seguridad y Privacidad de la Información, a efectos de garantizar que las prácticas de la DIMAR reflejen adecuadamente sus disposiciones y se pueda generar el mejoramiento continuo del sistema.

4.2.5. Acceso a la información por parte de terceros

- El líder de la seguridad de la información y el propietario de la información, deben llevar a cabo una evaluación de riesgo para identificar los requerimientos de controles específicos antes de otorgar acceso a terceras partes a la información de la DIMAR.
- El líder de la seguridad de la información y el propietario de la información deben realizar un documento/acta que describa dicha evaluación y la decisión tomada respecto a dar acceso a terceros, debidamente firmada.

4.3 GESTIÓN DE ACTIVOS

4.3.1. Responsabilidades generales

- Es responsabilidad de los propietarios de la información el inventariar, clasificar, documentar y mantener actualizada la información a su cargo de acuerdo con su grado de sensibilidad y criticidad, así como definir los permisos de acceso a la misma.
- El líder de la seguridad de la información debe asegurar que los lineamientos para la utilización de los recursos de la tecnología de la información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan. Los controles y riesgos definidos para cada caso.

4.3.2. Inventario de activos

- Es responsabilidad del Director, Subdirectores, Jefes de área, Coordinadores o Jefes de Oficina, identificar los activos de información asociados a cada sistema de información, sus respectivos propietarios y su ubicación.
- Es responsabilidad del Director, Subdirectores, Jefes de Área, Coordinadores o Jefes de Oficina, el mantener actualizado el inventario de activos de información, el cual debe ser revisado con una periodicidad no mayor a un (1) año y actualizado cada vez que se requiera el ingreso de nuevos registros.

4.3.3. Clasificación de la información

- Solo el propietario de la información, puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

  - Asignarle una fecha de efectividad.

  - Comunicárselo al custodio del recurso.

  - Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

- Es responsabilidad de los propietarios de la información, luego de clasificarla, identificar los recursos asociados (sistemas, equipamiento, servicios, entre otros) y los perfiles funcionales que deberán tener acceso a la misma.
- La clasificación de la información en la DIMAR se basa en la confidencialidad como el principio más importante, buscando contemplar el impacto que causaría sobre el activo de información, la pérdida de alguna de las propiedades de seguridad de la información (confidencialidad, integridad y disponibilidad).
- Para cada una de las propiedades se establecen los criterios específicos y lineamientos para el tratamiento adecuado de los activos de información e igualmente se definen cuatro (4) niveles que permiten determinar el valor del activo de información de acuerdo con la Ley 1712 de 2014.

  - **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

  - **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el Artículo 18 de la Ley 1712 de 2014.

  - **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el Artículo 19 de la Ley 1712 de 2014.

- **Información sin clasificar:** Es aquella información que aún no tiene definida una clasificación dependiendo del contenido de la misma.

4.4 SEGURIDAD DE LOS RECURSOS HUMANOS

4.4.1. Responsabilidades generales

El líder de seguridad de la información debe hacer el seguimiento, documentación y análisis de los incidentes de seguridad reportados y comunicar al comité de Seguridad de la Información y Gobierno Digital, y a los propietarios de la información y de ser necesario solicitar al secretario del comité citación extraordinaria.

El Comité de Seguridad de la Información y Gobierno Digital será responsable de implementar los medios y canales necesarios para que el líder de seguridad de la información maneje los reportes de incidentes y anomalías de los sistemas. Así mismo, dicho comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

Todo el personal de la DIMAR es responsable del reporte de debilidades e incidentes de seguridad que se detecten.

4.4.2. Antes de asumir el empleo

Es responsabilidad de todos los funcionarios, cualquiera sea su situación, firmar un compromiso de confidencialidad y no divulgación, en lo que respecta al tratamiento de la información de la Entidad; así mismo, el conocimiento, entendimiento y aceptación de la presente Política.

4.4.3. Durante la ejecución del empleo

- Es responsabilidad del Grupo de Informática y Comunicaciones y puntualmente del del líder de seguridad de la información, el coordinar las acciones de capacitación y/o concientización en temas de seguridad de la información por lo menos dos veces al año con la coordinación con el Grupo de Desarrollo Humano.
- Es responsabilidad y deber de cada funcionario asistir a las charlas de concientización en seguridad de la información que la Entidad programe y aplicar la seguridad según las políticas y los procedimientos establecidos.
- Todo el personal de la DIMAR debe comunicar al líder de seguridad de la Información los incidentes relativos a la seguridad de la información que perciba, a través de correo electrónico, mesa de ayuda y/o vía telefónica o con la utilización o acceso a algún activo de información.
- El líder de seguridad de la información indicará los recursos necesarios para la investigación, monitoreo y resolución del incidente. Así mismo, presentará al Comité de Seguridad de la Información y Gobierno Digital un reporte de la ocurrencia de incidentes de seguridad.

4.5 SEGURIDAD FÍSICA Y DEL ENTORNO

4.5.1. Responsabilidades generales

- Es responsabilidad de los propietarios de la información autorizar formalmente el trabajo fuera de las instalaciones con información de su interés a los funcionarios, cuando lo crean conveniente.
- Todo el personal de la DIMAR es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.
- El uso inadecuado de los recursos tecnológicos o incumplimiento a alguna de las presentes políticas dará lugar en primera instancia a llamado de atención por parte de la coordinación de GRUINCO (según informe del grupo de plataforma Redes y Seguridad Informática); de persistir y de reincidir se suspenderán los servicios a los usuarios implicados, y se informará a las segundas instancias GRUCOG y GRUDHU, por el incumplimiento de las políticas de la Entidad. En caso de considerarse el incumplimiento de mayor gravedad, se llevarán los debidos procedimientos descritos en el régimen de control interno y la normatividad aplicable en caso de presentarse un delito que afecte la seguridad de la información.
- El líder de la seguridad de la Información es el encargado de revisar que el centro de procesamiento de datos y el(los) cuarto(s) de equipos de TIC, deben de estar protegidos físicamente contra el acceso no autorizado, daño o interferencia.
- Todo equipo portátil, tablet, cámara fotográfica, USB propiedad de terceros contratistas y/o visitantes, deberá ser registrado en la guardia (recepción) de cada unidad, así mismo deberá ser inspeccionado su contenido, si el mismo va a hacer conectado a la red de la DIMAR, esta inspección deberá ser realizada por personal de GRUINCO especializado o el personal Oficial o Suboficial de guardia en las Unidades Regionales.

4.5.2. Perímetro de seguridad física

El líder de seguridad de la información debe definir y monitorear las medidas de seguridad a implementar en áreas restringidas.

Las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica y de aire acondicionado son consideradas áreas restringidas por lo tanto el área encargada debe realizar dicha marcación.

4.5.3. Controles de acceso físico

El líder de seguridad de la información determinará las áreas protegidas que se resguardarán mediante el empleo de controles de acceso físico a fin de permitir el acceso solo al personal autorizado y bajo el procedimiento de acceso definido.

4.5.4. Equipos desatendidos

- El líder de seguridad de la información debe garantizar que los equipos desatendidos sean protegidos adecuadamente por medio de la aplicación de controles técnicos que permitan el bloqueo automático por inactividad.
- Los usuarios son responsables de cumplir con las siguientes pautas: a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un

protector de pantalla protegido por contraseña. b) Proteger los computadores contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

- Está totalmente prohibido que personas ajenas a la DIMAR, utilicen los computadores y/o terminales de la Entidad, si no es autorizado por el superior jerárquico inmediato, responsable del área.
- El acceso a equipos o infraestructura ubicados en áreas restringidas, por parte de personas ajenas a la Entidad, deberán ser autorizados por el responsable del área y limitada al mantenimiento, soporte, inspecciones, programadas, transferencia de conocimiento, reparaciones, actualizaciones, ejecución de garantías, entre otras situaciones.

4.6 SEGURIDAD DE LAS OPERACIONES

4.6.1. Responsabilidades generales

El líder de seguridad de la información debe:

- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva.
- Definir el manejo de incidentes de seguridad y la administración de los medios de almacenamiento.
- Definir y documentar una guía clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información electrónica dentro de la Dirección.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y garantizar la seguridad de los datos y los servicios conectados en las redes de la Dirección.
- Desarrollar documentación adecuada de concientización de usuarios en materia de seguridad de la información.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.
- Evaluar de forma permanente los riesgos de ciberseguridad a los cuales se encuentra expuesta la entidad.
- Parametrizar dominios de confianza (Ministerio de Defensa Nacional, Armada Nacional, Comando General Fuerzas Militares, entre otros).
- Verificar el cumplimiento de los controles establecidos en el gobierno de Office 365.
- Coordinar y verificar la implementación de los controles de seguridad de la información definidos en la presente política con el área de Plataforma Redes y Seguridad del Grupo de Informática y Comunicaciones.

4.6.2. Controles contra software malicioso

- El líder de seguridad de la información debe definir controles de detección y prevención para la protección contra software malicioso.
- Es responsabilidad del Coordinador del Grupo de Informática y Comunicaciones - CGRUINCO gestionar la implementación de los controles contra software malicioso o solución informática equivalente.

- Es responsabilidad del Coordinador del Grupo de Informática y Comunicaciones – CGRUINCO gestionar los recursos para adquirir y mantener actualizado un programa de antivirus - antimalware corporativo.
- Todos los equipos informáticos de proveedores o terceros que sean autorizados para conectarse a la red corporativa de la DIMAR deben contar con una aplicación de antivirus - antimalware con su base de datos actualizada.
- El manejo de la aplicación de antivirus - antimalware corporativo para estaciones de trabajo y servidores (instalación, configuración, administración y/o desinstalación) debe ser realizado únicamente por el personal del Grupo de Informática y Comunicaciones – GRUINCO.

4.6.3. Copias de respaldo y restauración de la información

Es responsabilidad del Coordinador del Grupo de Informática y Comunicaciones – CGRUINCO:

- Determinar los requerimientos para resguardar cada software y datos en función de su criticidad.
- Disponer y revisar la realización de copias de respaldo de la información, así como asegurar que se realicen pruebas periódicas de su restauración.
- Designar un responsable para la administración y gestión de una solución de almacenamiento de información centralizada con las condiciones necesarias de seguridad de información.
- Destinar los recursos de almacenamiento para alojar información propia de la Dirección y no con fines personales del usuario.
- Implementar controles documentados para la administración de medios informáticos removibles (USB, discos externos, cintas entre otros).
- Definir procedimientos para la eliminación segura de los medios de información que se necesiten eliminar, como es el caso de CD, DVD, blue ray, cintas magnéticas, discos durso o cualquier dispositivo que pueda tener información de la Entidad.

Es responsabilidad de los usuarios:

- Mantener depurada la información de sus archivos públicos, como mejor práctica para la optimización del uso de los recursos que entrega la Entidad a su personal.

4.6.4. Registro de actividades y fallas

Es responsabilidad del Coordinador del Grupo de Informática y Comunicaciones – CGRUINCO:

- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Asegurar el registro de las actividades realizadas en los sistemas, como parte de un incidente de seguridad de la información, incluyendo según corresponda:
  - Errores del sistema y medidas correctivas tomadas.
  - Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.

- Ejecución de operaciones críticas.
- Cambios a información crítica.

4.7 SEGURIDAD DE LAS COMUNICACIONES

4.7.1. Responsabilidades generales

- El líder de seguridad de la información debe definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la DIMAR contra el acceso no autorizado.
- Salvo expresa autorización, ningún usuario está autorizado para escanear, acceder o manipular directa o indirectamente los sistemas de información y de comunicaciones de la red de datos de la DIMAR, e instalar nuevos sistemas de comunicaciones de redes que se conecten con la red de datos de la Institución.
- DIMAR, en coordinación con GRUINCO debe definir un responsable para la administración de cada red LAN en las sedes a nivel nacional, cuyas funciones y tareas estén claramente definidas y delimitadas, en apoyo de la empresa encargada del mantenimiento preventivo y correctivo de los equipos de cómputo en cada Sede, Capitanía o Centro.

4.7.2. Correo Electrónico y almacenamiento en la nube

- El líder de seguridad de la información debe definir y documentar el uso del correo electrónico que incluya los siguientes aspectos:
  - El alcance del uso del correo electrónico y el almacenamiento en la nube por parte del personal de la DIMAR.
  - Protección contra ataques al correo electrónico e información en la nube, por ejemplo, virus, interceptación, entre otros.
  - Protección de archivos adjuntos de correo electrónico o almacenados en la nube.
  - Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
  - Aspectos operativos para garantizar el correcto funcionamiento del servicio.
  - Es potestad de la Entidad, auditar los mensajes recibidos o emitidos por los funcionarios y contratistas, lo cual se incluirá en el "Compromiso de Confidencialidad".
- Los usuarios de correo electrónico no están autorizados a enviar información en forma masiva a múltiples direcciones de correo electrónico.
- Ningún usuario de correo electrónico debe modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o encabezado.
- Ningún empleado puede usar cuentas gratuitas de correo electrónico en internet para el envío de mensajes corporativos de la Entidad. Todos los mensajes de carácter corporativo deberán ser enviados a través del sistema de correo electrónico corporativo o correo autorizado como medio alterno.

- Salvo que exista una autorización, ningún funcionario o contratista está autorizado para interceptar, revelar o contribuir en la interceptación de mensajes de correo electrónico a través de herramientas de escaneo.
- Los usuarios del servicio del correo electrónico de la DIMAR no deben contestar mensajes spam.
- Ningún usuario del servicio de correo electrónico debe prestar atención a mensajes con falsos contenidos de virus, ofertas de premios, dinero, solicitudes de ayuda caritativa, venta de bienes (hardware o software) o financiamiento a muy bajo costo, productos medicinales, acceso gratuito a portales, advertencia de virus de fuentes desconocidas, entre otros.
- Para todos los funcionarios o usuarios del servicio de correo electrónico, está prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam, en esto se incluye casillas de correo, software para realizar spam, hosting de sitios de Web para realizar spam o que realicen spam, o bien que realicen bromas de mal gusto y/o fraudes, estos últimos definidos como un correo electrónico que atrae el interés del usuario y que esconde una maniobra deshonesta y brindar servicios que, de manera directa o indirecta, faciliten la proliferación de software malicioso o malware, software espía, spyware o phishing.
- A los usuarios que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asignará en el servidor una vez sean vinculados. El jefe inmediato, supervisor de contrato o el Grupo de Desarrollo Humano son los responsables de informar al Grupo de Informática y Comunicaciones - GRUINCO, las vinculaciones que requieran creación de cuenta de correo por medio de la activación del procedimiento A3-00-PRO-002 Creación Usuario de Dominio; de igual manera debe informar oportunamente los retiros de los usuarios para la suspensión de este servicio. Esta cuenta estará activa durante el tiempo que dure la vinculación del usuario con la Entidad, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la cuenta. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de ayuda por el jefe inmediato, supervisor de contrato o Grupo de Desarrollo Humano.
- El buzón de correo es personal e intransferible y corresponde al funcionario o contratista velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico.
- One Drive: No compartir información con terceros, configurar el perfil del usuario de la estación de trabajo con OneDrive, definir cuota de almacenamiento.
- Correo electrónico: Parametrizar DIM, DMARK y SPF, parametrizar el envió de correos masivos (personas autorizadas), y restringir la creación de .pst para evitar la fuga de información.

4.7.3. Conexiones a internet

- El Grupo de Informática y Comunicaciones - GRUINCO es la responsable de revisar regularmente todos los logs y archivos de auditoría de la actividad en línea de los usuarios de internet. Esta información se considera reservada.
- Es responsabilidad del Grupo de Informática y Comunicaciones – GRUINCO, evaluar e implementar las nuevas herramientas tanto de software como de hardware para que la conexión a internet sea lo más eficaz, eficiente y segura posible.
- El uso de internet debe estar destinado exclusivamente a la ejecución de las actividades de la Entidad y deben ser utilizados por el usuario para realizar las funciones establecidas para su cargo.
- El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- Queda prohibida la descarga o carga de música y videos excepto para los grupos definidos por el líder de seguridad de la información y que necesiten de este tipo de acciones para la ejecución de las funciones de su cargo (Área de Comunicaciones Estratégicas).
- Abstenerse de usar sitios que salten la seguridad del servidor de acceso a internet (proxy).
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los usuarios de la Entidad; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.
- Periódicamente se deben generar reportes que muestren, entre otros, información acerca del nombre de sitios visitados, duración, estaciones desde las cuales se accedió al servicio y cualquier otra que se estime conveniente. Cualquier anomalía deberá ser reportada a la Coordinación GRUINCO.

4.7.4. Carga y descarga de archivos

- Los ingenieros del Grupo de Informática y Comunicaciones - GRUINCO están autorizados para realizar una evaluación de virus a los archivos descargados por medio de internet.
- Los usuarios deben cumplir los requerimientos de licencia y las restricciones de copia asociadas con cualquier archivo descargado.
- El personal técnico del Grupo de Informática y Comunicaciones – GRUINCO o en el caso de un tercero que preste el soporte técnico, tendrá los permisos para instalar los archivos (ejecutables) absolutamente necesarios para las funciones de la DIMAR.

4.8 CONTROL DE ACCESO

4.8.1. Consideraciones generales

- El líder de seguridad de la información debe definir la gestión de accesos a todos los sistemas, bases de datos y servicios de información de la DIMAR incluyendo accesos a internet, el uso de computación móvil, teletrabajo y trabajo remoto.
- El líder de seguridad de la información debe verificar el cumplimiento de las pautas establecidas relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, registro de eventos, protección de puertos, segmentación de redes, control de conexiones a la red y control de ruteo de red.
- Es responsabilidad del líder de seguridad de la información gestionar campañas de concientización al personal sobre el uso apropiado de usuarios y contraseñas.
- Es responsabilidad del personal que apoya la gestión en el Grupo de Informática y Comunicaciones - GRUINCO cumplir con las siguientes funciones:

  - Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes y aplicativos.

  - Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

  - Implementar el control de puertos, de conexión a la red y de ruteo de red.

  - Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

  - Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera que garanticen la seguridad en su operación.

  - Analizar las medidas a ser implementadas para el control de acceso a internet de los usuarios.

  - Otorgar acceso a los servicios y recursos de red de acuerdo con las restricciones correspondientes y a partir de la solicitud formal respectiva.

  - Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

4.8.2. Creación y eliminación de usuarios (internos y externos)

- Los funcionarios, contratistas, outsourcing o terceros, antes de solicitar acceso a los sistemas de información deben firmar un acuerdo de confidencialidad.
- Las cuentas de usuario de los sistemas informáticos otorgados a los funcionarios de la DIMAR o terceros constituyen un activo de la compañía que permite identificar de manera única e irrepetible a cada usuario. En ninguna circunstancia las cuentas de usuario deberán ser compartidas, transferidas, reasignadas o su contraseña revelada.

- Las cuentas de usuario (internas/externas) creadas en los sistemas de información de la DIMAR deben tener un identificador único y deberán solicitarse mediante un requerimiento formal, especificando su identificación, nombres, apellidos y las funciones que va a desempeñar, y contar con autorización del Jefe Inmediato del usuario, tal como lo define el procedimiento A3-00-PRO-002 Creación usuario de dominio. Las cuentas de usuarios externos deben ser solicitadas y autorizadas a través del Director de la Dirección General Marítima o quien esté autorizado para tal fin, de acuerdo con el procedimiento citado anteriormente.
- La creación de cuentas genéricas, deben contar con el aval de la Dirección, Subdirección, Oficina o Área correspondiente. La persona responsable de su utilización es la encargada de notificar las novedades correspondientes de la cuenta y asignar un custodio o responsable de la misma.
- En el momento en que un funcionario o contratista se retire de la Entidad, el Jefe inmediato debe notificar su retiro conforme al procedimiento A3-00-PRO-002 Creación usuario de dominio, al administrador de los sistemas de información y revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-empleado.
- Los Jefes inmediatos están obligados a reportar, cualquier novedad que se presente con sus funcionarios o contratistas tales como vacaciones, licencias, incapacidades, etc., de acuerdo con el procedimiento A3-00-PRO-002 Creación usuario de dominio, para que se gestione ante el administrador de los sistemas de información, la solicitud de inactivación temporal.
- Las cuentas que no hayan sido utilizadas en los últimos treinta (30) días deben ser inactivadas de manera automática, dependiendo del caso.

4.8.3. Administración de privilegios

Los propietarios de activos de información deben aprobar o negar la asignación de privilegios a usuarios y solicitar su gestión en los diferentes sistemas de información a los que corresponda, todo bajo la supervisión del líder de seguridad de la información.

4.8.4. Administración de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, para lo cual deben cumplir, como mínimo, los siguientes lineamientos:

- Mantener las contraseñas en secreto.
- Pedir o generar el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo con las recomendaciones del personal del Grupo de Informática y Comunicaciones – GRUINCO y en cumplimiento de los siguientes parámetros:

  - Sean fáciles de recordar.

- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar contraseñas antiguas.
- Cambiar la contraseña provisional definida para el primer inicio de sesión.
- Notificar cualquier incidente y /o evento de seguridad relacionado con sus contraseñas, tal como pérdida o indicio de pérdida de confidencialidad.
- No deben estar basadas en algún dato personal que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona.
- Las “claves” de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 08 (ocho) caracteres, sin utilizar espacios en blanco. Deben contener tanto caracteres alfabéticos como numéricos, y al menos 4 (cuatro) caracteres distintos entre sí.

• Se debe mantener en un sobre sellado y bajo la responsabilidad de la Coordinación de GRUINCO un código de usuario de contingencia y respectiva “clave”, el cual debe poseer todos los privilegios del administrador de la red, administrador de base de datos, administrador de sistemas de información u otros, para ser utilizado solamente en caso de emergencia. De llegar a requerirse su uso, se debe documentar y dejar por escrito los motivos de acceso y los cambios realizados. Una vez se termine de adelantar los ajustes, se debe cambiar la clave y volver a dejar el sobre con la clave nueva en las condiciones iniciales. La “clave” debe ser cambiada periódicamente mínimo dos veces al año o cuando sea necesario.

4.8.5. Acceso a la red

- Únicamente se debe proporcionar a los funcionarios o contratistas el acceso a los servicios para los que específicamente se les haya autorizado su uso.
- Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos.
- Se deben implantar controles adicionales para el acceso por redes inalámbricas.
- Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

4.8.6. Autenticación de usuarios para conexiones externas

El acceso de usuarios remotos estará sujeto al cumplimiento de las directrices de autenticación correspondientes. El líder de seguridad de la información, junto con el propietario del activo de información de que se trate, deben realizar una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso y adelantar los procedimientos técnicos definidos.

4.8.7. Control de acceso al sistema operativo

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad y cuyo usuario tenga los roles correspondientes para adelantar las acciones respectivas a su perfil.

4.8.8. Control de acceso dispositivos móviles

- Los funcionarios o contratistas se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la Entidad, tales como escritorios remotos, sistemas de comunicación, redes y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros.
- El área de Plataforma Redes y Seguridad del Grupo de Informática y Comunicaciones debe controlar la configuración de aplicaciones de Office 365 en dispositivos móviles personales que no están autorizados.

4.9 DESARROLLO Y MANTENIMIENTO DE LOS SI

4.9.1. Responsabilidades generales

- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.
- Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal del Grupo de Informática y Comunicaciones – GRUINCO, siempre y cuando haya el personal idóneo para adelantar el proceso.
- El Grupo de Informática y Comunicaciones - GRUINCO debe elegir, elaborar, mantener y difundir el “Método de desarrollo de sistemas software en la Dirección General Marítima - DIMAR” que incluya lineamientos, procesos, buenas prácticas, plantillas y demás documentos que sirvan para regular el desarrollo de software interno en un ambiente de mitigación del riesgo y aseguramiento de la calidad.
- Todo proyecto de desarrollo de software interno debe contar con un documento de “Identificación y valoración de riesgos del proyecto”. La Entidad no debe emprender procesos de desarrollo – o mantenimiento – de sistemas de software que tengan asociados riesgos altos no mitigados.
- Se deben definir ambientes para desarrollo de sistemas de información que como mínimo deben estar definidos en desarrollo, pruebas y producción.
- Los sistemas de software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.
- El Líder de Seguridad de la Información define lineamentos y coordina con el área de Plataforma Redes y Seguridad, la implementación de mínimo los siguientes controles:
  - Guardar solo los ejecutables en el ambiente de producción.
  - Llevar un registro de auditoría de las actualizaciones realizadas.
  - Retener las versiones previas del sistema, como medida de contingencia.

- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones pertinentes, las pruebas previas a realizarse y el protocolo correspondiente para la gestión del cambio.
- Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
- Evitar que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.
- Adelantar pruebas de seguridad, antes de colocar el sistema en producción.
- Definir políticas de desarrollo seguro.

4.10. ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

La Dirección General Marítima -DIMAR diseñará y mantendrá vigente un plan de continuidad del negocio que atienda los requerimientos de seguridad de la información en la Entidad según el análisis de riesgos determinado para tal fin.

4.11. SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

En todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar acuerdos de confidencialidad sobre el manejo de la información, acorde con las directrices de la Subdirección Administrativa y Financiera – SUBAFIN, y con las disposiciones legales correspondientes.

Los Acuerdos de Confidencialidad de la Información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes, los niveles de responsabilidad y los controles de seguridad que se deben seguir, con apoyo del líder de seguridad de la información.

4.12. CUMPLIMIENTO

4.12.1. Política para el Cumplimiento y Normatividad Legal

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Entidad.

La base fundamental de las normas que rigen el presente documento y el sistema de seguridad de la información se encuentran definidas en el numeral 5 de este documento.

4.12.2. Estándares de la Política para el Cumplimiento y Normatividad Legal

4.12.2.1. Cumplimiento legal

Todos los requerimientos contractuales y legales que puedan afectar los sistemas de información deben definirse previamente y documentarse de acuerdo con la metodología empleada por la Entidad. Los controles específicos, medidas de protección y responsabilidades individuales que cumplan con los requerimientos, deben así mismo, definirse y documentarse. El Grupo Legal Marítimo asesorará al Comité de Seguridad de la Información y Gobierno Digital en dichos aspectos legales específicos.

4.12.2.2. Propiedad intelectual

Se protegerá adecuadamente la propiedad intelectual de la Entidad, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario.

4.12.2.3. Protección de datos

Los estándares de seguridad de la información son de obligatorio cumplimiento para los colaboradores con acceso a los datos de carácter personal y a los sistemas de información.

Deberán considerar, los siguientes aspectos:

- Ámbito de aplicación del procedimiento de protección de datos con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por la ley frente a protección de datos.
- Funciones y obligaciones del personal con acceso a las bases de datos.
- Estructura de las bases de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante los incidentes.
- Procedimientos de realización de copias de respaldo y de recuperación de los datos.
- Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad de información que se implemente.
- Medidas a adoptar cuando un soporte o documento va a ser transportado, desechado o reutilizado.
- Adelantar los reportes de las bases de datos con información personal, con la frecuencia definida por el ente regulador.

- El procedimiento se mantendrá actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización.

4.12.3. Cumplimiento de la Política de Seguridad y Privacidad de la Información

- Cada responsable de la Entidad (Director, Subdirectores, Jefes de Área, Coordinadores o Jefes de Oficina) deben velar por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.
- El líder de seguridad de la información y el Coordinador del Grupo de Informática y Comunicaciones, deben realizar revisiones periódicas de todas las áreas de la DIMAR a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- El Líder de Seguridad de la Información y el coordinador del Grupo de Informática y Comunicaciones – GRUINCO deben comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad.
- El Líder de Seguridad de la Información debe realizar auditorías periódicas con ayuda de herramientas automatizadas y se deben generar informes técnicos que reflejen la evaluación de riesgos de seguridad de la información, las vulnerabilidades y su grado de exposición al riesgo.

5. MARCO JURÍDICO Y CONCEPTUAL DE LA POLÍTICA DEL SISTEMA DE GESTIÓN INSTITUCIONAL

5.1. Marco normativo para el establecimiento de la Política de Seguridad y Privacidad de la Información

A continuación, se define el marco normativo colombiano sobre el cual se fundamenta el Sistema de Gestión de Seguridad de la Información.

- **Artículo 15 - Constitución Política de Colombia:** Establece que “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de Entidades públicas y privadas”.
- **Ley 23 de 1982:** Ley sobre derechos de autor.
- **Ley 1032 de 2006:** Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.
- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1273 de 2009:** Por la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y los datos" y se

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

- **Ley 1520 de 2012:** Por medio de la cual se implementan compromisos adquiridos por virtud del “Acuerdo de Promoción Comercial”, suscrito entre la República de Colombia y los Estados Unidos de América y su “Protocolo Modificatorio, en el Marco de la Política de Comercio Exterior e Integración Económica”.
- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014:** Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1928 de 2018:** Por la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001 en Budapest.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012 y se dictan disposiciones generales para la protección de datos personales.
- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1494 de 2015:** Por el cual se corrigen yerros en la Ley 1712 de 2014.
- **Decreto 2199 de 2015:** Por el cual se corrige un yerro en la Ley 1712 de 2014.
- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 2106 de 2019:** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Directiva Presidencial N°02 de 2019:** Por la cual se establecen lineamientos de simplificación de la interacción digital entre los ciudadanos y el Estado.
- **Directiva Presidencial N°03 de 2021**: Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- **Resolución 2710 de 2017:** Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- **Resolución 500 de 2021:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.
- **Resolución 1126 de 2021:** Por la cual se modifica la Resolución 2710 de 2017.
- **Resolución 0460 de 2022:** Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
- **Resolución 0463 de 2022:** Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.
- Circular Externa Conjunta N° 04 de 2019: Tratamiento de datos personales en sistemas de información interoperables.
- **Circular 5892 de 2013:** La DIMAR implementa el Manual - Política de Seguridad Informática y Física V. 2013.
- **CONPES 3701 de 2011:** Lineamientos de políticas para la Ciberseguridad y Ciberdefensa.

- **CONPES 3854 de 2016:** Lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.
- **CONPES 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital.

5.2. Marco conceptual para el establecimiento de la Política de Seguridad y Privacidad de la Información

Activo de información: Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Entidad (sistemas, soportes, activo físico, hardware, recurso humano).

Amenaza: Según ISO/IEC 13335-1:2004 , causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Ambiente de producción: Conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios, contratistas, operadores tecnológicos (en el caso que los haya) y demás partes interesadas para la ejecución de las operaciones de la Entidad. En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.

Aplicaciones: Software que se utiliza para la gestión de la información.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Sistema de Gestión de una organización.

Backup o copia de seguridad: Copia de respaldo de la información.

Confidencialidad: Propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, Entidades o procesos no autorizados.

Criticidad: Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.

Custodio: Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

Datos: Elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y se destruyen en la DIMAR. Recolección de hechos, cantidades, caracteres, símbolos y en general elementos crudos de conocimiento; que pueden ser persistidos y relacionados de alguna manera por la Institución, ya sea en medio físico o electrónico, y que no es necesario que hayan tenido un procesamiento, cálculos o estructuras elaboradas previas en su proceso de construcción.

Disponibilidad: Principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, Entidades o procesos autorizados

Evaluación de riesgos: Según ISO/IEC Guía 73:2002 , es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente de seguridad de la información: Violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, tales como, un acceso no autorizado o intento del mismo; uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

Información confidencial: Información, restringida o secreta, que es extremadamente sensible y únicamente puede ser conocida por personas específicas dentro de la Entidad. Para compartir esta información con terceros debe existir autorización expresa (escrita) de las directivas de la Entidad. Toda la información definida como reserva bancaria será clasificada como Confidencial.

Instalaciones: Todos los lugares físicos y virtuales en los que se aloja, se procesa y dispone la información de la Entidad.

Integridad: Principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción.

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

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza).

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. Es certificable. Primera publicación en 2005, segunda publicación en 2019.

Personal: Todo el personal de la DIMAR, funcionarios, contratistas, clientes, usuarios finales y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la DIMAR.

Política de Seguridad de la Información: Documento que establece el compromiso de la Dirección y el enfoque de la Entidad en la gestión de la seguridad de la información.

Principios de Seguridad de la Información: Confidencialidad, disponibilidad e integridad.

Propietario/responsable de la información: Individuo, Entidad o unidad de negocio que tienen bajo su responsabilidad la administración para el control, producción,

desarrollo, uso, mantenimiento y seguridad de los activos de información. Los propietarios de la información deben garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de políticas con otros propietarios de información y con propietarios de infraestructura.

Propietarios de infraestructura: Administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados. Los propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la información y de la Entidad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la Información: Consiste en resguardar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la Entidad, mediante un conjunto de medidas preventivas y correctivas.

Servicio: Cualquier acto o desempeño que una persona o Entidad puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

SGSI: Sistema de Gestión de Seguridad de la Información.

Soportes físicos: Documentos en soporte físico (cartas, informes, normas, contratos) y en medios de almacenamiento físico.

Tecnología: Equipos, sistemas de información, procesos y procedimientos utilizados para gestionar la información y las comunicaciones.

Terceros: Toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Usuarios: Personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos y a la información de la Entidad, por ejemplo: funcionarios, contratistas, terceros, proveedores, entre otros.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo de información. Según ISO/ IEC 13335-1:2004 se define como debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.