POLÍTICA
SISTEMA DE GESTIÓN INSTITUCIONAL

Proceso/Subproceso: G3 SISTEMA DE GESTIÓN INSTITUCIONAL
Código: G3-00-POL-001
Versión: 1

La Alta Dirección de la Dirección General Marítima – Dimar demuestra su liderazgo y compromiso con el **Sistema de Gestión Institucional** a través del establecimiento de esta Política y el aseguramiento de los recursos necesarios para su operación y mejora continua, proporcionando un marco de referencia para el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes.

SISTEMA DE GESTIÓN INSTITUCIONAL

La Dirección General Marítima, se compromete a contribuir al desarrollo de los intereses marítimos y fluviales del País, mediante la dirección, coordinación y control de las actividades marítimas, sustentados en un talento humano competente, el cumplimiento de los requerimientos legales, contractuales y regulatorios vigentes, la satisfacción de los requerimientos de los ciudadanos y demás partes interesadas, así como el mejoramiento continuo de su Sistema de Gestión Institucional y el desempeño de sus procesos.

En concordancia con lo anterior, la Dimar se compromete, mediante la identificación de los aspectos ambientales, a proteger el medio ambiente y prevenir la contaminación ocasionada por la operación de los procesos, con el fin de minimizar los impactos generados, así como a implementar las condiciones de trabajo y de salud necesarias para la eliminación y prevención de peligros y reducción de riesgos, mediante el desarrollo de acciones permanentes que implica al personal que desarrolla actividades al servicio de la Entidad.

Así mismo, la Entidad, reconociendo la importancia de la información propia y de los terceros con los que tiene contacto dentro del desarrollo de sus funciones se compromete a realizar una adecuada gestión de riesgos de sus activos de información, con el objetivo de mitigar el impacto y/o disminuir la probabilidad de la amplia variedad de amenazas a las que su información se encuentra expuesta; lo anterior le permite ofrecer a sus usuarios y partes interesadas información y servicios con la confidencialidad, integridad y disponibilidad adecuada.

De acuerdo a lo expresado previamente, es de resaltar que los principios orientadores en los cuales se basa la política para la operación del Sistema de Gestión Institucional son:

1. Gestión de la Calidad
2. Gestión Ambiental
3. Gestión de Seguridad y Salud en el Trabajo
4. Gestión de Seguridad en la Información

VA JUAN MANUEL SOLTAU OSPINA
Director General Marítimo

1. SUBPOLÍTICAS DE CALIDAD 4

1.1 Administración de riesgos 4

1.2 Mejora continua 4

2. SUBPOLÍTICAS DE SEGURIDAD Y SALUD EN EL TRABAJO 5

2.1 Regulación de la empresa 5

2.2 Regulación de horas de conducción y descanso 5

2.3 Regulación de velocidad 5

2.4 Uso de cinturón de seguridad 5

2.5 No uso de equipos de comunicaciones móviles mientras se conduce 5

3. SUBPOLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6

3.1 Administración y revisiones 6

3.2 Capacitación y sensibilización en seguridad de la información 6

3.3 Confidencialidad 6

3.4 Control de acceso 6

3.5 Disponibilidad del servicio e información 7

3.6 Dispositivos móviles 7

3.7 Gestión de activos 7

3.8 Gestión de cambios 7

3.9 Gestión de vulnerabilidades 8

3.10 Gestión de incidentes de seguridad de la información 8

3.11 Gestión de medios removibles 8

3.12 Gestión de vulnerabilidades 9

3.13 Integridad 9

3.14 No repudio 9

3.15 Organización de seguridad de la información 9

3.16 Registro y auditoria 10

3.17 Respaldos y recuperación 10

3.18 Seguridad informática 10

3.19 Seguridad física 10

3.20 Teletrabajo 11

3.21 Tratamiento de datos personales 11

3.22 Uso aceptable de activos y recursos 11

1. SUBPOLÍTICAS DE CALIDAD

1.1 Administración de riesgos

La Dirección General Marítima se compromete a establecer como estrategia la identificación, tratamiento, manejo y seguimiento de los riesgos de Gestión, Corrupción y Seguridad Digital a través de la creación y/o fortalecimiento de controles que incidan en la prevención de la materialización del riesgo y acciones de contingencia en caso de que esto suceda, con el fin de garantizar el cumplimiento de los objetivos institucionales de la Entidad.

Debido a lo anterior, la Dimar se compromete a controlar todos aquellos riesgos negativos que se identifique que pueden impedir el cumplimiento de los objetivos institucionales y potencializar los riesgos positivos (oportunidades) mediante una efectiva administración de los mismos (G3-00-PRO-005 Gestión de Riesgos), como herramienta de gestión que responda a las necesidades de la Entidad, contando con la participación activa de los servidores públicos responsables de los procesos y subprocesos, quienes deberán identificar, analizar y definir actividades de control para mitigar la materialización de los riesgos negativos.

1.2 Mejora continua

La Dirección General Marítima se compromete a implementar las acciones correctivas en respuesta a No Conformidades asociadas con desviaciones de políticas, objetivos y procedimientos, encontradas a través de revisiones y auditorias del sistema; esto con el fin de eliminar las causas que las originaron y evitar que vuelvan a ocurrir, asignando oportunamente a los responsables de formular e implementar las acciones de mejora en pro de un sistema eficaz y dinámico.

Por consiguiente, es responsabilidad directa de todo el personal de la Dimar la implementación de las acciones correctivas y de mejora identificadas, así como, la ejecución de las actividades designadas para subsanar las no conformidades presentadas en el Sistema de Gestión Institucional.

2. SUBPOLÍTICAS DE SEGURIDAD Y SALUD EN EL TRABAJO

2.1 Regulación de la empresa

La Dimar se compromete a generar un ambiente laboral saludable en cada unidad regional y sede central por lo cual prohíbe el ingreso, consumo, posesión, distribución o venta de bebidas embriagantes, tabaco, drogas alucinógenas y enervantes al interior de cada unidad regional y dentro del horario laboral. Cabe rescatar que, si se llegara a presentar un caso especial de requerir prueba de alcohol y/o drogas, especialmente en los cargos de conductores, estas se practicarán en una Entidad autorizada. En caso de negarse el empleado dará motivo suficiente para no laborar y se generará una sanción disciplinaria, que podrá ser suspensión temporal en el trabajo hasta la cancelación de su contrato, por justa causa de acuerdo a las circunstancias.

Es responsabilidad de cada funcionario, militar, civil y contratista, asegurar el desarrollo sus labores sin encontrarse bajo los efectos del alcohol, droga o cualquier medicina que pueda influenciar negativamente su conducta.

2.2 Regulación de horas de conducción y descanso

Todo empleado y/o conductor de la Dimar no debe exceder 8 horas de conducción, ampliable como máximo a 10 horas en un mismo turno, en caso de presentarse un exceso de la jornada máxima debe indicar la justificación y debe descansar como mínimo 7 horas. Tras 4,5 horas de conducción debe realizar una pausa de descanso 15 minutos.

2.3 Regulación de velocidad

La Dimar se acoge a los límites de velocidad establecidos en el código nacional de tránsito terrestre y a la normatividad legal vigente. Es obligación del conductor acatar las normas establecidas en dicho código y respetar las normas de tránsito existentes.

2.4 Uso de cinturón de seguridad

Todo empleado y/o conductor de la Dimar debe hacer uso del cinturón de seguridad siempre que conduzca un vehículo, por corto que sea el trayecto y es responsable por que cada uno de los ocupantes del vehículo lo usen de manera apropiada, segura y en todo momento.

2.5 No uso de equipos de comunicaciones móviles mientras se conduce

La Dimar aprueba el uso de equipos móviles con fines laborales, pero prohíbe que los conductores los utilicen mientras conducen cualquier tipo de vehículo. Si es requerido realizar una llamada personal o laboral, es obligatorio que el conductor detenga el vehículo en un lugar habilitado bajo los parámetros del código nacional de tránsito y dando cumplimiento a los requisitos de ley legales y aplicables.

3. SUBPOLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1 Administración y revisiones

La Política de Seguridad de la Información, las políticas relacionadas y demás documentos que forman parte de la estructura de la Seguridad de la Información deberán ser revisados con periodicidad. Los documentos se revisarán minino una (01) vez al año. El Oficial de Seguridad de la Información deberá presentar sus observaciones al Comité de Seguridad, quienes conceptuarán y redirigirán las modificaciones a la Alta Dirección.

3.2 Capacitación y sensibilización en seguridad de la información

La Dirección General Marítima, se compromete con la capacitación y sensibilización de su personal con respecto a la Seguridad de la Información; Se deben implementar capacitaciones y divulgaciones en seguridad de la información y de los procedimientos de gestión de incidentes de seguridad. Los funcionarios deben conocer la normatividad relacionada con la seguridad de la información de la Dirección General Marítima, ya que el desconocimiento de la misma no los exonerará de los procesos disciplinarios definidos ante violaciones de las políticas de seguridad.

3.3 Confidencialidad

Por medio de la Política de la Confidencialidad, la Dirección General Marítima manifiesta su compromiso en mantener y conservar la información relacionada a la privacidad, intimidad y buen nombre de las personas / usuarios de los que se almacena y/o registra información en el ejercicio de su actividad como Autoridad Marítima Colombiana.

3.4 Control de acceso

La Dirección General Marítima se compromete a mantener niveles de acceso adecuados según los roles y responsabilidades de las personas que trabajan o colaboran con la Entidad.

Los controles del acceso son tanto lógicos como físicos y se deben considerar en conjunto. A los usuarios y a los proveedores de servicios se les debe brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

Se debe tener en cuenta:

- Requisitos de la Entidad para el control de acceso.
- Gestión del acceso de usuarios.
- Responsabilidades de los usuarios.
- Control de acceso a las redes.
- Control de acceso al sistema operativo.
- Control de acceso a las aplicaciones y a la información.

- Dispositivos móviles
- Teletrabajo.

3.5 Disponibilidad del servicio e información

La Entidad se compromete a disminuir los posibles efectos de las interrupciones en los sistemas de información o el normal funcionamiento de la infraestructura tecnológica, así como asegurar los procesos críticos con los controles necesarios documentados preventivos y de auto recuperación. El Grupo de Informática y Comunicaciones garantizara los niveles de disponibilidad de acuerdo a los acuerdos de nivel de servicio establecidos, incluyendo la segregación de ambientes y gestión de cambios para el control de los sistemas de información. Con esto, se garantiza la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

3.6 Dispositivos móviles

La Dirección General Marítima pone a disposición de algunos miembros del personal dispositivos móviles institucionales para facilitar el desempeño de sus labores y propende porque dichos funcionarios hagan un uso responsable de ellos. Los dispositivos tipo PC Portátil, laptop, notebook o similar se regirán bajo la política de seguridad informática y reglamento de seguridad Informática de la Dimar; Las directrices aplican a teléfonos inteligentes, tabletas y asistentes personales y/o dispositivos con Sistema Operativo IOS y/o Android.

3.7 Gestión de activos

La Dirección General Marítima se compromete a gestionar los activos de información con una visión integral de su ciclo de vida considerando la mitigación del riesgo como objetivo principal enfocado en Confidencialidad, Integridad, Disponibilidad y la optimización de costos, con el propósito de lograr los objetivos de la organización de manera sostenible.

La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la compañía, la información deberá estar clasificada según la ley 1712 Publica, Publica Privada y Publica Reservada. La información Publica Privada y Publica Reservada debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

3.8 Gestión de cambios

La Entidad gestionara adecuadamente los cambios sobre sistemas de información, canales de comunicaciones y en general en sus servicios tecnológicos; Los cambios deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los

Colaboradores o Terceros que por sus funciones tienen relación con el sistema de información.

Antes de ejecutar un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto. Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente. Se debe disponer de un plan de roll-back en la aplicación de cambios para garantizar el normal funcionamiento de servicios de la Entidad.

3.9 Gestión de vulnerabilidades

Dimar documentará la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. En el proceso de gestión de riesgos asociados a los activos de Información, propenderá a través del Oficial de Seguridad de la Información y el Grupo de Informática y comunicaciones y/o el Proceso A3-Gobierno y gestión de TICs por asegurar un enfoque coherente, eficaz y documentado para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

3.10 Gestión de incidentes de seguridad de la información

La Entidad documentará la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. En el proceso de gestión de riesgos asociados a los activos de Información, propenderá a través del Oficial de Seguridad de la Información y el Grupo de Informática y comunicaciones y/o El Proceso A3-Gobierno y gestión de TICs por asegurar un enfoque coherente, eficaz y documentado para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

3.11 Gestión de medios removibles

La Dirección General Marítima se compromete a gestionar la información que puede ser almacenada en medios digitales y sobre todo en medios extraíbles como almacenamientos USB. El uso de dispositivos de almacenamiento externos y/o extraíbles queda autorizado solamente para los Coordinadores y/o Jefes de Grupo o a quienes ellos designen por medio del formato disponible en el SIMEC.

La Entidad gestionara y revisara los dispositivos de almacenamiento conectados a las estaciones de trabajo y contara con las herramientas necesarias para validar que NO se presenten fugas de información por estos medios.

La responsabilidad de la Información que se pueda almacenar en medios removibles recae directamente sobre el usuario que autoriza el uso de los medios de almacenamiento.

3.12 Gestión de vulnerabilidades

La Dirección General Marítima se compromete a realizar monitoreo, análisis y gestión permanente de vulnerabilidades y amenazas de su red integral de servicios digitales y servicios tecnológicos, con el fin de minimizar la exposición a riesgos que puedan llegar a afectar la Confidencialidad, Integridad o Disponibilidad de sus activos de Información.

3.13 Integridad

A todo usuario le corresponde utilizar los activos de información de la Dirección General Marítima en forma responsable, profesional, ética y legal. En particular, la Entidad velará porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones ni alteraciones, al destinatario correspondiente. Igualmente, la Entidad protege su información de las amenazas originadas por parte del personal.

Para dar mandato a lo anterior, se deberá:

- Mantener la privacidad de las comunicaciones personales y un nivel de servicio apropiado.
- Monitorear la carga de tráfico de la red y cuando sea necesario tomar acción para proteger la integridad y operatividad de sus redes.

La información generada y recibida de la Entidad, debe ser usada por los usuarios únicamente para los propósitos de la Entidad, por las funciones propias de su cargo y para responder por información de los entes de control o terceros (previa autorización del jefe inmediato o del jefe de la dependencia responsable de la información).

3.14 No repudio

La Entidad se compromete a generar mecanismos de control de usuarios (logs) en los sistemas de información; de tal manera que quede y conste cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado, y que se haga seguimiento a los mismos, de tal manera que un usuario no pueda negar su responsabilidad sobre un cambio en los ejercicios de intercambio electrónico de la información. En la construcción de aplicaciones o sistemas de información nuevos o existentes garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

3.15 Organización de seguridad de la información

La Dirección General Marítima con el fin de crear y soportar su Sistema de Gestión de Seguridad de la Información y alinear el mismo en el marco del MSPI, determina los roles necesarios dentro del mismo como son:

- Roles:
  - Comité De Seguridad De La Información
  - Oficial De Seguridad De La Información

De igual forma, se declaran y asignan responsabilidades a:

- Alta dirección de la Dirección General Marítima
- Funcionarios, contratistas, terceros y partes interesadas

3.16 Registro y auditoria

La Dirección General Marítima – Dimar se compromete a auditar periódicamente los sistemas y actividades relacionadas a la gestión de activos de información, así como a almacenar los registros de cualquier evento de seguridad, garantizando una adecuada gestión de los eventos e incidentes de seguridad y las debilidades identificadas a los sistemas.

3.17 Respaldos y recuperación

Siendo la información de Dimar su activo más importante, la Entidad se compromete a realizar una adecuada gestión y procesos de *BackUps*, Copias de Seguridad y respaldo con el fin de minimizar el impacto de incidencias que puedan afectar la disponibilidad de la Información; Dado que Dimar ha presentado un desarrollo en la infraestructura tecnológica con el fin de optimizar los procesos misionales y de apoyo que ofrece la Entidad, el grupo de informática y comunicaciones (GRUINCO) ha establecido procesos internos para generar respaldo y contingencia, en pro de la continuidad del negocio y disponibilidad de la información. GRUINCO maneja información a nivel de plataforma tecnológica (Máquinas Virtuales y físicas), bases de datos (Aplicativos misionales), portales Web (Dimar, CIOH y CCCP), aplicaciones administradas por terceros y la información de usuario final, donde se han dispuesto diferentes métodos de respaldo de acuerdo con el requerimiento y necesidades del proceso.

3.18 Seguridad informática

La Dimar se compromete a realizar una gestión adecuada de la información que circula a través de su red de datos, por lo cual genera la Política de Seguridad Informática A3-00-POL-001, por medio de la Cual la Entidad dicta los lineamientos generales de uso adecuado de medios, dispositivos, licenciamiento y Software entre otros.

3.19 Seguridad física

Se debe evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la Entidad, como se encuentra establecido en G1-00-POL-002. Los servicios de procesamiento de información sensible o crítica deben estar ubicados en

áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deben estar protegidas físicamente contra acceso no autorizado, daño e interferencia. El nivel de la protección suministrada debe estar acorde con los riesgos identificados.

3.20 Teletrabajo

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información en un entorno de teletrabajo, se establece que la Entidad debe proveer a los teletrabajadores los recursos necesarios para realizar su labor en el sitio en que la desarrollen de acuerdo a lo establecido en el decreto 0884 de 2012 y a la demás normatividad aplicable y vigente. A parte de ello se debe definir el modelo de Teletrabajo a aplicar en la Dimar, identificar los funcionarios que van a contar con un esquema de teletrabajo, establecer el protocolo de asignación de recursos para trabajar en el lugar establecido y definir protocolos de monitoreo de actividades de los teletrabajadores que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

3.21 Tratamiento de datos personales

En cumplimiento de la Ley 1581 de 2012 y del Decreto 1377 de 2013, la Dirección General Marítima (Dimar) elabora su Política de Tratamiento de Protección de Datos Personales A3-00-POL-002 aplicable en la Entidad. La Dirección General Marítima, ha elaborado el documento con el fin de determinar de controles, directrices y garantías legales aplicables para el procedimiento de recolección, tratamiento, uso, circulación y supresión de datos personales.

En consecuencia de lo anterior, la Dirección General Marítima se compromete con el cumplimiento de las disposiciones establecidas por la mencionada normatividad relacionadas con la protección de datos, con el propósito de respetar y garantizar los derechos de habeas data, libertad, autodeterminación informática, intimidad, entre otros, dé los titulares de la información personal que sea tratada al interior de la organización, en virtud de la existencia de una relación comercial, civil o laboral. En este sentido, cualquier persona natural que suministre información relacionada con datos personales, tendrá las facultades de autorizar el uso y tratamiento de la misma, actualizarla, corregirla o rectificarla.

3.22 Uso aceptable de activos y recursos

Todas las personas que trabajan para la Dirección General Marítima, así como colaboradores, contratistas, pasantes, terceras partes y en general, quienes usen activos de información que sean propiedad de Dimar, son responsables de cumplir y acoger con integridad la Política de Uso Aceptable para dar un uso racional y eficiente los recursos asignados.

El uso correcto y Adecuado de las herramientas tecnológicas que Dimar pone a disposición de sus colaboradores esta consignada en la Política y Reglamento de Seguridad Informática.