Con el propósito de implementar y alinear las políticas de Seguridad de la Información, establecidas por el Ministerio de Defensa Nacional, mediante la Directiva Permanente No.DIR2014-18 del 19 de junio de 2014, con las actividades productivas, operativas y administrativas de COTECMAR, y así mismo, crear un ambiente adecuado para todos los funcionarios y terceros que integran la Corporación, para el desarrollo y cumplimiento de sus funciones, en un ámbito de trabajo en el cual se mantengan los principios de integridad, confidencialidad y disponibilidad de la información, el Presidente de la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y fluvial – COTECMAR, establece las siguientes disposiciones, de estricto cumplimiento, a las Vicepresidencias, Gerencias, Oficinas y usuarios de la información corporativa, así como a todas las terceras partes que se relacionen de manera directa o indirecta con los activos informáticos de la organización.

El no acatamiento de las políticas de seguridad de la información, normas, procedimientos, estándares, directrices, disposiciones y órdenes impartidas con relación a ésta área, será considerado como una falta y los responsables del incumplimiento o violación de las mismas, estarán sujetos a las acciones administrativas, disciplinarias, penales o civiles a que haya lugar, de acuerdo con la legislación colombiana y los reglamentos que rigen la Corporación.

Para tal efecto, se establecen los siguientes aspectos:

1. Creación y activación del Comité de Seguridad de la Información

   El "Comité de Seguridad de la Información", se establece como el maximo organismo Corporativo para asuntos relacionados con la Seguridad de la Información, estará integrado por representantes de las áreas productivas, de apoyo y operativas de la Corporación, teiniendo como función principal, realizar el análisis y proyecciones asociadas al tratamiento, gestión y manejo de la seguridad de la información y el apoyo manifiesto a las acciones administrativas, disciplinarias, penales y/o civiles que la Corporación deba adelantar.

   Las funciones del Comité de Seguridad de la Información son las siguientes:

   a. Revisar y proponer al Presidente de la Corporación para su consideración y posterior aprobación, la actualización de las políticas y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para COTECMAR.
   b. Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Corporación frente a posibles amenazas, sean internas o externas.
   c. Tomar decisiones ante posibles acciones por incumplimiento.
   d. Tener conocimiento y supervisar la investigación y monitoreo de los incidentes, relacionados con la seguridad de la información, que se produzcan en la Corporación.
   e. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información
   f. Evaluar y coordinar la implementación de controles específicos de seguridad de la información, para los sistemas o servicios de esta Corporación (sean preexistente o nuevos).

g. Promover la difusión y apoyo en materia de seguridad de la información dentro de la Corporación y así coordinar el proceso de administración de la continuidad de las actividades.
h. Todas las demás que se consideren relacionadas con la seguridad de la información, y que por delegación de la junta directiva o por situaciones especiales, deban ser abordadas por este comité.

2. Cuidado de los activos de información de la Corporación

a. Cada usuario debe firmar y aceptar lo establecido en el Anexo F "Formato Solicitud Recursos y Servicios de Tecnología y Uso Adecuado de los Mismos", el cual le dá la responsabilidad y custodia sobre los activos de información que le son asignados; el anexo G "Declaración de Aceptación y Compromiso de Cumplimiento Políticas de Seguridad de la Información" y el anexo I "Formato promesa de reserva y secreto corporativo".
b. La información de proyectos, desarrollos, investigaciones, propuestas de negocios, procesos administrativos, procesos operativos, procesos productivos y demás actividades relacionadas con el cumplimiento de la misión corporativa, se considera clasificada, además la clasificación de la información deberá obedecer a lo establecido en el Anexo F "Reglas de clasificación y niveles de acceso de la información clasificada de cotecmar", por lo tanto debe ser almacenada única y exclusivamente en dispositivos informáticos corporativos, implementando las medidas de seguridad adecuadas.
c. Los mensajes y la información contenida en los buzones de correo corporativo son de propiedad de la Corporación. Cada usuario como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y el tráfico de la misma, se considera de interés del sector.
d. Todos los incidentes informáticos deben ser informados y reportados. Sobre la investigación, se elaborará un informe escrito y detallado que identifique el incidente, los resultados y acciones tomadas o recomendaciones, el cual debe ser enviado a la Oficina de Tecnologías de su Información, para que por su conducto sea conocida por el Líder de Seguridad de la Información.

3. Gestión de activos de información

Cada una de las Vicepresidencias, Gerencias, Oficinas y Usuarios de la Información Corporativa, tienen la custodia sobre todo dato, información y mensaje generado, procesado y contenido por los sistemas y activos de información que le hayan sido asignados, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información. Por lo tanto deben:

a. Identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información. (Anexo "N").
b. Realizar la clasificación y control de activos de información con el objetivo de garantizar que reciban un apropiado nivel de protección; clasificar la información para señalar su sensibilidad, criticidad y definir los niveles de protección y medidas de tratamiento de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información.
c. Realizar la clasificación de la información, evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.
d. Definir procedimientos para el rotulado y manejo de información de acuerdo al esquema de clasificación de la información establecido (Anexo "F").

4. Uso adecuado de los activos de información

Los Vicepresidentes, Gerentes y Jefes de Oficinas según el caso, podrán solicitar a la Oficina de Tecnologías de la Información, que se realice monitoreo y supervisión a 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 consideraran aceptables los siguientes usos:

a. 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:

1) Navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
2) Se prohíbe toda actividad, tipificada como delito informático o delitos sexuales realizados a través de los activos informáticos corporativos.
3) Publicar, enviar o adquirir material sexualmente explícito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.
4) Publicar o enviar de información confidencial hacia afuera de COTECMAR, sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
5) Utilizar otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados.
6) Publicar anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.
7) Promover o mantener asuntos o negocios personales.
8) 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.
9) Navegar en las cuentas de correo de carácter personal, no Corporativo, o en redes sociales, sin una justificación por parte de la Entidad.
10) Uso de herramientas de mensajería instantánea no autorizadas por la oficina de tecnologías de la Información y las Comunicaciones, o la que haga sus veces.
11) Emplear cuentas de correo externas no corporativos para el envío o recepción de información corporativo.
12) 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.
13) 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.
14) Dado el caso que por la naturaleza del cargo se requieran accesos especiales, estos deben ser solicitados y justificados por su jefe inmediato.

b. Correo electrónico corporativo

1) La cuenta de correo electrónico corporativo debe ser usado para el desempeño de las funciones asignadas dentro de cada una de las Vicepresidencias, Gerencias, Oficinas y dependencias de la Corporación y deberá ser solicitado si es necesario, al momento

de ingresar a la corporación, mediante Formato Solicitud Recursos y Servicios de Tecnología y Uso Adecuado de los Mismos (Anexo "L").

2) Los mensajes y la información contenida en los buzones de correo corporativo son de propiedad de COTECMAR. 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 Corporación.
3) El correo corporativo de cada funcionario se creará con inicialprimernombreapellido@cotecmar.com, en caso que el usuario ya exista se creará como inicialprimernombreinicialsegundonombreapellido@cotecmar.com.
4) Para el correo saliente, con información clasificada o sensible, debe ser trasmitida atendiendo los lineamientos establecidos en el Anexo F "Reglas de Clasificación y Niveles de Acceso de la Información Clasificada de COTECMAR".
5) Todo el personal de COTECMAR, debe tener asignada una cuenta de correo electrónico corporativo "@cotecmar.com", el cual es el medio autorizado para el envío de información.
6) El tamaño de los buzones es de cincuenta (50) gigas y mensajes de correo adjuntos es de veinte (20) megas.
7) 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.
8) Es responsabilidad del asignatario de la cuenta mantener el buzón por debajo de su capacidad para evitar que se sature (leyéndolo regularmente, eliminando mensajes antiguos, etc.).
9) No está autorizada la utilización de correos comerciales para transmitir información de carácter Corporativo.
10) Al interior de la corporación y alineados con la política de seguridad de la información emitida por el Ministerio de Defensa Nacional, queda prohibido el uso, configuración, acceso, envío de información y manejo de cuentas de correo electrónico diferentes a la corporativa.
11) No se considera aceptado el uso del correo electrónico Corporativo para los siguientes fines:

    a) Utilizar sistemas y servicios de la Corporación con mensajes, imágenes o contenidos que sean violatorios al derecho a la intimidad de cualquier persona.
    b) Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, discriminatorio, sexista, pornográfico, publicitario no Corporativo, 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.
    c) 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 su jefe inmediato, o quien haga sus veces.
    d) El envío de información de proyectos que adelanta la Corporación, en relación con la defensa y la seguridad nacional, a otras entidades diferentes a las que suscriben el contrato, sin la autorización previa del propietario de la información, o la que haga sus veces.
    e) Toda información que requiera ser transmitida fuera de COTECMAR, y 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, siempre y

cuando sean empleadas y aplicadas, medidas de aseguramiento de la información como cifrado y/o ofuscación.

12) Todo correo electrónico deberá respetar el estándar de formato e imagen corporativo definido para COTECMAR, y deberá contener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

a) El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
b) El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
c) En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
d) Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

13) Todo el personal de la Corporación, deberá configurar su correo electrónico Corporativo de tal manera que en la firma de su correo quede claramente identificado, así:

a) Nombres y apellidos completos.
b) Cargo completo y no abreviado.
c) Datos de Contacto.
d) Dirección Oficina.
e) Teléfono Oficina con extensión, si la tiene.
f) Celular corporativo, si lo tiene.
g) Ciudad y país.
h) Correo Corporativo.
i) Línea de transparencia

De igual forma, ésta debe cumplir lo establecido por el departamento de comunicaciones estratégicas de la corporación.

5. Control de los recursos tecnológicos

a. La instalación de cualquier tipo de software en los equipos de cómputo de la Corporación, es responsabilidad exclusiva de OFTIC, por tanto son los únicos autorizados para realizar esta labor, la cual deberá ser solicitada a través de la mesa de ayuda SIMAC.
b. 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 le debe realizar la configuración adecuada de seguridad, con apoyo del personal técnico de OFTIC, el cual debe ser solicitado a través de la mesa de ayuda SIMAC.
c. Los usuarios no deben realizar cambios relacionados con la configuración del equipo en las estaciones de trabajo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por el personal técnico de OFTIC.
d. 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 y/o autorizadas por el personal técnico de OFTIC.
e. Los equipos de comunicación y cómputo asignados por la corporación, deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación.

f. De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de comunicación y cómputo en las oficinas, una vez haya cesado el uso de los mismos.
g. Los requerimientos o necesidades de recursos tecnológicos de las dependencias de COTECMAR, deben ser avalados por la Oficina de Tecnologías de la Información y las Comunicaciones.
h. 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 y Corporativas y deben tener las restricciones adecuadas a su cargo.
i. El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.
j. La oficina de TIC como área encargada de la administración de la plataforma tecnológica, deberán implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento, almacenamiento y comunicación.
k. Sobre los equipos más críticos de la red se deben configurar políticas de arranque a través de contraseña de setup (inicio).
l. Todo acceso para lectura o ejecución de programas, documentos o aplicaciones que se haga desde dispositivos de almacenamiento externos, debe ser previamente revisado por un sistema antivirus o anti-spyware para evitar la infección de las estaciones de trabajo, con código malicioso.
m. La adquisición de cualquier equipo tecnológico relacionado con las actividades de manejo, procesamiento, almacenamiento y/ tratamiento de datos corporativos, deberá ser canalizado por intermedio de la Oficina de TIC; siendo obligatorio, que la División de adquisiciones, exija que éste tipo de procedimientos sean elevados únicamente por OFTIC.
n. El usuario de recursos y activos de la información Corporativos, no deberá sacarlo de su sitio de trabajo, sin la debida autorización y trámite del formato establecido en el "Anexo "M" Solicitud Ingreso Salida de Equipos de Computo y Accesorios Institucionales".
o. El usuario asignatario de un recurso informático o de información, deberá aceptar y emplear de forma adecuada los equipos que le son asignados para cumplir con las funciones propias de su cargo, sin pretender o aplicar acciones no adecuadas para que le sea mejorado, cambiado o asignado mas recursos tecnológicos de los que de acuerdo a la evaluación técnica le son entregados.

6. Seguridad y mantenimiento de los equipos

a. Los equipos que hacen parte de la infraestructura tecnológica de COTECMAR, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.
b. Las Vicepresidencias, Gerencias, Oficinas y Usuarios de Activos de información de COTECMAR, adoptarán los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.
c. Los funcionarios y terceros velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
d. Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, 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.

e. Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con una guaya o mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de COTECMAR.

7. Seguridad de los equipos fuera de las instalaciones

a. Los usuarios que requieran manipular los equipos o medios tecnológicos fuera de las instalaciones de COTECMAR, deben velar por la protección de los mismos sin dejarlos desatendidos, comprometiendo la imagen o información de la Corporación.
b. El propietario del activo, con el apoyo de OFTIC, identificará mediante la aplicación de lo establecido en el Anexo C "Procedimiento de Identificación y tratamiento del Riesgo", los riesgos potenciales que puede generar el retiro de equipos o medios de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.
c. En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información clasificada y que esté además relacionada con las actividades de desarrollo, investigación e innovación de la corporación, el responsable del equipo deberá poner en conocimiento de la Oficina de TIC y realizar inmediatamente el respectivo reporte de incidente de seguridad, activando el Procedimiento por perdida, daño o afectación de activos de información corporativos (Anexo "D"), así como realizar la correspondiente denuncia ante la autoridad competente.
d. Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de COTECMAR, deberán contener únicamente la información estricta y necesaria para el cumplimiento de sus funciones, así mismo, se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene, además, la información contenida en éste deberá estar cifrada.
e. Todo el personal que por cumplimiento de sus funciones corporativos necesite retirar un equipo, medio de almacenamiento, información o software de las instalaciones de la Corporación, deben ser debidamente identificados y registrados antes de conceder la autorización respectiva (Anexo "M").
f. Los equipos de contratistas y demás terceros que hayan sido autorizados para acceder a las instalaciones de COTECMAR, sólo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a través del proceso de verificación de equipos. La OFTIC, generarán un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.

8. Traslado de propiedad

a. El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica, debe ser autorizado por el propietario del activo previa solicitud del funcionario interesado. Si el activo está clasificado como relacionado con actividades de desarrollo, investigación, innovación y/o actividades comerciales, el retiro deberá estar autorizado también por el Vicepresidente a la cual está cargado el activo de información (o quién haga sus veces).
b. Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones de COTECMAR, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.
c. COTECMAR, por intermedio de la Oficina de Seguridad Física, proporcionará los mecanismos y recursos necesarios para que en cada punto de acceso a las instalaciones, se realice revisión y se lleve el control de los equipos que son ingresados y retirados.
d. Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos, sólo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información. La OFTIC, generará un paz y salvo

como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.

9. Protección contra software malicioso

   a. Los sistemas operacionales y aplicaciones deberán mantener un adecuado proceso de actualización y parcheo, de acuerdo a como lo recomienden los fabricantes; de igual forma, la plataforma tecnológica deberá recibir el mismo tratamiento, realizando las acciones necesarias para garantizar la disponibilidad y continuidad de las operaciones.
   b. Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.
   c. Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de la Oficina de TIC, previo diligenciamiento del Anexo P "Formato de Excepción de Instalación Software de Seguridad".
   d. No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red corporativo.
   e. Todos los medios de almacenamiento que se conecten a equipos de la infraestructura tecnológica de COTECMAR, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.
   f. El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por el área competente.
   g. Cada Vicepresidencia, gerencia, oficina y dependencia de la Corporación, 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.
   h. Los sistemas, equipos e información corporativos deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

10. Derechos de propiedad intelectual

   a. Las Vicepresidencias, Gerencias, Oficinas y dependencias de la Corporación, cumplirán con la reglamentación vigente sobre propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.
   b. No se permitirá el almacenamiento, descarga desde internet, intercambio, uso, copia, reproducción y/o instalación de: software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.
   c. Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
   d. Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor, canalizando las adquisiciones y compras, por intermedio de la Oficina de TIC.
   e. El software a la medida, adquirido a terceras partes o desarrollado por funcionarios de COTECMAR, serán de uso exclusivo de la Corporación y la propiedad intelectual será de quien lo desarrolle.

11. Declaración de aplicabilidad

a. 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.
b. Estos controles están basados en el código de buenas prácticas definido en la norma ISO/IEC 27002.
c. La declaración de aplicabilidad debe ser documentada y actualizada cuando cambian las condiciones propias del negocio, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros.

12. Concientización y capacitación en seguridad de la información

a. Las Vicepresidencias, Gerencias, Oficinas y dependencias de la Corporación, deberán coordinar con la Oficina de TIC, la ejecución de actividades de concientización y capacitación para todos sus funcionarios, así como para los contratistas y terceros que interactúen con la información corporativo y desarrollen actividades en sus instalaciones.
b. Todos los funcionarios y terceros al servicio de COTECMAR, deben ser informados y capacitados en el cumplimiento de las Políticas de Seguridad de la Información y en los aspectos necesarios para desempeñar sus funciones, durante su proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas.
c. 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 les son de aplicación en caso de incumplimiento.

13. Documentación de procedimientos operativos

a. La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los formatos siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.
b. 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.
c. 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.

14. Gestión de la capacidad

a. La Oficina de Tecnologías de la Información y las Comunicaciones, como área responsable de la administración de la plataforma tecnológica, deberá implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma, sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación.
b. El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.

15. Estaciones de trabajo

    a. Sobre los equipos más críticos de la red se deben configurar políticas de arranque a través de contraseña de setup (inicio).
    b. Todo acceso para lectura o ejecución de programas, documentos o aplicaciones que se haga desde dispositivos de almacenamiento externos, debe ser previamente revisado por un sistema antivirus o anti-spyware para evitar la infección de las estaciones de trabajo, con código malicioso.
    c. 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, y la información sensible o clasificada que contengan, debe estar cifrada en el disco duro o borrada en forma segura.
    d. Se prohíbe la instalación de juegos o software diferente al instalado y autorizado para el cumplimiento de las funciones relacionadas con su cargo.
    e. El usuario debe cancelar todas las sesiones activas antes de dejar el equipo desatendido.
    f. El equipo debe tener configurada la opción de protector de pantalla con contraseña, con un tiempo mínimo de activación.
    g. Los equipos que almacenan información clasificada o sensible, no deben tener salida a internet.
    h. Los equipos que requieran acceso a internet deben estar autorizados previamente mediante formato establecido en el Anexo L "Formato Solicitud Recursos y Servicios de Tecnología y Uso Adecuado de los Mismos".
    i. Los usuarios asignatarios de las estaciones de trabajo de escritorio y portátiles, son responsales de la elaboración de los backup y copias de respaldo de la información que es manejada por ellos; para tal fin, se establece que la política de Backup corporativa, hace parte integral de las políticas de seguridad de la información para COTECMAR, y su incumplimiento acarrea las acciones disciplinarias, administrativas y penales establecidad en la directiva.

16. Seguridad de la información en la continuidad de las actividades Operativas, Administrativas y de Apoyo

    a. La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso de la alta dirección.
    b. Las Vicepresidencias, Gerencias, Oficinas y dependencias que conforman COTECMAR, 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.
    c. Para COTECMAR, su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.
    d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan de recuperación de desastres, estarán incorporados y definidos en el Plan de Continuidad.
    e. Se deberá dar cabal cumplimiento y aplicabilidad a la política de Backup corporativa, definiendose éste tema como de vital importancia para la continuidad de las operaciones en COTECMAR.
    f. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad.

Atentamente,

Contralmirante **JORGE ENRIQUE CARREÑO MORENO**

15. Estaciones de trabajo

    a. Sobre los equipos más críticos de la red se deben configurar políticas de arranque a través de contraseña de setup (inicio).
    b. Todo acceso para lectura o ejecución de programas, documentos o aplicaciones que se haga desde dispositivos de almacenamiento externos, debe ser previamente revisado por un sistema antivirus o anti-spyware para evitar la infección de las estaciones de trabajo, con código malicioso.
    c. 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, y la información sensible o clasificada que contengan, debe estar cifrada en el disco duro o borrada en forma segura.
    d. Se prohíbe la instalación de juegos o software diferente al instalado y autorizado para el cumplimiento de las funciones relacionadas con su cargo.
    e. El usuario debe cancelar todas las sesiones activas antes de dejar el equipo desatendido.
    f. El equipo debe tener configurada la opción de protector de pantalla con contraseña, con un tiempo mínimo de activación.
    g. Los equipos que almacenan información clasificada o sensible, no deben tener salida a internet.
    h. Los equipos que requieran acceso a internet deben estar autorizados previamente mediante formato establecido en el Anexo L "Formato Solicitud Recursos y Servicios de Tecnología y Uso Adecuado de los Mismos".
    i. Los usuarios asignatarios de las estaciones de trabajo de escritorio y portátiles, son responsales de la elaboración de los backup y copias de respaldo de la información que es manejada por ellos; para tal fin, se establece que la política de Backup corporativa, hace parte integral de las políticas de seguridad de la información para COTECMAR, y su incumplimiento acarrea las acciones disciplinarias, administrativas y penales establecidad en la directiva.

16. Seguridad de la información en la continuidad de las actividades Operativas, Administrativas y de Apoyo

    a. La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso de la alta dirección.
    b. Las Vicepresidencias, Gerencias, Oficinas y dependencias que conforman COTECMAR, 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.
    c. Para COTECMAR, su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.
    d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan de recuperación de desastres, estarán incorporados y definidos en el Plan de Continuidad.
    e. Se deberá dar cabal cumplimiento y aplicabilidad a la política de Backup corporativa, definiendose éste tema como de vital importancia para la continuidad de las operaciones en COTECMAR.
    f. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad.

Atentamente,

Vicealmirante **JORGE ENRIQUE CARREÑO MORENO**
Presidente COTECMAR.