



**CORPORACIÓN DE CIENCIA Y TECNOLOGIA PARA EL DESARROLLO DE LA
INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL**

**DIRECTIVA PERMANENTE No. 043 PCTMAR-VPEXE – OTIC
(19 de abril de 2024)**

**POR MEDIO DE LA CUAL SE ESTABLECEN LAS POLÍTICAS DE SEGURIDAD
DE LA INFORMACIÓN PARA LA CORPORACIÓN DE CIENCIA Y TECNOLOGÍA
PARA EL DESARROLLO DE LA INDUSTRIA NAVAL, MARÍTIMA Y FLUVIAL -
COTECMAR**

DIRIGIDO A:

**VICEPRESIDENTES, GERENTES UNIDADES DE NEGOCIO,
JEFES DE OFICINA, USUARIOS DE LA INFORMACIÓN
CORPORATIVA**

INTRODUCCIÓN

La presente Directiva tiene como objetivo impartir instrucciones para la actualización, desarrollo, aplicación, cumplimiento y supervisión de las políticas de seguridad de la información que deben seguir todos los funcionarios, contratistas, practicantes y cualquier persona que tenga una relación con la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR, o que tenga acceso a los activos de información, con el propósito de preservar los principios de confidencialidad, integridad y disponibilidad de la información para fortalecer la continuidad de las actividades operacionales, administrativas y logísticas, protegiendo ésta de forma adecuada, reduciendo los riesgos y optimizando el empleo de tecnologías de información al servicio de la organización.

La Directiva de seguridad de la información para COTECMAR define las políticas, la estructura de la organización de seguridad de la información, funciones, controles de uso aceptable, las directrices, verificación y auditoría para el Sistema de Gestión de Seguridad de la Información (SGSI) en COTECMAR.

Las políticas establecidas y sus posteriores actualizaciones aplican y son de obligatorio cumplimiento para todos aquellos que tengan acceso a los recursos y activos de información de las dependencias y unidades de negocio que componen COTECMAR, y cualquier persona o entidad que tenga una relación con la Corporación, así como a los designados para su uso y custodia en el territorio nacional y fuera de él.

Los procedimientos y anexos de la presente directiva se encuentran en la plataforma ISOLUCION en el módulo de documentos; al igual que la directiva, establecen pautas e instrucciones de obligatorio cumplimiento para todos los funcionarios, contratistas, practicantes y cualquier persona que tenga relación con la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial - COTECMAR o que tenga acceso a los activos de información, así como los asignados para su uso y custodia.

DESARROLLO DE LA DIRECTIVA

1. INFORMACIÓN GENERAL

a. DEFINICIONES

Para efectos de entendimiento de la presente Directiva, se toma como factor determinante entender el significado de la terminología propia de este tema, motivo por el cual se establece el anexo A “Glosario, definiciones y términos”.

b. OBJETIVOS

La Política de Seguridad de la Información de COTECMAR, tiene como objetivo general, impartir lineamientos para la protección de los activos estratégicos de la Corporación, que dependen o usan las tecnologías de la información y las comunicaciones y que son accedidos y/o usados por todo el personal que por ejercicio de sus funciones o por relacionamiento comercial y/o contractual, tiene acceso a algún tipo de información de relevancia corporativa:

1. Establecer lineamientos generales relacionados con la aplicación de la seguridad de la información y ciberseguridad.
2. Ser el documento rector para comunicar los lineamientos establecidos por la alta dirección respecto a la seguridad de la información y la ciberseguridad, generando cultura y compromiso en todos los niveles de la corporación.
3. Establecer y comunicar la responsabilidad y autoridad sobre el manejo de la seguridad de la información y la ciberseguridad de la Corporación.
4. Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad.
5. Garantizar un nivel aceptable de confiabilidad, imagen corporativa y credibilidad de COTECMAR con todos sus clientes internos y externos.
6. Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la Corporación.
7. Establecer lineamientos para la protección de la confidencialidad de la información relacionada con el objeto Corporativo, con los clientes y con los planes de negocio y desarrollo de COTECMAR.

8. Aportar a los procesos de conservación de niveles aceptables de integridad de los registros operativos, administrativos y de apoyo de la Corporación.
9. Impartir lineamientos para garantizar niveles aceptables de disponibilidad de la información requerida en el ejercicio de las funciones de los colaboradores y quienes acceden y requieren de la información corporativa.
10. Entender y dar cobertura a las necesidades de seguridad de la información que se identifiquen en cada uno de los niveles de la Corporación.

c. INFORMACIÓN

La Política de Seguridad de la Información para la Corporación, pretende fomentar la cultura de seguridad y buenas prácticas con el manejo de la información en todos los procesos operativos y administrativos de la organización, contribuyendo a la identificación de los niveles de seguridad de la información y a establecer responsabilidades por su manejo, garantizando la adecuada protección de los activos de información, recursos informáticos, datos y archivos. Estas políticas sirven de referencia para el personal que tenga acceso a la información, recursos y servicios tecnológicos, además permiten definir un marco de control para brindar seguridad a los activos de información dispuestos en cada dependencia. De igual forma, es importante considerar que el cumplimiento de las normas dispuestas en la presente política, son de obligatorio cumplimiento y aplicación por parte de todos los que de forma directa o indirecta interactúan con la Corporación, quienes deben conocer y aceptar el reglamento vigente sobre su uso, en tal razón, el desconocimiento del mismo no exonera de responsabilidad a los usuarios, ante cualquier eventualidad que afecte o implique una acción en contra de la seguridad de la información o de los recursos tecnológicos de la Corporación.

La estructuración de los controles y marco de referencia, fueron fundamentados en las normas NTC-ISO/IEC 27001, 27002 y 27005, las cuales permiten garantizar la existencia de una serie de procesos continuos para evaluar, mantener y administrar la seguridad de la información e implementar políticas de seguridad de la información y estándares locales, mediante una sucesión de procedimientos donde la identificación y análisis de riesgos sobre los activos informáticos permiten establecer mecanismos de control.

Los activos de información se constituyen como un soporte de la misión y la visión de la Corporación, por lo que requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

d. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Al interior de la Corporación, se establece una cultura de la seguridad de la información, para lo cual se integran como principios en este aspecto, los siguientes:

1. Gestión de riesgos: La Corporación afronta la toma de riesgos y tolera aquellos que, con base a la información disponible, son comprensibles, controlados y tratados cuando es necesario.
2. Cultura de seguridad: Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.
3. Compromiso: La alta dirección dispondrá de los recursos requeridos para la gestión operativa de los controles relacionados con la seguridad de la información y de requerirse, integrará en el presupuesto de funcionamiento y PDTI – TIC, los recursos para su implementación y mantenimiento.
4. Responsabilidad: Cada integrante de la Corporación y quienes, por el ejercicio de sus funciones, hagan uso de la información corporativa, será responsable por el uso adecuado de los recursos de los que haga uso, teniendo en cuenta aquellas posibilidades de fraude relacionadas con el uso abusivo de los sistemas de información dentro del uso y acceso a los sistemas de información.

e. GENERALIDADES

El continuo desarrollo tecnológico y la tendencia para digitalizar y automatizar los procesos administrativos, técnicos y operativos de las organizaciones, implican que las entidades deben afrontar una serie de amenazas y riesgos que se derivan de los procesos de tecnificación; esta situación conlleva a que se haga necesario aplicar medidas que permitan mejorar continuamente los esquemas de aseguramiento sobre las plataformas y recursos tecnológicos de la Corporación, con el fin de minimizar el impacto que se genera por la materialización de algún riesgo que pueda afectar las actividades cotidianas e inclusive el nombre y know how de la Corporación.

Teniendo en cuenta lo anterior, la Corporación de Ciencia y Tecnología para el Desarrollo de la industria Naval, Marítima y Fluvial – COTECMAR, estructura la política de seguridad de la información, estableciendo como foco de interés dentro de ésta, los siguientes aspectos:

- 1) Identificación de las necesidades de seguridad, amenazas y riesgos informáticos de los activos de información que se encuentran al servicio de la Corporación, así como sus posibles consecuencias.
- 2) Plantear un modelo de organización de seguridad de la información, definiendo claramente los roles y responsabilidades de los que intervienen en la implementación de la Política.
- 3) Proteger los recursos de información y tecnología frente a amenazas y riesgos internos y externos, con el propósito de asegurar la información en sus principios básicos de confidencialidad, integridad y disponibilidad mediante la implementación de controles.
- 4) Promover y sensibilizar al personal en la cultura de seguridad y reserva de la información para mitigar los riesgos, amenazas y disminuir de esta forma los incidentes de seguridad que se puedan presentar.
- 5) Implementar un Sistema de Gestión de Seguridad de la Información para COTECMAR, cuya finalidad es mantener de forma estandarizada un sistema efectivo que permita el tratamiento seguro de la información.
- 6) Mantener actualizadas las políticas de seguridad a efectos de mantener su vigencia y nivel de eficacia.
- 7) Estructurar procedimientos claros para la adopción de mecanismos que permitan integrar mejores prácticas en Seguridad de la Información.
- 8) Promover el cumplimiento, por parte del personal bajo su responsabilidad, de las políticas de seguridad de la información.

f. ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN

- 1) Cada Vicepresidencia, Gerencias, Jefes de Oficina, Usuarios de la información Corporativa, al igual que los encargados de procesos administrativos, operativos y técnicos en COTECMAR, deberá realizar el análisis y evaluación de los riesgos como base para identificar y controlar los riesgos de seguridad de la información en

sus activos; para lo cual se deberá seguir el procedimiento de identificación y tratamiento de riesgos (Anexo C “Procedimiento de Identificación y Tratamiento del Riesgo”) empleando la metodología de la ISO/IEC 27005:2008 que contiene las siguientes actividades generales:

- a) Identificación de activos de información y valoración del impacto.
- b) Identificación de escenarios de riesgo basados en las amenazas y vulnerabilidades posibles.
- c) Valoración de la probabilidad de ocurrencia de los escenarios de riesgo y la efectividad de los controles implementados.
- d) Cálculo del nivel de riesgo de seguridad de la información.
- e) Identificación de opciones para el tratamiento de los riesgos que sean valorados en un nivel no aceptable.

Igualmente, para la identificación de opciones de tratamiento de riesgos se deberá seguir el procedimiento para evaluación y tratamiento de riesgos.

- 2) El proceso de gestión de los riesgos de información en la Institución será asesorado, monitoreado y verificado por la Oficina de Tecnologías de la Información, a través del líder de seguridad de la información.
- 3) Las actividades necesarias para ejecutar el análisis de riesgos se realizan de acuerdo con el siguiente esquema:
 - a) Definición de los procesos críticos a los cuales se le aplicará el análisis de riesgos.
 - b) Entrevistas con los responsables de los activos con el propósito de dar a conocer la metodología y hacer el levantamiento de activos de información.
 - c) Análisis y evaluación de los riesgos de seguridad de la información para los activos que soportan los procesos críticos.
 - d) Identificación de opciones de tratamiento de riesgos.
 - e) Comunicación de resultados al Comité de Seguridad de la Información.
- 4) El análisis y evaluación de riesgos deberá realizarse y/o

actualizarse una vez al año, cuando resultados de auditorías lo recomienden, cuando se vulnere la seguridad de los sistemas, cada vez que ocurren cambios significativos en la estructura orgánica de las unidades de negocio y dependencias que conforman la Corporación, tanto en sus plataformas tecnológicas como en sus procesos o cuando se detecten nuevas amenazas o riesgos.

2. EJECUCIÓN

Considerando que los aspectos que se plantean en la presente directiva son de aplicación y manejo transversal a todos los procesos corporativos, se establecen las siguientes responsabilidades que deberán ser ejecutadas y verificadas en cada una de las dependencias, así:

a. RESPONSABILIDAD GENERAL

La Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial – COTECMAR, en cumplimiento con lo establecido por el Ministerio de Defensa Nacional, mediante Directiva Permanente N° DIR2014-18 “Políticas de Seguridad de la Información del Sector Defensa”, del 19 de junio de 2014; de igual forma alineándose con los códigos de mejores prácticas y estándares que tienen como propósito prevenir, detectar y neutralizar el riesgo de fuga de información, dispone a partir de la fecha estandarizar las políticas de seguridad de la información para Vicepresidencias, Gerencias, Oficinas, dependencias y terceros, que participan en los procesos y/o tienen acceso a los activos de información de la corporación.

b. RESPONSABILIDADES PARTICULARES

1) Vicepresidente Ejecutivo

- a) Presenta para aprobación de la Presidencia, el Comité Corporativo de Seguridad de la Información, con las funciones especificadas en el Reglamento del Comité Corporativo de Seguridad de la Información.
- b) Ejerce el liderazgo sobre las actividades de coordinación y gestión operativa entre las oficinas Jurídica, Seguridad Física, TIC, Sistemas Integrados de Gestión y Auditoría Interna, con el fin de avalar e integrar los procedimientos de seguridad de la información en cada uno de los procesos de la organización.
- c) Verifica que los procesos establecidos en la presente directiva, sean aplicados en cada una de las dependencias de la Corporación, prestando el apoyo requerido para que las

necesidades de seguridad informática puedan ser atendidas por la Oficina de Tecnología de la Información y las necesidades de seguridad física y de las Instalaciones, sean atendidas por la Oficina de Seguridad Física, realizando las coordinaciones a las que haya lugar y presentando los proyectos que sean requeridos para garantizar la disponibilidad, confidencialidad e integridad de los activos de información corporativos.

- d) Participa y hace seguimiento a las reuniones del Comité de Seguridad de la Información y realiza seguimiento a los compromisos que de éste se derivan en materia de seguridad de la información.
- e) Emite lineamientos, para que los requerimientos tecnológicos y de actualización de plataformas, sean evaluados y avalados por el área de seguridad de la información, esto incluye la adquisición de hardware y software; en el caso de requerir instalaciones o áreas especiales, deberá ser avalado por la oficina de seguridad física.
- f) Supervisa y hace seguimiento al cumplimiento de la presente Directiva.

2) Vicepresidente de Tecnología y Operaciones

- a) Emite las instrucciones para la consolidación del inventario de activos de información de las unidades de negocio de la Vicepresidencia de Tecnología y Operaciones, realizando seguimiento y control sobre las actividades que sobre este tema se impartan.
- b) Hace parte activa del Comité Corporativo de Seguridad de la información.

3) Gerentes y Jefes de Oficina

- a) Integrar el Comité de Seguridad de la Información, de acuerdo como se indica en el Reglamento del Comité Corporativo de Seguridad de la Información.
- b) Verificar que todo el personal de la dependencia tenga diligenciados y firmados los formatos de conocimiento y aceptación de la Política de Seguridad de la Información; autorización y uso adecuado de activos de información y solicitud de acceso a sistemas y recursos de información corporativos (Los formatos se encuentran incluidos en los

anexos de la presente Directiva); remitiéndolos a la Gerencia de Talento Humano para que sean anexados al respectivo contrato de trabajo y/o respectiva “Hoja de vida” del funcionario.

- c) Los Gerentes de las áreas donde se maneje información de nivel calificado y/o clasificado relacionada con los procesos productivos, técnicos, administrativos y de apoyo de la Corporación (Investigación, desarrollo, Innovación, licitaciones, contratación y todas aquellas que puedan verse afectadas por la fuga de información), deberán hacer firmar, adicional a los documentos señalado en el literal “b”, la promesa de reserva y secreto corporativo (formato establecido en el Anexo “H” de la presente Directiva); de igual forma, en el mismo documento, deberá especificarse si el funcionario debe tener acceso a áreas seguras de la corporación.
- d) En caso de pérdida de un activo de información corporativo, aplicar y verificar el cumplimiento del procedimiento establecido, en cuanto a las acciones y actividades a seguir para notificar este tipo de novedades (Procedimiento definido en el Anexo “D” de la presente directiva); de igual forma, diligencia el formato de informe de pérdida de activos de información corporativa (Anexo “Q”).
- e) Garantizar que, en cada reunión operativa, administrativa y/o técnica, donde se tenga acceso a información clasificada que incluya personal externo, se diligencie la promesa de reserva colectiva (Anexo “I” de la presente directiva).
- f) Verificar permanentemente el cumplimiento por parte de su personal, de cada uno de los lineamientos establecidos en la Política de Seguridad de la Información.
- g) Brindar el apoyo que le sea requerido en las inspecciones de verificación que se adelanten por parte del Equipo de Seguridad de la Información, Auditoría Interna y equipos auditores, para constatar el cumplimiento de la presente política.

4) Gerente de Talento Humano

- a) En coordinación con la Oficina Jurídica, verifica que estén integradas en los contratos de trabajo, medidas que permitan dar cumplimiento a lo establecido en la Ley estatutaria 1581 de 2012 “Protección de Datos Personales”, en cuanto a la aceptación de manejo y tratamiento de la información personal (Título IV, Artículo 12).

- b) En los casos que sea detectado un incidente de seguridad de la información (Pérdida y/o afectación de activos de información), deberá adelantar el Procedimiento para comprobación de faltas y formas de aplicación de las sanciones disciplinarias, contemplado en el Capítulo XV del Reglamento Interno de Trabajo de la Corporación; de igual forma, determina el procedimiento para que en los casos en los que se establezca el responsable del activo de información afectado, haga el pago del costo del elemento y/o del deducible establecido por la aseguradora.
- c) Diseña y establece el mecanismo y los procedimientos necesarios, que permitan determinar la aplicación de las acciones administrativas necesarias, para que los responsables por la pérdida, daño o alteración de los activos de información realicen la reparación y/o restitución de los bienes y/o elementos que fueron objeto de las acciones antes descritas.
- d) Verifica que esté integrado en el capítulo XII Obligaciones especiales para Cotecmar y los Trabajadores, del Reglamento Interno de Trabajo, el artículo y subnumeral que indique: “Cumplir con los lineamientos establecidos en la Directiva de Seguridad de la Información para COTECMAR”.
- e) Verifica que esté integrado en el capítulo XIII Prohibiciones especiales para Cotecmar y los Trabajadores, del Reglamento Interno de Trabajo, el artículo y subnumeral que indique: “Incumplir y/o violar los lineamientos establecidos en la Directiva de Seguridad de la Información para COTECMAR”.
- f) Verifica que esté integrado en el capítulo XIV Escala de Faltas y Sanciones Disciplinarias, del Reglamento Interno de Trabajo, como faltas o infracciones Leves, el artículo y subnumeral que indique: “La violación y/o incumplimiento a las políticas de seguridad de la información descritas en la Política de Seguridad de la Información o la vulneración de éstas, cuyo impacto afecte activos de información con nivel de calificación PÚBLICA o PÚBLICA RESERVADA o el nivel equivalente, implica, por primera vez, sanción disciplinaria de un llamado de atención con copia a la hoja de vida; por segunda vez o reincidencia, en este tipo de acciones, hasta dos (2) días de suspensión en el trabajo; a partir de la segunda violación y/o incumplimiento referido en éste numeral, se sancionará al infractor con suspensión en el trabajo hasta por ocho (8) días”.
- g) Verifica que esté integrado en el capítulo XIV, Escala de Faltas y Sanciones Disciplinarias, del Reglamento Interno de Trabajo,

como faltas o infracciones Graves, el artículo y subnumeral que indique: “La violación y/o incumplimiento a las Políticas de Seguridad de la Información descritas en la Política de Seguridad de la Información o la vulneración de éstas, cuyo impacto afecte directa y/o indirectamente los activos de información con nivel de calificación PÚBLICA RESERVADA o EXCEPTUADA o el nivel equivalente”.

- h) Verifica que esté integrado en el capítulo XIV, Escala de Faltas y Sanciones Disciplinarias, del Reglamento Interno de Trabajo, el artículo que indique: “Las infracciones, violaciones y/o incumplimiento de las políticas de seguridad de la información, que después de aplicar el procedimiento para comprobación de faltas y formas de aplicación de las sanciones disciplinarias, sean catalogadas como “moderadas”, tendrán una sanción disciplinaria hasta por ocho (8) días laborales la primera vez; y por segunda vez, suspensión en el trabajo hasta por treinta (30) días.”
- i) Integra en los planes de inducción del personal que se incorpora a la Corporación, temas relacionados con la sensibilización y conocimiento de la política de seguridad de la información.
- j) Integra al archivo de hojas de vida de cada funcionario, los formatos y documentos establecidos en la presente política.
- k) Notifica a la Oficina de Tecnologías de la Información y las Comunicaciones, la causación de cualquier novedad administrativa de personal (retiro, vacaciones, suspensión, licencia, etc.), que implique ausentarse de su trabajo por un período determinado, lo anterior con el fin de tomar las acciones pertinentes sobre los accesos a recursos tecnológicos y sistemas de información corporativos que tenga otorgados.
- l) Hace parte activa del comité de seguridad de la Información de COTECMAR.

5) Jefe Oficina Jurídica:

- a) Verifica que el contenido de los documentos asociados a las actividades de seguridad de la información establecidos en la presente política, estén alineados con la normatividad legal aplicable a cada caso.
- b) Asesora a la alta gerencia y al Comité Corporativo de Seguridad de la Información, sobre las acciones legales que

deben ser adelantadas cuando las consecuencias por la materialización de un evento de seguridad de la información lo requieran.

- c) Acompaña cualquier proceso jurídico a que haya lugar en caso de que un incidente de seguridad de la información tenga alguna repercusión legal.
- d) Hace parte activa del comité de seguridad de la Información de COTECMAR.

6) Jefe Oficina de Tecnologías de la Información y las Comunicaciones

- a) Presenta a la Vicepresidencia Ejecutiva, la estructura de Seguridad de la Información para su validación y posterior aprobación por parte de la Presidencia.
- b) Supervisa y controla la instalación de cualquier tipo de software en los equipos de cómputo al servicio de la corporación, el cual debe enmarcarse en términos de legalidad.
- c) Implementa y administra las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
- d) Registra y mantiene la información requerida para evaluar la ejecución de los controles específicos de seguridad de la información.
- e) Incluye los controles de seguridad de la información en el diseño, desarrollo, instalación y mantenimiento de las aplicaciones bajo su responsabilidad.
- f) Implementa y administra los controles de seguridad sobre la información y conexiones de las redes de datos bajo su gestión.
- g) Custodia la información y los medios de almacenamiento de los centros de datos que se encuentran bajo su responsabilidad.
- h) Supervisa y verifica la implementación de las recomendaciones generadas en los análisis de vulnerabilidades de los activos informáticos de la Corporación.
- i) Define, mantiene y controla la lista actualizada de software y aplicaciones autorizadas; así mismo realizar el control y verificación de cumplimiento del licenciamiento de software y aplicaciones asociadas.

- j) Monitorea y evalúa los procesos o actividades sobre las plataformas tecnológicas y/o servicios, delegados en terceros.
- k) Establece, verifica, monitorea y valida los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.
- l) Establece, documenta, actualiza y difunde los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías que gestionan la información.
- m) Gestiona los programas de capacitación, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con seguridad de la información.
- n) Consolida el plan de continuidad de tecnología en coordinación con la Vicepresidencia Ejecutiva, la Oficina de Sistemas Integrados de Gestión HSEQ y la Oficina de Planeación.
- o) Realiza el análisis de vulnerabilidades a la plataforma tecnológica en coordinación con cada uno de los gerentes de las unidades de negocio, áreas administrativas y de apoyo, con el propósito de generar recomendaciones y mejora continua del sistema.
- p) Asegura de acuerdo con el presupuesto disponible, que, en la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática se realicen mantenimientos periódicos con el objeto de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.
- q) Prepara y presenta ante el Comité de Seguridad de la Información, la información a analizar y deliberar en materia de Seguridad de la Información.

7) Jefe Oficina de Auditoría Interna

- a) Integra dentro de los procesos de verificación y auditoría, los aspectos establecidos en la política de seguridad de la información para COTECMAR.
- b) Incluye dentro de las auditorías realizadas a la Corporación, al líder de seguridad de la Información, para desarrollar verificaciones del cumplimiento de las políticas de seguridad

de la información de las Vicepresidencias, Gerencias y dependencias.

- c) Hace parte activa del comité de seguridad de la información de la corporación.

8) Jefe Oficina Sistemas Integrados de Gestión HSEQ

- a) Verifica que los procesos y procedimientos estandarizados en las herramientas colaborativas y de gestión, estén alineadas con los planteamientos realizados en la presente política.

9) Líder Seguridad Informática y/o Seguridad de la Información.

- a) Actualiza el documento que sintetiza y recopila las políticas de Seguridad de la Información Corporativa, anualmente o cada vez que se requiera.
- b) Adelanta campañas de sensibilización sobre las políticas de Seguridad de la Información y buenas prácticas.
- c) Elabora la programación semestral de visitas de inspección, para confrontar el uso adecuado y seguro de los activos de información corporativa.
- d) Estructura el plan de capacitación básica, que debe ser integrado en el programa de inducción a cada funcionario al momento de su ingreso a la Corporación.
- e) Implementa y realiza mejora continua a las políticas estipuladas en el “Anexo B” de la presente directiva.
- f) Promueve el desarrollo de una cultura de seguridad de la información implementando estrategias de sensibilización, capacitación y concientización, para los funcionarios y terceros.
- g) Gestiona los incidentes de seguridad de la información que se presenten al interior de la Corporación y/o la afecten desde el exterior de esta.
- h) Será competente para adelantar la solicitud de descargos y práctica de pruebas, acuerdo lo establecido en el Reglamento interno de trabajo, en aquellos casos que se presenten infracciones de Seguridad de la Información.

c. INSTRUCCIONES DE COORDINACIÓN

- 1) Las vicepresidencias , gerencias , oficinas y dependencias de la Corporación coordinarán con la Oficina de Tecnologías de la Información , los procesos de apoyo tendientes a cumplir lo establecido en la presente directiva de Seguridad de la Información , en aspectos relacionados con la socialización , sensibilización , diligenciamiento de formatos y aplicación de procedimientos.
- 2) En el anexo “B” de la presente directiva, se presentan los controles y requerimientos aplicables a cada uno de los aspectos considerados en política de seguridad de la información Corporativa , los cuales están alineados al estándar internacional ISO IEC 27002 y las consideraciones propias de la Corporación.

3. DESCRIPCIÓN NARRATIVA

Actualmente , la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval , Marítima y Fluvial , por tratarse de una entidad enfocada a la investigación y desarrollo de nuevas tecnologías, donde se consolida la información y el conocimiento como el activo más valioso para el cumplimiento de los objetivos corporativos ; por este motivo, viene implementando en muchos de sus procesos productivos y operativos , sistemas de información para apoyar cada vez más los procesos de misión crítica, que requieren contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos.

De igual forma, y por ser una entidad del sector defensa , que proyecta las capacidades navales del estado, los sistemas de información, esquemas de conectividad y transporte de información e inclusive el recurso humano, enfrentan amenazas de seguridad que incluyen , entre muchas otras: el fraude por computadora , espionaje , sabotaje , vandalismo , fuego , robo e inundación , lo que implica que las posibilidades de daño y/o pérdida de información por causa de la materialización de un riesgo por acción de la explotación de una vulnerabilidad, se hacen cada vez más comunes.

La presente Política de Seguridad de la Información para COTECMAR , formaliza los deberes, obligaciones y derechos de los funcionarios y terceros que de una u otra forma tienen acceso a los activos de la información Corporativa ; de igual forma , se pretende garantizar la integridad, confidencialidad y disponibilidad de los activos de información, para mantener la continuidad operativa que tiene como derrotero, el cumplimiento de los objetivos misionales y la protección del activo más importante “La información”.

Para mantener a la corporación avante con este objetivo, es importante considerar que las Vicepresidencias, Gerencias, Oficinas y dependencias de COTECMAR, se comprometan con los siguientes aspectos:

a. Revisión independiente – Revistas internas

Cada Unidad Organizacional y dependencia de la Corporación, es responsable de garantizar que se realicen revisiones periódicas al cumplimiento de la Política de Seguridad de la Información, para verificar su vigencia, correcto funcionamiento y efectividad.

b. Acuerdos de confidencialidad

Todos los funcionarios y terceros deben firmar la cláusula o acuerdo de confidencialidad que deberá ser parte integral de los contratos, contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal, aprendices o cuando se permita el acceso a la información o a los recursos, a personas o entidades externas.

c. Acuerdos de intercambio de información y software

- 1) Todo funcionario o tercero es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
- 2) Los propietarios de información que se requiera intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por su parte, los custodios de esta son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad, de acuerdo con la reglamentación vigente.
- 3) El intercambio de información y de software con otras entidades, se realiza previa celebración de convenio, contrato o acto interadministrativo, en el que se deben establecer cláusulas de responsabilidad, deberes y derechos.
- 4) Los protocolos de intercambio deben, en todo caso, velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo, deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de esta.

- 5) Cuando la información sea solicitada por autoridad judicial o administrativa competente, la entrega se realizará siguiendo el procedimiento establecido por la Corporación para la entrega de la información solicitada (Anexo E “Procedimiento para entrega de información a terceros”).
- 6) El intercambio de información deberá contemplar las siguientes directrices:
 - a) Respeto por los derechos de autor.
 - b) Términos y condiciones bajo la cual se suministra o intercambia la información.
 - c) Aplicación de los parámetros establecidos en el Anexo “F” “Reglas de Clasificación y Niveles de Acceso de la Información Clasificada de COTECMAR”.
 - d) Informar al titular de los datos, sobre las actividades de intercambio de éstos con otras entidades.
 - e) Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

d. Acciones Disciplinarias

El incumplimiento a los lineamientos establecidos en la Política de Seguridad de la Información de COTECMAR, dará lugar al inicio de las acciones disciplinarias y administrativas que se consideren pertinentes y se ajusten a la calificación de la falta cometida, de acuerdo con el reglamento interno de trabajo; sin embargo, es importante considerar que las acciones que atenten contra los activos de información, que se considere que están enmarcados en la Ley 1273 de 2009 “Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”, darán lugar al inicio de las acciones legales respectivas.

4. DISPOSICIONES ADMINISTRATIVAS

- a. Las políticas dispuestas en la presente directiva, los procedimientos enunciados en el alcance y sus anexos son de obligatorio cumplimiento, con el propósito de mejorar los esquemas de seguridad informática y de la información de la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y fluvial - COTECMAR y se implementarán de manera inmediata.
- b. Los planes de contingencia y disposiciones derivadas de esta directiva deberán contener todos los mecanismos de prevención, detección, recuperación y análisis tendientes a fortalecer y garantizar altos niveles

de seguridad de la información.

- c. Al término del primer año de aplicación , la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y fluvial – COTECMAR , evaluará los niveles de desarrollo e implementación de estas políticas de seguridad.
- d. Todos los equipos , infraestructura y aplicaciones dispuestos al servicio del personal contratado , son propiedad de COTECMAR y sólo se permite su utilización para desarrollar las tareas establecidas en el ámbito laboral.
- e. La información manejada en medios físicos, electrónicos, instalaciones físicas y por el personal corporativo, son propiedad de la Corporación y, por tanto , solo debe ser utilizada para las actividades propias del negocio, quedando estrictamente prohibido el envío de información a terceros sin autorización del Jefe Inmediato, Vicepresidencias o Presidencia de la Corporación, según sea el nivel de calificación o clasificación de esta.
- f. La Corporación hará conocer al usuario de activos de información , la presente política y las consecuencias que se derivarían de su incumplimiento. Así mismo, el usuario se compromete, desde el mismo momento de su ingreso a la Corporación , a acatarlas , dejando constancia de ello con la firma del Anexo “G” Declaración de Aceptación y Compromiso de Cumplimiento Políticas de Seguridad de la Información”, por parte del usuario.
- g. La Corporación se reserva el derecho de evaluar periódicamente el cumplimiento de lo establecido en la Política de Seguridad de la Información para COTECMAR . Cualquier falta derivada del incumplimiento de esta (tales como llamadas de atención , suspensiones o despidos), se realizará de acuerdo con la clasificación y sanciones que para ello estipule el Reglamento Interno del trabajo de COTECMAR.
- h. En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con esta política será directamente responsable de las sanciones legales (que, por responsabilidad laboral , penal y/o civil se incurra), derivadas de sus propios actos . Igualmente , será responsable de los costos y gastos en que pudiera incurrir la Corporación , derivados de la defensa por el uso no autorizado o indebido de licencias de software . En razón de lo anterior , no es permitido alegar ignorancia a estas políticas (cuya última versión siempre estará disponible en la Intranet Corporativa).
- i. Los equipos tecnológicos y cuentas asociadas son dadas a los usuarios para facilitarles su trabajo. Los usuarios no deben tener una expectativa de privacidad en relación con cualquier material que creen,

almacenen, envíen o reciban en los equipos suministrados por la Corporación para el cumplimiento de sus funciones. Estos equipos pertenecen a la Corporación y deben ser utilizados para propósitos relacionados exclusivamente con el objeto social de la corporación

- j. Los usuarios renuncian expresamente a la privacidad en relación con cualquier material que ellos creen, almacenen, envíen o reciban en el computador corporativo, a través de Internet o de cualquier otra red de la corporación o al servicio de esta.
- k. La Corporación, a través del área de seguridad de la Información o a quien por necesidad o requerimiento corporativo se delegue, podrá acceder y revisar periódicamente, cualquier tipo de material que los funcionarios de COTECMAR creen, almacenen, envíen o reciban en los equipos tecnológicos suministrados por la corporación, a través de Internet o de cualquier otra red al servicio de esta. Los usuarios entienden y aceptan que la Corporación puede utilizar procedimientos y recursos manuales o automáticos para monitorear la utilización de los recursos tecnológicos Corporativos.
- l. En el caso en el que razonablemente se asuma que el usuario está haciendo uso ilegal o incorrecto de los recursos tecnológicos, la Corporación estará en absoluta libertad de limitar o remover estos recursos, sin asumir por ello responsabilidad de ningún tipo.

5. REFERENCIAS

- a. Constitución Política de Colombia.
- b. Ley 57 de 1985 Publicidad Datos y Documentos Oficiales
- c. Ley 80 de 1993 “Estatuto general de contratación de la administración pública”.
- d. Ley 87 de 1993 “Control Interno en los organismos del Estado”.
- e. Ley 527 de 18 de agosto de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones” y su Decreto 1747 de 2000 “Por el cual se reglamenta parcialmente esta Ley.
- f. Ley 594 de 2000 “Ley General de Archivo”.
- g. Ley 599 de 2000 “Código Penal Colombiano”.
- h. Ley 603 de 2000 “Control de Legalidad del Software”.
- i. Ley 734 de 2002 “Código Disciplinario Único”.
- j. Ley 1266 de 2008 “Por lo cual se dictan disposiciones generales de habeas data y se regula el manejo de información”.
- k. Ley 1273 de 2009 “Protección de la información y de los Datos”.
- l. Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.

- m. Ley 1712 de 2014 Transparencia y Derecho a la información.
- n. Decreto Ley 2663 “Código sustantivo del trabajo”.
- o. DIR2014-18 Ministerio de Defensa del 19 de junio de 2014 “Políticas de seguridad de la información para el sector defensa”.
- p. Directiva 009/2015 “Políticas de Seguridad de la Información para la Armada Nacional”
- q. Manual Fundamental de Contrainteligencia Naval Versión tres (03) 2014
- r. Norma Técnica Colombiana NTC – ISO/IEC 27000.
- s. Reglamento interno de trabajo COTECMAR.
- t. Código de ética COTECMAR.
- u. Manual de las políticas de gestión humana.

6. DEROGATORIA

A partir de la vigencia de la presente Directiva Permanente, los lineamientos contenidos en anteriores Directivas o Disposiciones quedan derogados y por ende sin validez, de tal motivo que no se deberá aplicar en lo absoluto.

7. VIGENCIA

La presente Directiva rige a partir de la fecha de su expedición.


Vicealmirante LUIS FERNANDO MÁRQUEZ VELOSA
Presidente COTECMAR

Anexos:

Anexo "A"	Glosario, Definiciones y Términos de Seguridad de la Información
Anexo "B"	Normas y Estándares de Seguridad de la Información para COTECMAR
Anexo "C"	Procedimiento de Identificación y tratamiento del Riesgo
Anexo "D"	Procedimiento por pérdida, daño o afectación de activos de información corporativos
Anexo "E"	Procedimiento entrega de información a terceros
Anexo "F"	Reglas de Calificación y Niveles de Acceso de la Información Clasificada de COTECMAR
Anexo "G"	Declaración de Aceptación y Compromiso de Cumplimiento Políticas de Seguridad de la Información
Anexo "H"	Formato promesa de reserva y secreto corporativo
Anexo "I"	Formato Acta Promesa de Reserva Colectiva
Anexo "J"	Formato Acta Compromiso de Reserva por Desvinculación o Cambio de Rol
Anexo "K"	Formato Solicitud Recursos y Servicios de Tecnología y Uso Adecuado de los Mismos
Anexo "L"	Formato Autorización Ingreso/Salida de Equipos de Cómputo y Accesorios Corporativos
Anexo "M"	Formato Inventario de Activos de Información
Anexo "N"	Formato Reporte Incidentes de Seguridad
Anexo "O"	Formato de Excepción de Instalación Herramienta de Seguridad
Anexo "P"	Formato informe por pérdida, daño o afectación de activos de información corporativos

HISTÓRICO DE ACTUALIZACIONES

FECHA	ELABORÓ	REVISÓ	APROBÓ	FECHA DE APROBACIÓN	SECCION No.	DESCRIPCION DEL CAMBIO
02-Sep-2020	JOFTIC	VPEXE	PCTMAR		Numeral 1, Literal B	Se incluyen los objetivos específicos de la directiva, alineándolos con la norma ISO – 27001.
02-Sep-2020	JOFTIC	VPEXE	PCTMAR		Numeral 2, Literal B, Subnumeral 4	Se cambia la actividad de incluir en el RIT, por verificar la inclusión en el RIT de las acciones disciplinarias y administrativas que puede tomar la corporación.
02-Sep-2020	JOFTIC	VPEXE	PCTMAR		Numeral 2, Literal A, Subnumeral 7	Se cambia la denominación de Oficina de Control Interno a Oficina de Auditoría Interna.
19-Abr-2024	JOFTIC	VPEXE	PCTMAR		Numeral 2, Literal B, Subnumeral 4	Se ajustan literales acuerdo actualización del RIT
19-Abr-2024	JOFTIC	VPEXE	PCTMAR		Numeral 2, Literal B, Subnumeral 9	Se incluye el subliteral h en complemento a las Responsabilidades del Líder de Seguridad de la Información



ANEXO “A”

GLOSARIO, DEFINICIONES Y TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN

D-PERMA-043

Versión: 1

Fecha de Aprobación: 19 Abr 2024

TÉRMINO	DEFINICIÓN
Activos	Algo que posee valor potencial o real para una organización. El valor puede variar entre diferentes organizaciones y sus partes interesadas y puede ser tangible o intangible, financiero o no financiero. ¹
Activos de Información	Bases de datos, documentación física y digital, hardware, software, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado...) y las personas (quienes genera, transmiten y destruyen información). ²
Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización. ³
Amenaza Informática	Aparición de una situación potencial o actual donde un agente tiene la capacidad de genera una agresión cibernética contra la población, el territorio y la organización política del estado. ⁴
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. ⁵
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. ⁶
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. ⁷
Evaluación de riesgos	Todo proceso de análisis y valoración del riesgo. ⁸
Evento de Seguridad de la Información	Presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación previamente desconocida que puede ser pertinente para la seguridad. ⁹
Gestión del Riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. ¹⁰
Incidente de Seguridad de la Información	Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información. ¹¹
Integridad	Propiedad de la información relativa a su exactitud y completitud. ¹²

¹ Norma Técnica Internacional ISO – 55000. Gestión de activos. Aspectos generales, principios y terminología. 2014

² Norma Técnica Internacional ISO/IEC – 27000. Estándar sobre Sistemas de Gestión de Seguridad de la Información. 2005

³ Norma Técnica Colombiana NTC – ISO/IEC – 27002. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. 2007.

⁴ Documento CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa. 2011

⁵ Documento CONPES 3701. Lineamientos de Política para Ciberseguridad y Ciberdefensa. 2011

⁶ Norma Técnica Internacional ISO/IEC – 27000. Estándar sobre Sistemas de Gestión de Seguridad de la Información. 2005

⁷ Norma Técnica Internacional ISO/IEC – 27000. Estándar sobre Sistemas de Gestión de Seguridad de la Información. 2005


⁸ Norma Técnica Colombiana NTC – ISO/IEC – 27002. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. 2007.

⁹ Ídem

¹⁰ Ídem


¹¹ Norma Técnica Internacional ISO/IEC – 27000. Estándar sobre Sistemas de Gestión de Seguridad de la Información. 2005

¹² Norma Técnica Internacional ISO/IEC – 27000. Estándar sobre Sistemas de Gestión de Seguridad de la Información. 2005

	<p style="text-align: center;">ANEXO “A”</p> <p style="text-align: center;">GLOSARIO, DEFINICIONES Y TÉRMINOS DE SEGURIDAD DE LA INFORMACIÓN</p>		
	D-PERMA-043	Versión: 1	Fecha de Aprobación: 19 Abr 2024

Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. ¹³
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información. Además de otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucrados. ¹⁴
Sistema de Gestión de Seguridad de la Información (SGSI)	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. ¹⁵
Tratamiento del Riesgo	Proceso de selección e implementación de medidas para modificar el riesgo. ¹⁶
Valoración del Riesgo	Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. ¹⁷
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas. ¹⁸

¹³ Ídem¹⁴ Ídem¹⁵ Tomado de: <https://www.iso27000.es/glosario.html>¹⁶ Norma Técnica Colombiana NTC – ISO/IEC – 27002. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. 2007.¹⁷ Ídem¹⁸ Ídem

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

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 de información 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 esta área será considerado como una falta y los responsables del incumplimiento o violación de estas, 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.

En el marco del cumplimiento y aplicación de la presente directiva, se aclara que con respecto a trabajadores vinculados a través de empresas de servicios temporales, considerando que en muchos casos, tiene acceso a las herramientas y plataformas informáticas con las que cuenta la Corporación (correos corporativos, mensajería instantánea, internet, intranet), ellos también tienen la obligación de cumplir con las políticas de seguridad de la información Corporativa, sin que esto implique ningún tipo de relacionamiento laboral entre COTECMAR y el funcionario vinculado a través de la empresa de servicios temporales, para lo cual, las empresas temporales, deben dar a conocer a sus empleados la presente política, diligenciando y firmando los documentos establecidos en la misma, haciendo claridad sobre la aplicación de las acciones disciplinarias, administrativas y/o penales que en cada caso se requieran por el incumplimiento de las mismas.


Para tal efecto, se establecen los siguientes aspectos:

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

El “Comité Corporativo de Seguridad de la Información”, se establece como el máximo organismo Corporativo para asuntos relacionados con la Seguridad de la Información, estará integrado de conformidad como se establece en el reglamento del Comité, para lo cual, todos los representantes de las áreas productivas, de apoyo y operativas de la Corporación, deberán tener conocimiento de este y lo aplicarán conforme a como se indica en el reglamento.

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 da 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

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

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 esta, 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 con el procedimiento de Inventario y Clasificación de Activos de Información. (Anexo “M”).
- 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 con el 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 con el 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 considerarán aceptables los siguientes usos:

- a. Internet:

La navegación en internet estará controlada de acuerdo con las categorías de navegación

	<p style="text-align: center;">ANEXO “B”</p> <p style="text-align: center;">NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR</p>		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

definidas para los usuarios y solo debe ser utilizado para la atención de los requerimientos y necesidades propias en el ejercicio de las funciones; 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 de información no autorizados, así como, el almacenamiento de información crítica corporativa en servicios de nube pública.
- 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 considerados dentro del esquema de licenciamiento de la Corporación.
- 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 corporativa.
- 12) Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios y terceros autorizados. Así mismo, se puede inspeccionar, registrar, permitir o bloquear el acceso de conectividad a la red corporativa si se evidencia un uso inadecuado 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 a la OFTIC y deben ser justificados por el 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 “K”).
- 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

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

mantener solamente los mensajes relacionados con el desarrollo de sus funciones. Por este motivo la información y el tráfico de esta, se consideran de interés de la Corporación.

- 3) El correo corporativo de cada funcionario se creará con inicialprimernombreapellido@cotecmar.com, en caso de que el usuario ya exista se creará como inicialprimernombreinicialsegundonombreapellido@cotecmar.com.
- 4) Para el correo saliente, con información clasificada o sensible, debe ser transmitida 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 máximo de cien (100) 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 de 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.
 - f)

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

- g) La utilización de la identificación del buzón, para suscripción a servicios digitales, descarga de software, identificación ante cualquier servicio en línea, descarga de contenido digital, manejo y gestión de información de índole personal no relacionada con el cumplimiento de sus funciones y cualquier otra actividad que no se considere de interés corporativo.
 - h) Inicio de sesión y/o activación de productos mediante el uso de la cuenta de correo corporativa “@cotecmar.com” en equipos de cómputo que no sean de propiedad de Cotecmar y que en estos además se tengan instaladas herramientas informáticas no autorizadas por sus fabricantes (licencias de origen desconocido, fraudulentas o crackeadas, etc.)
- 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 con lo establecido por el Departamento de Comunicaciones Estratégicas de la Corporación.

- 14) Una vez termine la relación laboral, contractual, comercial y de cualquier índole que impulsó la creación de la cuenta de correo electrónico corporativo, esta deberá ser comunicada a la Oficina de Tecnologías de la Información y las Comunicaciones, para que sea cerrada y recuperado el buzón con el fin de tener disponible la licencia para asignación a otro solicitante. Es responsabilidad del área en la cual se desempeñaba el asignatario de la cuenta de correo, de realizar la extracción de la información que consideren necesaria para su aseguramiento y control.

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, por lo que todo

	<p align="center">ANEXO “B”</p> <p align="center">NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR</p>		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

- equipo de Cómputo corporativo será configurado con una cuenta de Usuario estándar.
- 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 estos.
 - 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, 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, 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 antispyware 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/o tratamiento de datos corporativos, deberá ser canalizado por intermedio de la Oficina de TIC; siendo obligatorio, que la División de Adquisiciones, exija que este 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 “L” Solicitud Ingreso Salida de Equipos de Cómputo 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 asignando más recursos tecnológicos de los que de acuerdo con la evaluación técnica le son entregados.

	<p style="text-align: center;">ANEXO “B”</p> <p style="text-align: center;">NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR</p>		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

- p. Para el caso del personal de contratistas que requieran el ingreso y uso de equipos de cómputo dentro de la corporación bajo la actividad propia del objeto del contrato, deberán contar con la configuración básica: antivirus comercial, sistema operativo con últimos parches de seguridad, paquete de ofimática, y el software que se requiera para el ejercicio de sus funciones, todos estos debidamente licenciados, los cuales deberán ser verificados por personal técnico de la OFTIC con el fin que se les pueda autorizar el acceso y uso de los servicios dentro de la red corporativa.
 - q. Las cuentas de Usuario administrador serán configuradas en los equipos de cómputo corporativos y solo serán de uso exclusivo del personal técnico de OFTIC.
 - r. Los usuarios deben aplicar las siguientes recomendaciones para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:
 - i. Las contraseñas son de uso personal y por ningún motivo se deben prestar a otros usuarios.
 - ii. Las contraseñas no deberán ser reveladas por ningún motivo.
 - iii. Las contraseñas no se deberán escribir en ningún medio.
 - iv. Es deber de cualquier usuario reportar cualquier sospecha que una persona está empleando un usuario y contraseña que no le pertenece.
 - v. La longitud mínima de las contraseñas debe ser de 8 dígitos y contener mínimo una mayúscula, una minúscula, un número y un carácter especial.
 - vi. Las contraseñas no deben estar basadas en temas que puedan descifrarse fácilmente o usando información relacionada con la persona (nombres, números de teléfono, identificación, fechas de nacimiento, etc).
 - vii. Las contraseñas deben estar libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos.
 - viii. En caso de que un tercero deba por razones del servicio conocer una contraseña, la misma deberá ser cambiada dentro de las 24 horas siguientes.
 - s. Para el uso de dispositivos de telefonía móvil, se deben implementar controles de acceso como pin, contraseñas o patrones.
 - t. La conexión de los dispositivos móviles a la red inalámbrica corporativa deberá ser debidamente autorizada por la OFTIC, previa verificación que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura.
 - u. El asignatario de un dispositivo móvil corporativo deberá mantener siempre actualizadas las aplicaciones y el sistema operativo de este.
 - v. No está permitida la alteración de la información que identifica el dispositivo móvil (IMEI, Dirección MAC, etc.).
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,

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

- d. portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
- e. 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.
- f. 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 estos 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 activo de información 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 pérdida, 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 corporativas 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, generará el respectivo paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.
- g. Los equipos de cómputo portátiles Corporativos de los trabajadores los cuales sean autorizados para trabajar en la modalidad de teletrabajo suplementario, en caso de presentarse daño, extravío, pérdida total o parcial por causa imputable a la responsabilidad del trabajador, por descuido, uso indebido y/o malos tratamientos deberá hacerse cargo de las responsabilidades legales y/o administrativas que tuviesen lugar.
- h. Solo se podrá tener acceso a los servicios y la información Corporativa desde redes externas mediante un proceso de autenticación y uso de conexiones seguras como VPN previamente solicitadas por el usuario al personal técnico de la OFTIC.


	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

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 el respectivo 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 las aplicaciones deberán mantener un adecuado proceso de actualización y parcheo, de acuerdo cómo 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.

	<p align="center">ANEXO “B”</p> <p align="center">NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR</p>		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

10. Derechos de propiedad intelectual


- 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.
- 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.
- Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
- Los procesos de adquisición de aplicaciones y paquetes de software 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.
- 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

- La declaración de aplicabilidad menciona los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información y realizar el análisis de riesgos, así como los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y, por ende, en las definiciones dadas en el plan de tratamiento del riesgo.
- Estos controles están basados en el código de buenas prácticas definido en la norma ISO/IEC 27002.
- 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

- 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.
- 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.
- 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.

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

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 antispyware 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 calificada, 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”.

	<p style="text-align: center;">ANEXO “B”</p> <p style="text-align: center;">NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR</p>		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

- i. Los usuarios asignatarios de las estaciones de trabajo de escritorio y portátiles son responsables de la elaboración de 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 establecidas en la directiva.
- j. En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
- k. Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.
- l. Todas las estaciones de trabajo deben emplear únicamente el papel tapiz y el protector de pantalla establecido por COTECMAR.
- m. Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos o accesos directos a los mismos, para esto se debe hacer uso correcto del espacio en el disco local del equipo o en las unidades de red dispuestas por la OFTIC.
- n. No está permitido a los funcionarios hacer uso de equipos de cómputo de carácter personal dentro de las instalaciones de COTECMAR.

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 relacionadas 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, definiéndose este 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 LUIS FERNANDO MÁRQUEZ VELOSA
 Presidente COTECMAR

	ANEXO “B” NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN PARA COTECMAR		
	D-PERMA-043	Versión: 2	Fecha de Aprobación: 19 Abr 2024

HISTÓRICO DE ACTUALIZACIONES

FECHA	ELABORÓ	REVISÓ	APROBÓ	FECHA DE APROBACIÓN	SECCIÓN No.	DESCRIPCIÓN DEL CAMBIO
30-Oct-2020	JOFTIC	VPEXE	PCTMAR		Numeral 1	Se hace el cambio del texto, para que se haga referencia al Reglamento del Comité Corporativo de Seguridad de la Información.
19-Ene-2024	JOFTIC	VPEXE	PCTMAR		Numeral 4, Literal a	Se hace complemento de los numerales 5 y 12 en el uso del servicio de internet.
19 Abr 2024	JOFTIC	VPEXE	PCTMAR		Numeral 4, Literal b, Subnumeral 11	Se incluye subliteral g como complemento al uso adecuado del correo electrónico
19 Abr 2024	JOFTIC	VPEXE	PCTMAR		Numeral 5	Se hace complemento del literal a en el control de los recursos tecnológicos. Se incluyen literales p, q, r, s, t, u, v como complementos al Control de los Recursos Tecnológicos
19 Abr 2024	JOFTIC	VPEXE	PCTMAR		Numeral 7	Se incluyen los literales g, h como complemento a la Seguridad de los equipos fuera de las instalaciones
19 Abr 2024	JOFTIC	VPEXE	PCTMAR		Numeral 15	Se incluyen los literales j, k, l, m, n como complemento a Estaciones de Trabajo