GrupoMarina®

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:	Aprobado por:
Encargado de Ciberseguridad **Fecha:** 24-06-2024	Gerente de TI **Fecha:** 01-07-2024 Gerente de Auditoría y Contraloría **Fecha:** 23-07-2024 Gerente de Adm y Finanzas **Fecha:** 31-07-2024	Gerente General **Fecha:**

Contenido

1. INTRODUCCIÓN

La información es uno de los principales activos de Grupo Marina y su protección es esencial para asegurar la continuidad, el desarrollo y la imagen del negocio. Esta protección no solo es una exigencia legal, sino también una forma de generar confianza en nuestros clientes, proveedores, accionistas, visitantes y colaboradores.

La seguridad de la información es responsabilidad de todos los integrantes de la organización. Este documento establece directrices e instrucciones para gestionar los temas de seguridad, describir y asignar responsabilidades, y proporcionar un marco de referencia para velar por la confidencialidad, disponibilidad e integridad de la información.

2. OBJETIVO

- Establecer los lineamientos corporativos para la seguridad de la información por medio de un marco general de principios sobre el cual se elaboran las políticas, normas y procedimientos asociados.
- Promover una cultura de seguridad de la información en Grupo Marina y sus socios de negocio.
- Salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.
- Identificar las amenazas y tratar los riesgos de los activos de información.
- Cumplir con las regulaciones legales o reglamentarias vigentes donde Grupo Marina opera, basándose en estándares internacionales (ISO 27001, NIST)

3. ALCANCE

Abarca de manera integral y transversal todas las operaciones, sistemas, recursos y procesos críticos que se relacionen directa o indirectamente con los activos de información, esto incluye tanto la información digital como la información impresa, así como los ambientes y recintos en los que se almacena, procesa y transmite.

Se aplica a todos los colaboradores, clientes, proveedores, visitantes y más amplio, todo aquel que tenga relación con Grupo Marina (stakeholder), y que accedan a sus dependencias, ya sea de manera física o remota, para utilizar datos almacenados o procesados por la empresa, y/o que utilicen recursos tecnológicos provistos por la organización.

4. DEFINICIONES

- **Socios de negocio:** Todo proveedor, cliente, contratista que tiene Grupo Marina.

- **Stakeholder:** Cualquier individuo, grupo u organización que se relacione con Grupo Marina y que puede afectar o ser afectado por las actividades, decisiones y políticas de la organización.

- **Activo de información:** Se refiere a cualquier elemento valioso para el cumplimiento de los objetivos de la organización. Se divide en tres niveles:
    - Información: En cualquier formato ya sea físico o digital, texto, imagen, audio, video, etc.
    - Tecnología: Cualquier equipo, sistema, aplicación, red y/o tecnología en general donde se realice tratamiento de la información.
    - Personas: Cualquier persona ya sea interna o externa que utilice dicha información.

- **Tratamiento de información:** Actividad de creación, modificación, procesamiento, almacenamiento, transmisión, consulta, eliminación y/o cualquier otra que tenga relación con manipulación de información.

- **Política general de seguridad de la Información:** Directriz u orientación general para la seguridad de la información en Grupo Marina, de la cual se desprenden políticas, normas y procedimientos.

- **Normas de seguridad de la Información:** Directrices “específicas” donde se establecen, regulaciones, obligaciones, restricciones y prohibiciones corporativas.

- **Procedimiento:** Secuencia temporal de operaciones interrelacionadas, destinadas a llevar a cabo una actividad o tarea específica dentro del campo de los controles de Seguridad de la Información.

- **Confidencialidad:** Propiedad de la información que garantiza que los datos solo sean accesibles para aquellas personas, entidades, sistemas y/o procesos que estén debidamente autorizados.

- **Integridad:** Propiedad de la información que garantiza que los datos no sean modificados o alterados de manera indebida, ya sea por error humano, por una acción malintencionada o fallos en el sistema, permitiendo que la información conserve su confiabilidad y precisión.

- **Disponibilidad:** Propiedad de la información que garantiza su accesibilidad y utilización a las personas, entidades, sistemas y/o procesos autorizados cuando estos la necesiten.

5. DOCUMENTOS RELACIONADOS

A continuación, se dan a conocer todos los documentos que forman parte integral de esta política formalizados y publicados al día de hoy por la Compañía. (se irá actualizando de acuerdo a la publicación de cualquier documento relacionado).

- **Reglamento interno de orden, higiene y seguridad:** Establece las normas, directrices, derechos y obligaciones de los colaboradores con el objetivo de lograr y mantener un ambiente laboral armonioso y productivo. Asimismo, se indican las sanciones e infracciones en caso de incurrir en una falta.
- **Código de conducta y ética:** Define los principios básicos que deben guiar el actuar de todos los colaboradores en el desarrollo de sus funciones, orientados a los más altos estándares éticos y en concordancia con la misión y visión de la empresa.

6. RESPONSABILIDADES

A continuación, se ofrece una visión general de las responsabilidades y obligaciones en materia de gestión y cumplimiento de esta política.

Responsable	Función
Encargado de Ciberseguridad	✓ Desarrollar políticas, normas y procedimientos relacionados con la seguridad de la información y ciberseguridad. ✓ Identificar, evaluar, clasificar y gestionar los riesgos que afecten la seguridad de la información. ✓ Proponer estrategias, soluciones o controles para el tratamiento de los riesgos. ✓ Velar por la seguridad de la información y ciberseguridad asegurando el cumplimiento y actualización de las políticas y de gestionar la administración de la seguridad de la información. ✓ Gestionar el tratamiento de los incidentes que afecten la seguridad de la información de Grupo Marina. ✓ Responsable de entregar formación y concientización a los colaboradores en materias de ciberseguridad.
Gerente de TI	✓ Revisar, corregir y orientar las políticas, normas y procedimientos en función de los objetivos de Grupo Marina a corto, mediano y largo plazo, dirigiéndolas hacia un equilibrio entre la seguridad y la operación del negocio. ✓ Garantizar que la Política de Seguridad de la Información y sus objetivos estén establecidos y sean compatibles con la dirección estratégica de Grupo Marina.
Gerente de Auditoría y Contraloría	✓ Otorgar aseguramiento al directorio sobre el cumplimiento de la Política de Seguridad de la Información y sus ramificaciones por medio de auditorías internas o externas.
Gerente de Administración y Finanzas	✓ Asegurar los recursos necesarios para lograr que los objetivos de la Política de Seguridad de la Información se concreten.
Gerente General	✓ Impulsar de manera transversal el cumplimiento, compromiso y adherencia con respecto la Política de Seguridad de la Información.
Colaboradores y socios de negocio	✓ Identificar y comunicar el riesgo de cualquier activo de información o proceso del cual son responsables. ✓ Utilizar la información sólo para el propósito para el que se recibió autorización. ✓ Conocer y cumplir la Política de Seguridad de la Información junto con sus normas y procedimientos que desde ahí se desprenden. ✓ Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización. ✓ Comunicar los incidentes relacionados con la seguridad de la información.

7. ACTIVIDADES

La alta gerencia de Grupo Marina destaca y comunica la importancia y el compromiso corporativo con la seguridad de la información. Para ello, publican esta política que servirá de base para la implementación de un Sistema de Gestión de Seguridad de la Información, cuyo objetivo es proteger la confidencialidad, integridad y disponibilidad de los activos de información señalados en el alcance.

La organización debe asegurar la protección de su información y la de terceros de acuerdo con su valor y sensibilidad, sin importar el medio en que se encuentre, cada colaborador y/o proveedor dueño de cualquier activo de información o proceso, debe identificar y comunicar cualquier riesgo que pueda impactar a la seguridad de la información al Encargado de Ciberseguridad para que evalúe, clasifique y gestione el riesgo por medio de controles administrativos y/o técnicos. Así mismo, el Encargado de Ciberseguridad también puede identificar el riesgo de manera transversal en todos los activos de información y procesos de Grupo Marina.

Las medidas de control implementadas deben estar alineadas con la estrategia de seguridad de la información y los objetivos de la empresa, así como con las regulaciones, normas y leyes vigentes en los lugares donde Grupo Marina opera.

Para proteger los activos de información, se debe contar con tecnología de seguridad, establecer procesos sólidos, asignar recursos y personal necesarios, y generar una cultura de seguridad de la información en todos los colaboradores de Grupo Marina, esto por medio de campañas de capacitación, formación, entrenamiento y evaluaciones. También, se deben realizar de forma periódica análisis de riesgos de seguridad de la información, de manera de que estos se gestionen y traten de forma adecuada mitigando así sus impactos.

Esta política debe ser aplicada, difundida y conocida por todos los colaboradores, socios de negocio y stakeholders de Grupo Marina y su incumplimiento constituye una falta grave. En caso de un incumplimiento por parte de un colaborador, será sancionado de acuerdo con lo estipulado en el *"Reglamento interno de orden, higiene y seguridad"* y el *"Código de Conducta y Ética";* por otro lado, en caso de un incumplimiento por parte de un socio de negocio se aplicarán las sanciones estipuladas a nivel contractual y/o según lo establecido en los elementos de protección de *"Gestión Proveedores",* según corresponda. Todas las políticas, normas y procedimientos que se deriven de esta política también se consideran parte integral de la misma.

El Encargado de Ciberseguridad, debe asegurar la implementación, cumplimiento, revisión y mejora continua de las políticas, normas y procedimientos específicos de seguridad de la información señaladas en el "*punto 5"* de este documento y contará con el respaldo y apoyo de la alta gerencia para lograrlo.

8. GENERALIDADES.

8.2 Responsabilidad del documento.

Será responsabilidad del Encargado de Ciberseguridad difundir y velar por el cumplimiento de esta política y será responsabilidad de la Alta Gerencia revisar y aprobar esta política en las instancias que corresponda, según lo establecido.

8.3 Vigencia y mantenimiento del documento.

Esta política se actualizará al menos una vez al año o frente a cambios del entorno.

9. ELEMENTOS DE PROTECCIÓN

Los elementos de protección son políticas, normas y/o procedimientos que tienen como objetivo salvaguardar de manera específica los activos de información involucrados en los procesos que se llevan a cabo en Grupo Marina. Cada gerencia o área propietaria de un proceso debe considerar dentro de su gestión (entre otros que se puedan identificar y agregar en un futuro), los siguientes elementos de protección en su desarrollo.

- **Gestión de recursos humanos:** Proteger la información durante los procesos de selección, contratación, vigencia del contrato, remuneraciones y una vez finalizada la relación laboral con los colaboradores.
- **Gestión de activos de información:** Lograr y mantener una protección adecuada de los activos de información en todas sus formas y medios, a través de un proceso de gestión que incluya actividades de clasificación.
- **Gestión de criptografía:** Utilizar de manera eficaz el cifrado, a fin de proteger la confidencialidad e integridad de la información.
- **Gestión de control de acceso lógico:** Controlar el acceso a la información digital para evitar el acceso no autorizado, protegiendo su confidencialidad e integridad.
- **Gestión de seguridad física y ambiental:** Controlar el acceso físico a los lugares sensibles y restringidos, evitar el daño a las instalaciones y la realización de actividades no autorizadas.
- **Gestión de las operaciones:** Operar de manera segura y correcta los medios de procesamiento de información, evitando la divulgación no autorizada, la corrupción de los datos y la pérdida de disponibilidad.
- **Gestión de las comunicaciones:** Proteger la información transmitida en las redes y en las instalaciones de procesamiento.
- **Gestión de adquisición, desarrollo y mantenimiento de sistemas de información:** Integrar la seguridad de la información en todo sistema, desde su desarrollo y mantenimiento hasta el final de su vida útil.
- **Gestión de proveedores:** Proteger los activos de información accesibles a los proveedores, evitando la divulgación no autorizada, la corrupción y la pérdida de información.
- **Administración de incidentes de seguridad de la información:** Detectar, reportar, evaluar, responder y recopilar evidencias ante incidentes de seguridad de la información.
- **Administración de continuidad del negocio:** Garantizar que la organización pueda continuar con sus operaciones esenciales durante y después de una interrupción significativa.
- **Cumplimiento:** Prevenir infracciones a la legislación vigente, regulaciones y obligaciones contractuales; garantiza el cumplimiento de las políticas, normas y procedimientos internos.
- **Gestión en la nube:** Utilizar y administrar los servicios y recursos en la nube, orientandolos a la seguridad de la información y a las buenas prácticas.
- **Gestión de identidades:** Administrar de manera segura y eficiente las identidades digitales y la gestión de permisos, asegurando que los colaboradores sean autenticados a través de fuentes autoritativas y tengan acceso únicamente a los recursos específicos necesarios.

Gestión de ciberseguridad: Implementar mecanismos de seguridad en los aplicativos e infraestructura, que incluyan un inicio seguro, la evaluación de la existencia de código malicioso, análisis de vulnerabilidades y su solución.

10. ELABORACIÓN Y CONTROL DE CAMBIOS DEL DOCUMENTO

ELABORACIÓN			
Identificación		**Fecha**	**Gerencia**
Creador	Encargado de Ciberseguridad	24/06/2024	Gerencia de Tecnologías de la Información
Revisor	Gerente de TI	01/07/2024	Gerencia de Tecnologías de la Información
Revisor	Gerente de Auditoría y Contraloría	23/07/2024	Gerencia de Auditoría y Contraloría
Revisor	Gerente de Administración y Finanzas	31/07/2024	Gerencia de Administración y Finanzas
Aprobador	Gerente General		Gerencia General

CAMBIOS				
Revisión		**Elaborado por**	**Descripción del cambio**	**Aprobado por**
Versión	**Fecha**			
1.0		Encargado de Ciberseguridad	Creación de la política	