POLÍTICAS Y PROCEDIMIENTO DE INFORMACIÓN TECNOLÓGICA

Políticas de Contraseñas

Con la intención de establecer los lineamientos para crear, mantener y proteger efectivamente las contraseñas del Sistema de Harvey Gulf International Marine de Mexico (HGIMM). Esta política deberá ser aplicada a todos los empleados, contratistas y afiliados a HGIMM y deberán utilizar contraseñas aceptables para poder tener acceso a la Red de HGIM o almacenar datos de HGIMM.

Creación de Contraseñas

1. Todos los usuarios y contraseñas de los administradores deberán ser de al menos ocho (08) caracteres de longitud. Las contraseñas más largas o parafraseadas son altamente recomendables.
2. Cuando sea posible, se deberá utilizar un diccionario de contraseñas para prevenir el uso de contraseñas comunes y fáciles de adivinar.
3. Las contraseñas deberán ser completamente únicas y no deberán ser utilizadas por ningún otro sistema, aplicación o cuenta personal.
4. Las contraseñas asignadas automáticamente por el sistema deberán ser cambiadas inmediatamente después de haber concluido la instalación.

Tiempo de uso de Contraseñas

1. Las contraseñas de los usuarios deberán ser cambiadas cada tres (03) meses. Las contraseñas utilizadas previamente no deberán ser utilizadas nuevamente.
2. Contraseñas de Nivel del Sistema deberán ser cambiadas trimestralmente.

Protección de Contraseñas

1. Las contraseñas no deberán ser compartidas con nadie (incluyendo compañeros de trabajo y supervisores), y no deberán ser reveladas o enviadas electrónicamente.
2. Las contraseñas no deberán ser escritas o almacenadas físicamente en ningún lugar del interior de la oficina.
3. Las contraseñas no deberán ser almacenadas en algún formato no encriptado.
4. Los nombres de usuario y contraseñas no deberán ser guardadas de manera que tengan acceso automático.
5. Todos los objetivos móviles que se conecten a la red de la compañía deberán ser asegurados con una contraseña y/o con autenticación biométrica.

Si tú crees que tu contraseña pudo haber sido comprometida, por favor reporta inmediatamente el incidente al Departamento de Información Tecnológica y cambia la contraseña.

Compromiso

Es la responsabilidad del usuario final el asegurar el cumplimiento de las políticas descritas anteriormente.

Políticas de Acceso Remoto

Con la intención de definir las reglas y requerimientos concernientes a la conexión con la Red de HGIMM desde cualquier HOST (celulares, tabletas, laptops). Estas reglas y requerimientos fueron diseñadas para minimizar el riesgo potencial de daños en los cuales puedan resultar en el uso no autorizado de los recursos de la compañía. Esta política debe ser aplicable a todos los empleados, contratistas y afiliados a HGIMM y deberán contar con acceso remoto satisfactorio en todos los sistemas que se conecten con la Red de HGIMM o que tengan acceso a los datos almacenados de HGIMM.

General

Es la responsabilidad de los empleados de HGIMM, contratistas, vendedores y agentes con privilegios de acceso remoto a la red corporativa de HGIMM el asegurar que su conexión de acceso remoto es obtenida bajo las mismas consideraciones que las de uso en sitio.

El acceso a la red de HGIMM está estrictamente limitada a los empleados de HGIMM.

Contratistas, vendedores y agentes pueden tener acceso garantizado a la red solamente mediante aprobación previa.

Cuando se accede a la Red de HGIMM desde una computadora que no pertenece a HGIMM, los usuarios autorizados serán los responsables de prevenir el acceso a cualquier recurso de la empresa o datos por usuarios no autorizados.

Está prohibida la ejecución de actividades ilegales a través de la red de la compañía por cualquier usuario (Autorizado o de cualquiera otra índole). El usuario autorizado tiene la responsabilidad de y las consecuencias ocasionadas por el acceso de los Usuarios Autorizados.

Los Usuarios autorizados no deberán utilizar nuestra red para accesar a Internet por intereses o negocios externos. Para información adicional con respecto a las opciones de conexión mediante acceso remoto, incluyendo como obtener acceso remoto contraseña/VPN, programa antivirus, solución de problemas, etc., ver la Información Tecnológica del vicepresidente.

Procedimientos de Conexión.

- El acceso remoto Seguro será controlado estrictamente mediante encriptado a través de nuestra Red Privada (VPN) y contraseñas fuertes.
- Los Usuarios Autorizados deberán proteger su Usuario y contraseña, incluso de sus familiares.
- Cuando esté usando una de las computadoras de la compañía para conectarse a nuestra red corporativa, los Usuarios Autorizados deberán asegurarse de que el Puerto Remoto no está conectado a ninguna otra red al mismo tiempo, con la excepción de redes personales que estén bajo su completo control, de un Usuario Autorizado o de un Tercero.
- El uso de recursos externos para realizar actividades de la empresa deberá ser aprobado previamente por el Gerente de la Unidad.
- Todos los puertos que estén conectados a nuestra red interna mediante tecnología de acceso remoto deberán utilizar un programa de antivirus más actualizado.

Cumplimiento

El equipo técnico de la compañía verificará el cumplimiento de estas políticas mediante varios métodos, incluyendo mas no limitándose a, visitas periódicas, herramientas de reporte de negocios, auditorías internas y externas, y/o inspección. Los resultados de este monitoreo serán entregados al personal correspondiente.

Política de Red Privada Virtual (VPN)

Diseñada para proveer los lineamientos para las conexiones de la VPN con la Red corporativa y deberá ser aplicada a todos los empleados, contratistas y afiliados a HGIMM.

General

Es la responsabilidad de los empleados de la compañía, contratistas, vendedores y agentes con privilegios de acceso remoto a nuestra red corporativa de utilizar la conexión VPN adecuada.

Procedimientos de conexión

- Es la responsabilidad de los empleados con privilegios de VPN el asegurarse que usuarios no autorizados no tengan permitido el acceso a las redes interna de nuestra compañía utilizando su acceso.
- El uso de la VPN es controlado utilizando una llave del sistema privada o pública con una contraseña muy fuerte (Ver los detalles de la Política de Contraseñas).
- Las rutas de acceso a la VPN serán instalados y controlados por nuestro Departamento de Información Tecnológica.
- Todas las computadoras conectadas a nuestra red interna mediante VPN o cualquier otra tecnología deberán contar con la versión de antivirus más vigente de acuerdo con la normativa de la compañía; esto incluye computadoras personales.
- El concentrador VPN está limitado a un tiempo de conexión absoluto de 24 horas.
- Los usuarios propietarios de equipo no corporativo deberán configurar el equipo para cumplir con nuestras políticas de VPN y Red.
- Solamente los clientes aprobados por la compañía podrán utilizar la VPN.

Cumplimiento

El equipo técnico de la compañía verificará el cumplimiento de estas políticas mediante varios métodos, incluyendo mas no limitándose a, visitas periódicas, herramientas de reporte de negocios, auditorías internas y externas, y/o inspección. Los resultados de este monitoreo serán entregados al personal correspondiente.

Política de Privacidad y Protección de Datos

Debido al hecho de que HGIMM obtiene y utiliza datos sensibles para conducir sus operaciones de negocio, esta política provee los lineamientos en base a cuáles datos son sensibles, como deben ser protegidos y como pueden ser utilizados apropiadamente. Esta política debe ser aplicada a todos los empleados, contratistas y afiliados a HGIMM y todos los sistemas que conecten, tengan acceso a la red o que almacenen datos de la red de HGIMM.

General

- No se debe almacenar o retener Información Personal Identificable (IPI) más tiempo del necesario para realizar las operaciones de negocio. Nuestro equipo Técnico de Informática puede asistir en proveer la información de los esquemas o procedimientos de retención de datos.
- Resguardar la información durante la transmisión y almacenamiento de datos mediante el uso de métodos adecuados de encriptación como archivos protegidos por contraseña.
- La información confidencial y la IPI no deberá ser transmitida hacia/desde cuentas de correo no corporativas.
- No se debe revelar información confidencial o IPI sin la autorización apropiada para hacerlo;
- Utilizar solamente servicios de internet aprobados por la Compañía para almacenar Información Confidencial o IPI o para transferir dicha información;
- Cuando se mande un correo, se imprima o se envíe un fax, se deberá validar la lista de distribución y/o los detalles del destino antes de hacer el envío;
- No se deberá compartir información confidencial o IPI telefónicamente, se debe tener cuidado cuando se contesten preguntas de fuentes desconocidas mediante llamada telefónicas;
- Siempre se deberá confirmar que se está utilizando la impresora correcta;
- Retirar inmediatamente los documentos de la bandeja de salida cuando se utilicen impresoras públicas.

Política de Seguridad Física

Con la intención de establecer las reglas para garantizar, controlar, monitorear y remover los accesos físicos de las instalaciones de HGIMM y sus barcos, y se debe aplicar a todos sus empleados, contratistas y afiliados de HGIMM.

General

- Sistemas de seguridad física debe cumplir con todas las regulaciones aplicables incluyendo, pero no limitante a códigos de las instalaciones y códigos de prevención de incendios.
- El acceso físico a todas las instalaciones/barcos restringidos deberá ser documentada y controlada.
- Todas las instalaciones/barcos deberán ser protegidas físicamente en proporción de la importancia crítica de su función.

- El acceso a instalaciones/barcos restringidos deberá ser garantizado para dar apoyo al personal y contratistas quienes sus responsabilidades requieran acceso a dicha instalación.
- Todas las entradas a las instalaciones, cuando sea personas no autorizadas, deberán ser controlada.
- Las áreas seguras deberán ser protegida para reducir el riesgo de amenazas y riesgos ambientales, además de oportunidades para accesos no autorizados. Esto incluye:
    - Procesar información de instalaciones que manejen información confidencial debe ser colocada cuidadosamente para reducir el riesgo de que dicha información sea vista por personas no autorizadas durante su uso;
    - Se deben adaptar controles para minimizar el riesgo de potenciales amenazas físicas;
    - condiciones ambientales, tales como temperatura y humedad, deben ser monitoreadas para condiciones en las cuales pueda verse afectada la operación de las instalaciones de procesamiento.
- Directorios y agendas telefónicas internas que identifiquen las ubicaciones o información confidencial de instalaciones de procesamiento no deberán ser de fácil acceso para ninguna persona no autorizada.
- Los equipos deben ser protegidos de fallas de energía eléctrica u otras interrupciones causadas por fallas en las instalaciones.
- Los lugares y las ubicaciones restringidas no deberán tener señalamiento o evidencia de su importancia.
- Todas las instalaciones que permitan el acceso a visitantes deberán llevar un registro de su acceso mediante el registro de entrada y de salida.
- Las tarjetas de registro de acceso y los libros de registro de las instalaciones/embarcaciones deben mantener una rutina de revisión en base al nivel considerando en el nivel de la información que se está protegiendo.
- Las visitas a las áreas controladas de las instalaciones/embarcaciones debe ser acompañada de personal autorizado en todo momento.
- El personal responsable de manejar la seguridad de las instalaciones debe revisar los registros de acceso y los accesos de visitantes a las instalaciones periódicamente e investigar cualquier acceso inusual.

Tarjetas de Acceso

- Cada individuo que tenga derechos de acceso garantizado a una instalación deberá firmar el acceso apropiado y los acuerdos de confidencialidad.
- Las tarjetas de acceso y/o las llaves no deberán ser compartidas o encargadas a otras personas.
- Las tarjetas de acceso y/o las llaves que ya no sean requeridas deberán ser regresadas al personal responsable del manejo de la seguridad de las instalaciones. Las tarjetas no deberán ser reubicadas a ningún otro sitio sin haberse llevado a cabo el proceso de retorno.
- La pérdida o el robo de tarjetas y/o llaves deberá ser reportado a la persona responsable del manejo de la seguridad de la instalación tan pronto sea posible.

- Se deberán realizar revisiones periódicas de las tarjetas y/o llaves de acceso a la instalación y remover los accesos a las personas que ya no lo requieran más.

Cumplimiento

El equipo técnico de la compañía verificará el cumplimiento de estas políticas mediante varios métodos, incluyendo mas no limitándose a, visitas periódicas, herramientas de reporte de negocios, auditorías internas y externas, y/o inspección. Los resultados de este monitoreo serán entregados al personal correspondiente.

Uso de la Política de Correo Electrónico e Internet

Diseñado para minimizar el riesgo asociado con los servicios de Internet y correos electrónicos, y definir los controles en contra las amenazas de accesos no autorizados, robo de información, robo de servicios e interrupción maliciosa de servicios. Esta política aplica a todos los empleados, contratistas y afiliados a HGIMM.

Internet

- El internet no debe ser usado para comunicar información confidencial o interna, a menos que la confidencialidad y la integridad de la información sea asegurada y la identidad del receptor(es) sea establecida.
- El uso del Internet utilizando la Red de trabajo o equipos de cómputo de HGIMM deberá ser utilizado para actividades relacionadas con el trabajo. Las actividades no aprobadas, pero no limitadas a son las siguientes:
    - Juegos recreativos.
    - Medios de streaming.
    - Medios sociales personales.
    - Accesar o distribuir materiales pornográficos u orientados sexualmente.
    - Intentar o realizar accesos no autorizados a cualquier red o computadora desde el internet.
- Accesar al internet desde una red externa a la de HGIMM utilizando equipo de cómputo de HGIMM deberá apegarse a las mismas políticas que aplican a las instalaciones/barcos de HGIMM.

Correo electrónico

- Está prohibido auto reenviar correos electrónicos fuera de los sistemas internos de HGIMM.
- Las comunicaciones electrónicas no deberán dejar de representar al remitente o a HGIMM.
- El personal es responsable de las cuentas que les sean asignadas y de las acciones que sean realizadas en sus cuentas.
- Las cuentas no deberán ser compartidas con nadie previo a la autorización de HGIMM, con la excepción de calendarios o funciones relativas a calendarios.
- Los empleados no deberán utilizar cuentas de correo electrónico personales para enviar o recibir

información confidencial.

- Cualquier uso personal desde el correo provisto por HGIMM no deberá:
    - Promoción indebida.
    - Estar asociada con alguna entidad política.
    - Tenga el potencial de dañar la reputación de HGIMM.
    - Crear una cadena de correos electrónicos.
    - Contener o promover comportamiento antisocial o antiético.
    - Violar las leyes o regulaciones locales, estatales, federales o internacionales.
    - Resultar en una fuga de información confidencial de HGIMM.

- El personal deberá tener precaución cuando responda a, dando clic en links dentro de, o abrir archivos adjuntos dentro de las comunicaciones electrónicas.
- El personal deberá ser discreto con el uso de información confidencial o interna dentro o fuera de la oficina u otra respuesta automática, tal como datos de empleados, números telefónicos internos, información de ubicación u otro dato importante.
- Si sospecha de algún correo electrónico, contacte al Departamento de Información Tecnológica de forma inmediata.
- En cualquier momento y sin previo aviso, HGIMM se reserva el derecho de examinar la Cuenta de Correo electrónico, carpetas de archivos personales y cualquier otra información almacenada en las computadoras. Esta examinación es para asegurar el cumplimiento con las políticas de la compañía, dar soporte al desempeño de investigaciones internas, y asistir con el manejo de los Sistemas de Información de HGIMM.

Política de Acceso

El acceso a sistemas críticos, aplicaciones y servicios puede proveer información importante e indicadores potenciales de incumplimientos (comprometedores). Aun cuando la información de acceso no sea vista periódicamente, es crítico tener un punto de inicio forense. El propósito de este documento es el de contener el propósito identificando los requerimientos específicos que los sistemas de información deben cumplir con el fin de generar los registros adecuados de auditoría. Esta política aplica a todos los sistemas de la red propiedad y operada por HGIMM.

General

- Todos los sistemas que contengan información confidencial, acepten conexiones a la red, o tengan decisión sobre el control de acceso (autenticación o autorización) deberán registrar y retener la suficiente información auditable de acceso para responder las siguientes preguntas:
    - ¿Cuál actividad se está desarrollando?
    - ¿Quién o qué desarrollo la actividad, incluyendo donde o con cual sistema fue desarrollada la actividad (subjetivo)?
    - ¿Cuándo fue desarrollada la actividad?

- Por tal motivo, los registros deberán ser creados cuando cualquiera de las siguientes actividades sea solicitado para ser desarrolladas por el Sistema:
    - Crear, leer, actualizar o borrar información confidencial, incluyendo la autenticación de información confidencial como contraseñas;
    - Iniciar una conexión con la red;
    - Acepar la conexión con la red;
    - Autenticación o autorización de usuario para realizar las actividades descritas en los puntos No. 1 y No. 2 tal como entrar y salir la cesión del usuario.
    - Cambios en la configuración del sistema, red, o servicios, incluyendo la instalación de programas, actualizaciones y parches, u otro cambio en los programas instalados.
    - Iniciar, apagar o reiniciar los procesos de aplicaciones;
    - Detectar cualquier actividad sospechosa/maliciosa tal como la Detección de un intruso Sistemas de Prevención (IDS/IPS), sistemas antivirus o cualquier sistema anti-softwares espía.

MANEJO DE RIESGOS DE CIBER SEGURIDAD

El manejo de Ciber riesgos es el proceso de identificar, analizar, asesorar y comunicar el ciber-riesgo relacionado a la compañía; aceptando, evitando, transfiriendo o mitigándolo a un nivel aceptable, mientras se consideran todos los costos y beneficios de las acciones realizadas por los perpetradores.

Propósito

El propósito del Manejo de Riesgos de Ciberseguridad es el proveer las prácticas de trabajo seguro relacionadas con la ciberseguridad para las operaciones del barco y para un ambiente de trabajo seguro; asesorar en todos los ciber riesgos a sus barcos, personal y al ambiente y establecer las medidas de prevención apropiadas; para continuar mejorando las habilidades para el manejo de la seguridad el personal en tierra y a bordo de los barcos; incluyendo la preparación para las ciber emergencias; y para asegurar la seguridad en la mar, prevenir algún daño humano o pérdida de vidas y evitar el daño a la propiedad y al medio ambiente.

Una de las políticas de HGIMM es la de proveer los recursos necesarios para mantener una transportación marítima sana y segura la cual es resiliente operacionalmente a ciber riesgos. El manejo y los empleados de HGIM están comprometidos con mejorar continuamente su capacidad en las operaciones, mientras que aseguran que todos los riesgos de ciber ataques son evaluados y se tomas las medidas para mitigarlos.

El Manejo de Ciber riesgos comienza con el manejo nivel senior. HGIMM posee una cultura de prevención de ciber ataques en todos sus niveles de organización y asegura un régimen holístico y flexible que está en continua operación y constantemente evalúa que sus mecanismos sean efectivos.

Propiedad

Los requerimientos del Sistema de Manejo de la Seguridad incluyen por todas las leyes y regulaciones aplicables. El Departamento de Información Tecnológica es responsable de asegurar el cumplimiento con las reglas y regulaciones mandatarias relativas a la ciber seguridad, incluyendo la Resolución OMI MSC.428(98) y todos los códigos aplicables, lineamientos y estándares recomendados por la Organización, la Administración, Casas Clasificadoras y Organizaciones de la Industria Marítima serán tomadas en cuenta.
El Capitán del barco tiene muchas responsabilidades relativas a la ciber seguridad, incluyendo
The Master of the vessel has many responsibilities relating to cyber security, including:

- Implementar las políticas de Ciber seguridad de la Compañía a bordo del buque incluyendo las cuales el Capitán utiliza actualmente.
- Se debe asegurar que todo el personal a bordo del barco tenga un buen conocimiento y haya leído y entendido todas las políticas y procedimientos de ciber seguridad.
- Verificar que todos los requerimientos de ciber seguridad son realizados a bordo.
- Revisar periódicamente las políticas y procedimientos de la compañía y reportar cualquier deficiencia a las instalaciones en tierra inmediatamente.

- El Capitán deberá contar con la Autoridad y Responsabilidad para tomar decisiones con respecto a las actividades de ciber seguridad a bordo de los barcos de la compañía y podrá solicitar asistencia de la compañía cuando sea necesario.

- Es la responsabilidad del Capitán tener completa participación en las Políticas y Procedimientos de Ciber seguridad de HGIMM. La Compañía proveerá recursos necesarios para lograr este objetivo.

El vicepresidente de Información Tecnológica tiene la última responsabilidad del manejo de los riesgos de ciber seguridad, incluyendo conducir la asesoría de Ciber Riesgos. HGIMM utiliza la "Tabla de Evaluación de Ciber Riesgos" (Ver el Documento de "Evaluación de Ciber Riesgos") para:

- Identificar: Identificar los sistemas, datos y capacidades que, cuando son interrumpidos representan un riesgo a las operaciones del barco. (Ver columna "Vulnerabilidades del Sistema" en la Tabla de Evaluación de Ciber Riesgos).
- *Proteger: Implementar los procesos y medidas de control de riesgos, planear la protección contra un evento de ciber seguridad y asegurar la continuidad de las operaciones de los barcos. (Ver la Columna "Medidas de Protección y Detección" y "Plan de Contingencia" en la Tabla de Evaluación de Ciber Riesgos).*
- *Detectar: Desarrollar e implementar las actividades necesarias para detectar un ciber evento de forma adecuada. (Ver la columna "Medidas de Protección y Detección" en la Tabla de Evaluación de Ciber Riesgos).*
- *Responder: Desarrollar e implementar actividades y planes que provean resiliencia y que restablezcan los sistemas necesarios para las operaciones de los barcos o para los servicios dañados debido a un ciber evento. (Ver la columna "Respuesta y Recuperación" en la Tabla de Evaluación de Ciber Riesgos).*
- Recuperación: Identificar las medidas de respaldo y restauración los ciber sistemas necesarios para las operaciones de los barcos comprometidos por un ciber evento. 8Ver la Columna "Respuesta y Recuperación" en la Tabla de Evaluación de Ciber Riesgos).

Sistemas, amenazas y vulnerabilidades

La diferencia entre Sistemas de Información Tecnológica (IT) y Sistemas de Tecnología Operativa (TO) son considerables. Los Sistemas de Información Tecnológica son aquellos que están focalizados en el uso de datos como información. Los Sistemas de Operación Tecnológica son los que están focalizados en el uso de datos para controlar y monitorear procesos físicamente.

- Esta política y lineamientos de soporte contienen todos los recursos del sistema (IT y TO) que son propiedad, operados, mantenidos y controlados por HGIMM y todos los demás recursos de sistemas, tanto internos como externos, que interactúan con estos sistemas.
- Los sistemas y tecnología de HGIMM provee beneficios significativos de eficiencia, pero también presentan un riesgo que puede ser crítico para los sistemas y procesos conectados a estos sistemas. Estos riesgos pueden resultar desde vulnerabilidades originadas por operación inadecuada, integración,

mantenimiento y diseño de sistemas ciber-relacionados y desde amenazas intencionadas e inintencionadas.

- Las amenazas se presentan mediante acciones maliciosas (ej., hackeo o introducción de virus) o como consecuencias de acciones inintencionadas (ej., mantenimiento de software o permisos de usuarios). Típicamente, estas acciones exponen las vulnerabilidades tecnológicas operacionales y de información.
- Estas vulnerabilidades pueden ser resultado de fallas en el diseño, integración y/o mantenimiento de sistemas, así como fugas en la ciber seguridad. En general, cuando las vulnerabilidades en la IT o TO son expuestas o detectadas, ya sea directamente (ej., contraseñas débiles que conducen a accesos no autorizados) y de confidencialidad, integridad y de información disponible. Adicionalmente, puede haber implicaciones de seguridad, particularmente cuando los sistemas críticos (ej., puente de mando o en el sistema de propulsión principal) son comprometidos.

Impacto Potencial

La compañía identifica los impactos de seguridad resultante de la exposición o la detección de las vulnerabilidades de los Sistemas de Información Tecnológica (IT) en la Tabla de Evaluación de Riesgos de Ciber seguridad (Seguridad Potencial/Impactos a la Seguridad). Esto puede ser resultado de una conexión inadecuada de los sistemas tecnológicos operacionales o de fisuras en procedimientos realizadas por el personal o por terceros, las cuales pueden comprometer estos sistemas.

Este procedimiento es diseñado para guiar a los empleados de HGIMM con respecto a las políticas/lineamientos de ciber seguridad y cuando la información relacionada con ellos no es encontrada. Las políticas/lineamientos a continuación definen el rol y las responsabilidades del personal para el manejo de los ciber riesgos, implementando procesos de control de riesgos y medidas de protección en caso de un ciber evento, implementando planes para proveer resistencia e identificar las medidas para respaldar o restaurar la información afectada en los ciber sistemas.

La Tabla de Evaluación de Ciber Seguridad es utilizad para ejecutar una evaluación de riesgos en todos los sistemas identificados, equipos, datos y capacidades. Esta evaluación fue desarrollada para promover la confiabilidad en la tecnología critica operacional (OT) y en la información tecnológica (IT).

Los Riesgos son clasificados como altos (rojo), medio (naranja) y bajos (verde). La posibilidad que exista un ciber ataque/falla es desglosado en rangos de nada probable, improbable, posible, probable y muy probable. Finalmente, la severidad de los ataques/fallas se clasifica en muy baja, menor, severa y mayor.

Rango	Descripción
Altamente improbable	Altamente improbable que la vulnerabilidad sea detectada
Improbable	Improbable que la vulnerabilidad sea detectada
Posible	Posiblemente la vulnerabilidad sea detectada
Probable	Probablemente la vulnerabilidad sea detectada
Muy Probable	Muy probablemente la vulnerabilidad sea detectada

Rango	Descripción
Muy baja	Hay una muy baja posibilidad que una falla ponga en riesgo las operaciones del barco.
Menor	Hay una posibilidad menor que una falla ponga en riesgo las operaciones del barco.
Severa	Hay una posibilidad muy alta que una falla ponga en riesgo las operaciones del barco.
Mayor	Hay una posibilidad mayor que una falla ponga en riesgo las operaciones del barco.

Nada probable	**5**	**10**	**15**	**20**
Probable	**4**	**8**	**12**	**16**
Posible	**3**	**6**	**9**	**12**
Poco probable	**2**	**4**	**6**	**8**
Muy probable	**1**	**2**	**3**	**4**
	Muy bajo	**Menor**	**Severo**	**Mayor**

TABLA DE EVALUACIÓN DE RIESGOS DE CIBER SEGURIDAD							
Sistema Vulnerable	**Potencial de Impacto en la Seguridad/Seguridad**	**Medidas de Protección y Detección**	**Respuesta y Recuperación**	**Plan de Contingencia**	**Similitud**	**Severidad**	**Rango Total de Riesgo**
Red de Oficinas de HGIM							
Red de Barcos de HGIM							
Cartas de Navegación Electrónicas/ECDIS							
Estación de Trabajo Puente/Máquinas							
Correo Electrónico Servidor/Bandejas de Correo							
Radar							
AIS							
Compás							
Girocompás							
Piloto automático							
Sistema de Posición Dinámico							
Computadora de Automatización							
Autopiloto							

Recursos y Soporte

HGIMM asegura los recursos adecuados y que el soporte desde tierra será provisto para permitir que los empleados designados, incluyendo el Capitán, realice sus funciones con respecto a la ciberseguridad. El vicepresidente de Información Tecnológica es el designado para proveer una conexión directa entre el Barco y el personal de las instalaciones en Tierra en temas relacionados con la Ciber Seguridad. El vicepresidente de Información Tecnológica tiene el acceso a los recursos necesarios así como a los más altos niveles de Administración de HGIMM.

Simulacros y entrenamiento

Los simulacros de ciber seguridad son realizados para ayudar a la compañía a identificar los puntos débiles y preparar al personal para un ciber evento. HGIMM realiza los simulacros de ciber seguridad de acuerdo con el criterio del Capitán de cada barco. Cada uno de los simulacros de ciber seguridad deberá ser registrado y se deberá elaborar un reporte; dependiendo del tipo de simulacro, el reporte podrá ser escrito o verbal. Todas las lecciones aprendidas deberán ser compartidas con los empleados a los que sea aplicable. La Tabla de Evaluación de Riesgos de Ciber Seguridad y los lineamientos/políticas deberán ser actualizadas por el vicepresidente de Información Tecnológica si es necesario. Los simulacros de ciber seguridad pueden consistir en, pero no están limitados a:

- Hackeo
- Ataques
- Archivos adjuntos maliciosos
- Virus
- Solicitud de Contraseñas
- Usuarios o Equipos No Autorizados

Nota: Los simulacros de ciber seguridad podrán o no ser realizados por una tercería.

Reporte

En el caso de que ocurra un ciber incidente/evento, el Departamento de Información Tecnológica y la Gerencia es el responsable de investigar, analizar, incluir medidas para prevenir su recurrencia. Todos los incidentes de ciber seguridad deberán ser registrados.

Si después a la investigación, aún se sospecha de alguna falla, el Departamento de Información Tecnológica y la Gerencia es el responsable de establecer la causa y el impacto, así como las acciones correctivas, incluyendo las medidas para prevenir su recurrencia. La Tabla de Evaluación de Riesgos a la Ciber Seguridad y los procedimientos aplicables deberán ser actualizados se es requerido para prevenir que un riesgo similar pueda ocurrir nuevamente.

> *Nota: El Personal de Información Tecnológica y/o la Gerencia puede ser localizado en tierra en cualquier momento, incluyendo fines de semana y horas de descanso al número 938-1414-250.*
>
> *Nota: Se puede recurrir a una Compañía Tercería dependiendo de la severidad del ciber incidente/evento.*

Verificación

El proceso de auditoría interna es un proceso que será llevado a cabo por el departamento de Información Tecnológica y/o de operaciones de HGIMM. Las auditorías internas son realizadas en tierra y a bordo en intervalos que no excedan los 12 meses. El proposito de estas auditorías es:

- Verificar que todo el personal que sea designado a actividades relacionadas con el ISM actúe en conformidad con las responsabilidades de la Compañía.
- Verificar que las actividades de ciber seguridad son efectivas.
- Verificar que la Tabla de Evaluación de la Ciber Seguridad está actualizada.
- Evaluar y comparar los procedimientos actuales y los objetivos de manejo de ciber riesgos por parte de HGIMM.
- Revelar las fallas que pueden ser resueltas para alcanzar los objetivos del manejo de la ciber seguridad.

Hasta la complementación de las auditorias, los resultados serán reportados al vicepresidente Ejecutivo de QHSSE/HR. Es la responsabilidad del Departamento de Información Tecnológica de HGIMM establecer las acciones correctivas, un programa para completar dichas acciones correctivas y a la persona/departamento responsable. Los resultados de las auditorias/revisiones internas deberán ser mostrados a todo el personal que tenga alguna responsabilidad en el área involucrada. Es responsabilidad del personal a cargo del área asegurarse que las acciones correctivas se están realizando para todas las deficiencias encontradas de forma oportuna.

La Ciber Seguridad es revisada anualmente como parte de la Política de Ciber Seguridad de la Compañía.

La revisión anual ayuda a HGIMM a desarrollar una estrategia, basada en la evidencia de la auditoria, para actualizar el plan de manejo de Ciber Seguridad, la Tabla de Evaluación de Ciber Riesgos y/o las políticas/procedimientos aplicables. La revisión es utilizada como una herramienta para ayudar a la compañía a utilizar en mejor forma y efectivamente sus recursos.