

24 Mayo 2018

Ciberataque deja
sin acceso a
13 millones
clientes



PULSO

Virus en Banco de Chile fue un distractivo para robarle US\$10 millones

El gerente general de la entidad financiera revela que el ciberataque del que fue objeto la institución a fines de mayo estuvo "destinado a dañar al banco, no a los clientes". Los autores serían una banda de Europa del Este o de Asia. 4-5

PULSO

Empresas & Mercados

Firmas

...

Cibercriminales filtran datos de 14 mil tarjetas de crédito. Regulador y firmas toman medidas

Pese a que ayer se filtró una base de datos de unos 14.000 clientes, la mayoría de las cuentas estarían vencidas y solo el 10% de las tarjetas afectadas se encontrarían vigentes.

Mariana Marusic 25 JUL 2018 09:27 PM Tiempo de lectura: 4 minutos



El 80% del comercio internacional se desplaza por mares y océanos.

MARCO LEGAL ASOCIADO A LA CIBERSEGURIDAD EN LA OPERACIÓN DE LAS AtoN

La experiencia chilena

James Crawford

Ingeniero en Administración Marítima

MSC Asuntos Marítimos - WMU Suecia

Temario:

- Introducción.
- La respuesta regulatoria marítima.
- Conclusiones.

Informaciones:

GASTO MUNDIAL EN CIBERSEGURIDAD

144.000
millones de euros
en **2019**

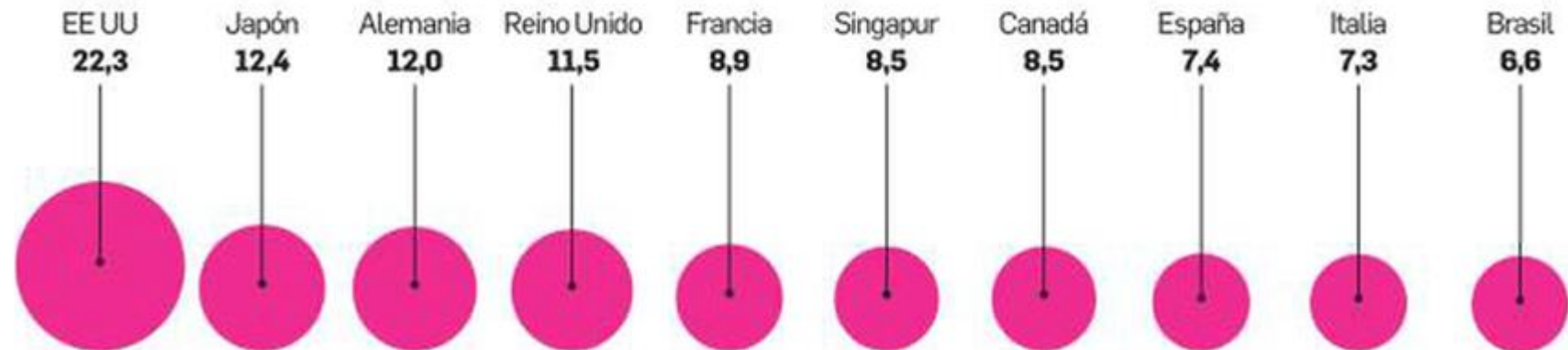
131.000
millones de euros
en **2018**

119.000
millones de euros
en **2017**

Un 77,6% de todos los ataques

QUE SE PRODUCEN EN EL MUNDO ESTÁN DIRIGIDOS A EMPRESAS, MIENTRAS QUE LOS PARTICULARES RECIBEN UN 22,4% DEL TOTAL.

COSTE MEDIO ANUAL DE LOS CIBERATAQUES EN GRANDES EMPRESAS POR PAÍS (MILLONES DE EUROS)



Introducción.

Introducción:



Sistemas operativos.

Desfasados e incompatibles con nuevas medidas de seguridad.

Alta rotación de tripulaciones.

Dificultan la disciplina informática.

Conectividad.

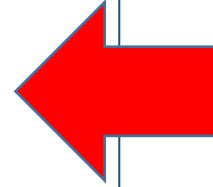
Entre sistemas de abordo y los terrestres.

Introducción:

ANEXO 10

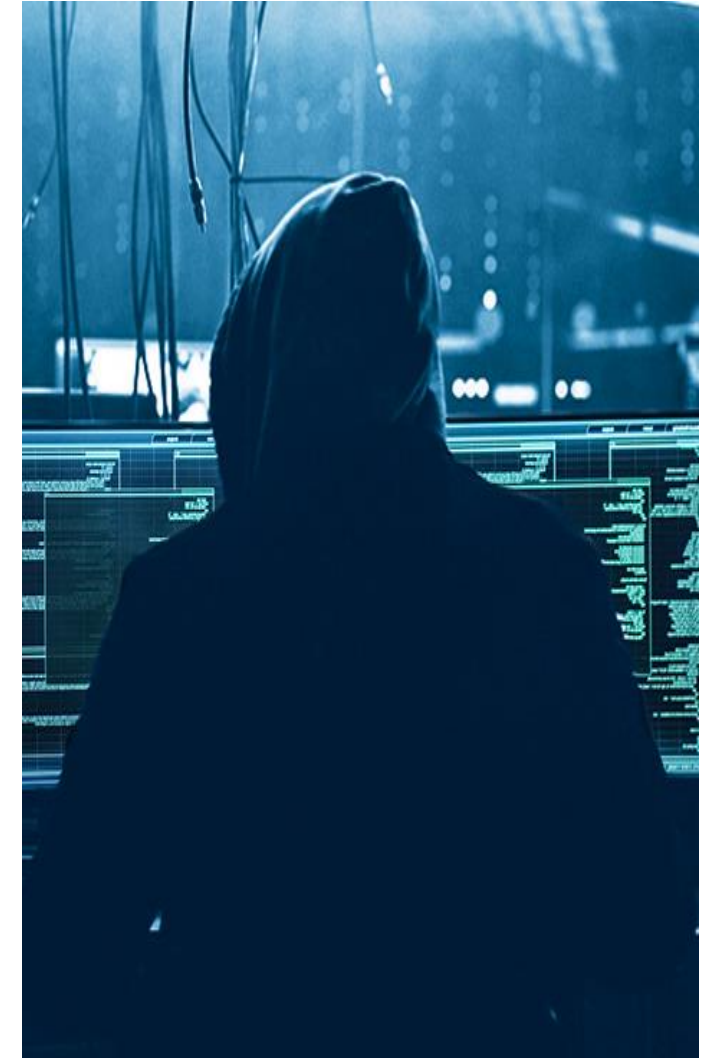
RESOLUCIÓN MSC.428(98)
(adoptada el 16 de junio de 2017)

GESTIÓN DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD



TOMANDO NOTA de los objetivos del Código IGS, entre los que se incluye establecer prácticas de seguridad en las operaciones del buque y en el medio de trabajo; evaluar todos los riesgos señalados para los buques, el personal y el medio ambiente; tomar las oportunas precauciones, y mejorar continuamente los conocimientos prácticos del personal de tierra y de a bordo sobre gestión de la seguridad,

- 1 AFIRMA que todo sistema de gestión de la seguridad aprobado debería tener en cuenta la gestión de los riesgos cibernéticos, de conformidad con los objetivos y prescripciones funcionales del Código IGS;
- 2 ALIENTA a las Administraciones a garantizar que los riesgos cibernéticos se abordan debidamente en los sistemas de gestión de la seguridad a más tardar en la primera verificación anual del documento de cumplimiento de la compañía después del 1 de enero de 2021;
- 3 RECONOCE que podrían ser necesarias precauciones para preservar la confidencialidad de algunos aspectos de la gestión de los riesgos cibernéticos;
- 4 PIDE a los Estados Miembros que pongan la presente resolución en conocimiento de todas las partes interesadas.



Introducción:

ANEXO 10

RESOLUCIÓN MSC.428(98)
(adoptada el 16 de junio de 2017)

GESTIÓN DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS EN LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD

TOMANDO NOTA de los objetivos del Código IGS, entre los que se incluye establecer prácticas de seguridad en las operaciones del buque y en el medio de trabajo; evaluar todos los riesgos señalados para los buques, el personal y el medio ambiente; tomar las oportunas precauciones, y mejorar continuamente los conocimientos prácticos del personal de tierra y de a bordo sobre gestión de la seguridad,

- 1 AFIRMA que todo sistema de gestión de la seguridad aprobado debería tener en cuenta la gestión de los riesgos cibernéticos, de conformidad con los objetivos y prescripciones funcionales del Código IGS;
- 2 ALIENTA a las Administraciones a garantizar que los riesgos cibernéticos se abordan debidamente en los sistemas de gestión de la seguridad a más tardar en la primera verificación anual del documento de cumplimiento de la compañía después del 1 de enero de 2021;
- 3 RECONOCE que podrían ser necesarias precauciones para preservar la confidencialidad de algunos aspectos de la gestión de los riesgos cibernéticos;
- 4 PIDE a los Estados Miembros que pongan la presente resolución en conocimiento de todas las partes interesadas.

RESOLUCIÓN MSC 428(98)
Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad.

Todo sistema IGS debería considerar los riesgos cibernéticos.

Se alienta a las administraciones a garantizar que los riesgos cibernéticos son abordados en los sistemas IGS a contar del 1º enero 2021.

Introducción:

MSC-FAL.1/Circ.3 – 5 julio 2017 Directrices sobre la gestión de los Riesgos Cibernéticos Marinos



- ✓ Aprueban las directrices contenidas.
- ✓ Directrices facilitan **recomendaciones de alto nivel** sobre la gestión de riesgos cibernéticos marítimos.
- ✓ **Elementos funcionales** que contribuyen a la gestión efectiva de los riesgos cibernéticos marítimos:
 - Identificación;
 - Protección;
 - Detección;
 - Respuesta;
 - Recuperación.

Introducción:



Guía de la IALA n.º 1081 sobre las Ayudas virtuales a la navegación

- ✓ Vulnerabilidad del Sistema Global de Navegación por Satélite (GNSS).
- ✓ Vulnerabilidad de las ayudas virtuales a la navegación; interferencia / falsificación.

La respuesta regulatoria marítima.

La respuesta regulatoria marítima:

OBJ.: Establece disposiciones relativas a la implementación de medidas de seguridad y protección marítima por parte de Buques, Instalaciones Portuarias y **Ayudas a la Navegación** en el marco de la gestión de riesgos cibernéticos marítimos.

D.G.T.M. Y M.M.

APRUEBA CIRC
DEL TERRITORIO
MERCANTE, OR

VALPARAÍSO,

VISTO: los Decretos (MINREL) N°384 y N°71, ambos de 2005, que promulgaron las enmiendas al Convenio Internacional para la Seguridad de la Vida Humana en el Mar, SOLAS 1974, adoptadas por el Comité de Seguridad Marítima de la Organización Marítima Internacional sobre la implantación del Código Internacional de gestión de la seguridad (IGS) y sobre el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias PBIP; los artículos 3º y 4º del D.F.L. (H) N° 292, de 1953, que aprueba la Ley Orgánica de la Dirección General del Territorio Marítimo y de Marina Mercante; lo dispuesto en los artículos 5º, 29º, 88º y 91º del D.L. (M) N° 2.222, de 1978, que sustituye la Ley de Navegación; lo dispuesto en el Decreto Ley N° 3.607 de 1.981, artículo 3º; la resolución MSC 428 (98) sobre "Gestión de los riesgos cibernéticos marítimos en los sistemas de gestión de la seguridad" (Comité de seguridad Marítima (MSC) OMI, 2017); la resolución MSC-FAL.1/Circ.3, sobre directrices para "La Gestión de los Riesgos Cibernéticos Marítimos" (Comité de Seguridad Marítima (MSC) - Comité de Facilitación (FAL) OMI, jul 2017), y las facultades del artículo 345º del D.S. (M) N°1340 bis, de 1941,

RESUELVO:

- 1.- **APRUEBASE** la siguiente circular que establece disposiciones relativas a la implementación de medidas de seguridad y protección marítima por parte de Buques, Instalaciones Portuarias y Ayudas a la Navegación en el marco de la gestión de riesgos cibernéticos marítimos.

CIRCULAR D.G.T.M. Y M.M. ORDINARIO N° O-XX/XXX

OBJ.: Establece disposiciones relativas a la implementación de medidas de seguridad y protección marítima por parte de Buques, Instalaciones Portuarias y Ayudas a la Navegación en el marco de la gestión de riesgos cibernéticos marítimos.

1

ORIGINAL

- I.- Informaciones.
- II.- Ámbito de aplicación.
- III.- Instrucciones.
 - A.- Generales.
 - B.- Compañías y buques.
 - C.- Inst. portuarias.
- IV.- Vigencia.
- V.- Anexos.

La respuesta regulatoria marítima:

I.- Informaciones.

- ✓ **Ley de Navegación**, Art. 5 que establece que “la Autoridad Marítima aplicará y fiscalizará los conv. internacionales”.
- ✓ **Decreto Ley** que establece que las Empresas Estratégicas deben contar con un estudio de seguridad.
- ✓ **SOLAS**, Cap. IX “Gestión de la Seguridad Operacional de los Buques” y el XI-2 “Medidas Especiales para Incrementar la Protección Marítima”.
- ✓ El Código **PBIP**.

La respuesta regulatoria marítima:

I.- Informaciones (cont.).

- ✓ Definición de riesgo cibernético.

RIESGO = PROBABILIDAD X IMPACTO

- ✓ Establece la importancia de la gestión de los riesgos cibernéticos es **fundamental para la seguridad y la protección de las operaciones del transporte marítimo.**

La respuesta regulatoria marítima:

II.- Ámbito de aplicación.

- ✓ Buques de tráfico internacional (Código IGS y PBIP).
- ✓ Buques de pasaje, transbordo rodado y trasiego de combustible bunker.
- ✓ Buques que realicen viajes al territorio antártico.
- ✓ Compañías que cumplan con el Código IGS.
- ✓ Inst. Portuarias (Código PBIP) y empresas estratégicas.
- ✓ **AtoN electrónicas particulares y estaciones VTS.**

La respuesta chilena:

III.- Instrucciones.



Generales



Compañías y
buques



Instalaciones
portuarias
(**AtoN**)

La respuesta chilena:

III.- Instrucciones Generales.



Generales
(aplicable a AtoN)

- ✓ Salvaguardar el transporte marítimo de amenazas actuales y emergentes.
- ✓ Incorporar **Sistema de Gestión de Riesgos Cibernéticos** conforme normas ISO.
- ✓ Identificar y analizar posibles **fuentes de amenazas y/o vulnerabilidades**.
- ✓ Designar **responsable GRC**.

La respuesta chilena:

III.- Instrucciones Generales (cont.).



**Compañías y
buques**

Sistema GRC de los sistemas vulnerables o sensibles, tales como:

- ✓ de puente;
- ✓ manipulación y gestión carga;
- ✓ propulsión y gestión máquinas y control suministros eléctricos;
- ✓ servicio / organización pasajeros;
- ✓ comunicaciones, etc.

La respuesta chilena:

III.- Instrucciones Generales (cont.).



Instalaciones
portuarias
(**considera AtoN**)

Sistema GRC de los sistemas vulnerables o sensibles, tales como:

- ✓ sistemas de control de acceso;
- ✓ servicios / organización pasajeros;
- ✓ sistemas de comunicaciones;
- ✓ sistemas de manipulación de carga;
- ✓ **ayudas a la navegación electrónicas y estaciones VTS.**

Conclusiones.

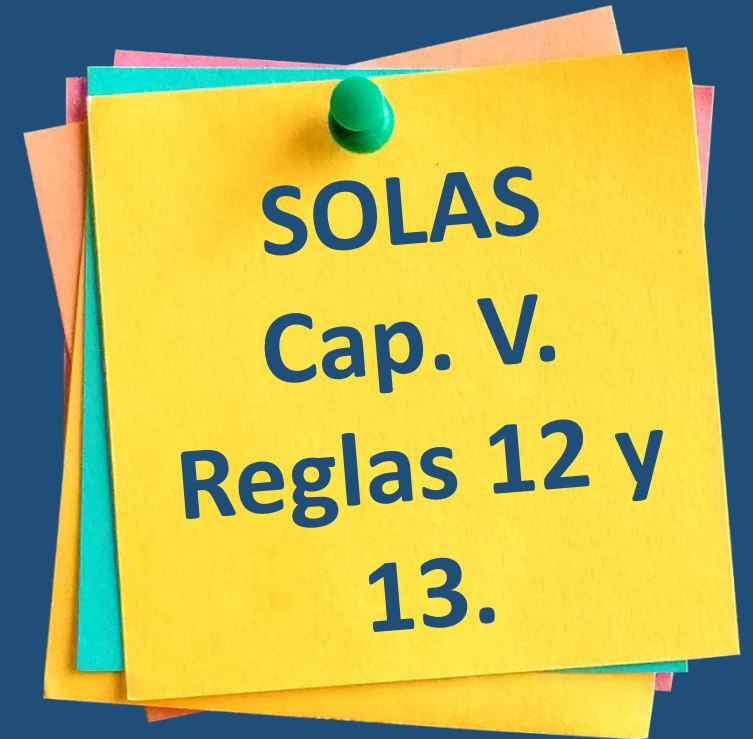
Conclusiones:

Las ciberamenazas a las ayudas a la navegación son factibles y reales.



Conclusiones:

La adopción de medidas de protección es **necesaria y exigida** por la Organización Marítima Internacional y **recomendada** por IALA.



MARCO LEGAL ASOCIADO A LA CIBERSEGURIDAD EN LA OPERACIÓN DE LAS AtoN

James Crawford

jamcrawf@icloud.com