III Conferencia Hemisférica sobre Seguridad Portuaria

Mayor eficiencia mediante operaciones seguras

Amenaza global – Respuesta nacional – Seguridad cibernética en puertos

Mto. Cap.Alt. Miguel Ángel Osuna Rodríguez

Red PBIP México - Internacional

Contenido.

- Datos general
  - Telecomunicaciones
  - Puertos e instalaciones portuarias
  - Movimiento de carga en puertos
- Problemática
- Principales acciones tomadas (herramientas normativas)

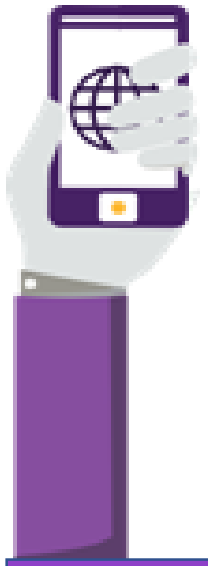
OEA
Mais direitos para mais pessoas

CIP
Comisión Interamericana de Puertos

- Entorno Ciber portuario en México
  - Telecomunicaciones
  - Puertos e instalaciones portuarias
  - Movimiento de carga en puertos

LAS TECNOLOGÍAS DE LA INFORMACIÓN SON CADA VEZ MÁS IMPORTANTES

300 millones de dispositivos conectados para 2025 – en México



El crecimiento de 70% de dispositivos para el 2025 requerirá un crecimiento de más de 300% del poder computacional de centros de datos

Más del 94% de este poder computacional estará en la nube

PERO PRESENTAN CADA VEZ MÁS RIESGOS:

En México, más de 33 millones de personas fueron afectadas por el cibercrimen en 2017

PARA 2019 SE ESTIMAN PÉRDIDAS POR CIBERATAQUES DE HASTA 2 BILLONES DE DOLAREA A NIVEL MUNDIAL

Ciberataque ⚠ **Intento no autorizado por la vía digital de acceder a un sistema de control**, dispositivo electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones

Se estima que el costo total anual del delito cibernético en la economía mundial sobrepase los **$2 billones de USD** para **2019**

Estimaciones de **costo** financiero y **consumidores** afectados en **2017**:

El costo financiero total del cibercrimen para consumidores globales fue de

$172 miles de millones de USD

El costo financiero del cibercrimen para consumidores mexicanos fue de

$7.7 miles de millones de USD

Los consumidores globales afectados por el ciberdelito en 2017 fueron **978** millones

Los consumidores **mexicanos** afectados por el ciberdelito en 2017 fueron **33** millones

FUENTE: Norton Cyber Security Insights "2017 Norton Cyber Security Insights Report" (encuesta en línea de ~25.5 mil participantes en 2017 en 20 países, considera robo de identidad, fraude de tarjetas y robo de contraseña, entre otros); Juniper Research "The Future of Cybercrime & Security 2017" (considera multas, costos de remediación y costos de oportunidad, entre otros)

Puertos de México

OEA

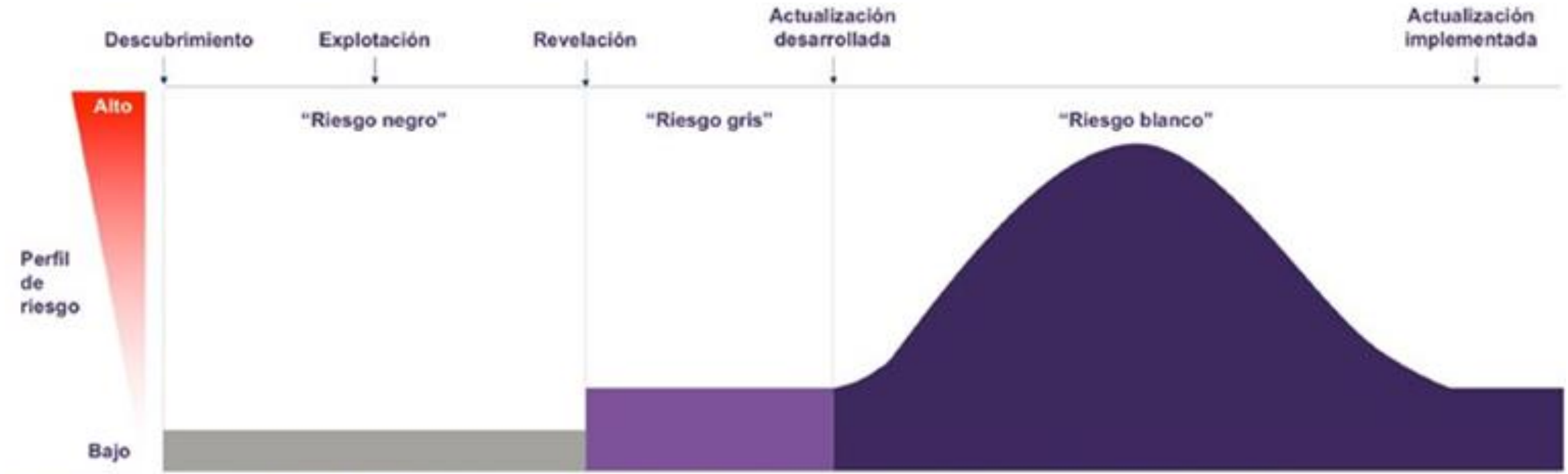
Mais direitos para mais pessoa

CIP

Comisión
ramericana de Pue

Problemática

El ciclo de vida de un ciberataque sistémico



Descripción

- Sólo un **grupo limitado** (p. ej., grupos de ciberespionaje, delincuencia organizada) están **conscientes del riesgo**
- El público, las instituciones y los proveedores del programa vulnerable generalmente no tienen **conocimiento del riesgo**

- El **riesgo se vuelve conocimiento público**, sin embargo, no se ha desarrollado ninguna solución
- Se utilizan **otros mecanismos/ procedimientos de seguridad** hasta que se publique una actualización de sistema

- La **exposición aumenta significativamente** después de la publicación de la actualización de sistema
  - **La actualización contiene información del código fuente** que ahora está disponible para más atacantes potenciales
  - **Se intensifican los ataques** sobre los sistemas no actualizados
- **Riesgo incrementa** mientras las organizaciones se **demoran** en actualizar sus sistemas
- Riesgo se reduce cuando la mayoría de las organizaciones instalan la actualización

FUENTE: ETH Zurich, Delta Risk, McKinsey

: Autoridades de respuesta a ciberataques

Autoridad	Mandato
Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas adscrita a la Agencia de Investigación Criminal	▪ Instancia de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyen las investigaciones relacionadas con medios electrónicos y tecnológicos bajo la conducción y mando del Ministerio Público de la Federación.
Policía Federal, a través, de su División Científica, auxiliada, entre otras, por: ▪ Coordinación para la Prevención de Delitos Electrónicos ▪ Dirección General de Prevención de Delitos Cibernéticos ▪ Dirección General del Centro Especializado en Respuesta Tecnológica ▪ Dirección General de Tecnologías de Información Emergentes ▪ Dirección General de Laboratorios de Investigación Electrónica y Forense	▪ Organismo público enfocado a salvaguardar la vida, la integridad, la seguridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos. Esto implica aplicar y operar la política de seguridad pública en materia de prevención y combate de delitos, prevenir la comisión de delitos, e investigar la comisión de delitos bajo el Ministerio Público de la Federación. ▪ Para lo anterior, la División Científica de la Policía establece mecanismos, lineamientos, políticas, protocolos y procedimientos para la aplicación de herramientas de naturaleza técnico-científicas. Selecciona e implementa tecnologías en los procesos y servicios de investigación de delitos electrónicos, criminalística, seguridad de la información y aquellos otros donde se necesite aplicar tecnología en las labores policiales. ▪ La Policía Federal también opera un Centro de Respuesta a Emergencias de Cómputo (CERT-MX), el cual realiza intercambio de información con agencias internacionales e identifica y da seguimiento a los delitos cibernéticos y a la protección de infraestructuras críticas en México.
Centro de Investigación y Seguridad Nacional (CISEN)	▪ Órgano desconcentrado de la Secretaría de Gobernación, cuyo propósito es operar tareas de inteligencia que contribuyan a preservar la integridad, estabilidad y permanencia del Estado Mexicano

FUENTE: Acuerdo A/076/17 por el que se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, Ley de la Policía Federal y su Reglamento, Ley de Seguridad Nacional

Los Angeles
Phoenix
San Diego
Tucson
Ensenada
El Paso
Dallas
Atlanta
Jackson
Mobile
Austin
Houston
New Orleans
Hermosillo
Chihuahua
San Antonio
Guaymas
Torreón
Monterrey
Culiacán
La Paz
México
Mazatlán
Tampico
Guadalajar
Mérida
Cancún
Campeche
Belize
Guatemala

Figura 17: Ejemplo de plan de respuesta a incidentes

1 *Business Information Security Officer*, encargado de seguridad a nivel unidad de negocio.

UNIDAD DE CIBERSEGURIDAD
POLICÍA FEDERAL

El CERT-MX se encarga de prevenir y mitigar las amenazas de seguridad informática que ponen en riesgo la infraestructura tecnológica y la operatividad del país

Centro Especializado en Respuesta Tecnológica

OEA

Mais direitos para mais pessoas

RED PBIP INTERNACIONAL MÉXICO

CIP

Comisión Interamericana de Puertos

Principales acciones tomadas *(herramientas normativas)*

- El reto de la próxima administración en materia de ciberseguridad será enlazar la Estrategia Nacional de Ciberseguridad, con el marco jurídico para que haya obligatoriedad de cumplirla.
- “La Estrategia Nacional de Ciberseguridad ya existe, está en papel y si la nueva administración quiere mejorarla, es posible hacerlo. Sería un gran error no utilizarla, porque es un trabajo que no hizo sólo la administración, es un esfuerzo de la industria, la academia, el gobierno y la sociedad civil”,
- La actual Estrategia Nacional de Ciberseguridad encomienda a la Subcomisión de Ciberseguridad, dentro de la Secretaría de Gobernación, la labor de coordinar al Gobierno de la República y articular los esfuerzos de los diferentes actores para la implementación y seguimiento de la estrategia”.

CIP
Comisión Interamericana de Puertos

OEA
Mais direitos para mais pessoas

La buena noticia

Medidas de ciberprotección en puertos

PUERTOS E INSTALACIONES PORTUARIAS

CODIGO PBIP

ANÁLISIS DE RIESGO

PPIP

EQUIPOS DE COMUNICACIÓN, DE PROTECCIÓN Y SISTEMAS INFORMÁTICOS

AUDUTORÍA Y EXAMEN

CONFIDENCIALIDAD DE LA INFORMACIÓN

ISO31000

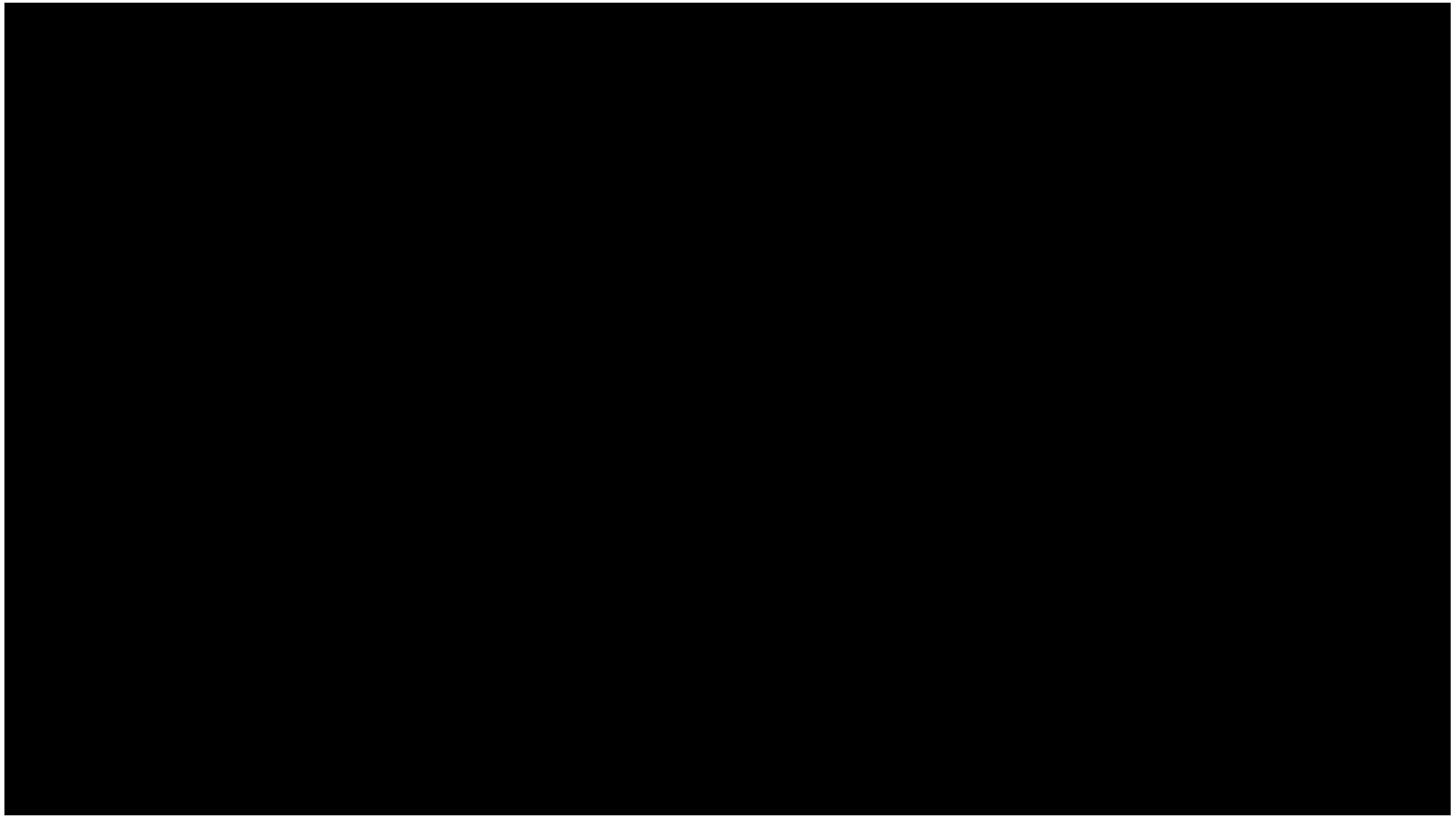
SISTEMAS INFORMÁTICOS

ISO27005

ISO27001

Modificaciones al PPIP en materia de ciber protección, Ciclo 2019 - 2024

RED PBIP MÉXICO INTERNACIONAL A.C.
JOJUTLA 42, CONDESA, CUAUHTÉMOC, MÉXICO CDMX
52 5552862412

Presidente
Mto. Miguel A. Osuna
ienpac@Prodigy.net.mx
525551054695

Seminario PBIP San Nicolas Argentina 20/19