



Una nueva realidad portuaria: Resiliencia ante ciberataques y otros riesgos.

## Ciberseguridad en el escenario pre y post-COVID-19

Rodrigo M. Díaz - CISSP

diaz.rodrido.m@gmail.com



**141.000.000 Videos YouTube**

**5.700.000.000 Correos Electrónicos**

**u\$s 33.000.000,00 Compras OnLine**

# 2020 *This Is What Happens In An Internet Minute*





**MOVILIDAD**  
**AUTOMATIZACIÓN**  
**DIGITALIZACIÓN**  
**AUMENTACIÓN**  
**DESINTERMEDIACIÓN**



**DATO**  
**Combustible de las empresas del futuro**





OEA

Más derechos para más gente



NACIONES UNIDAS

CEPAL



CIP

Comisión Interamericana de Puertos

# Evolución del uso de la tecnología



Fuente : IDC

# Los 10 rubros más afectados

Rubro	2019	2018
Servicios Financieros	1	1
Retail	2	4
Logística	3	2
Medios	4	6
Servicios Profesionales	5	3
Gobierno	6	7
Educación	7	9
Manufactura	8	5
Energía	9	10
Salud	10	8

- El ranking de la industria de logística en tercer lugar subraya el creciente atractivo de datos e infraestructura operados por este tipo de industrias e instituciones tanto del sector privado como gubernamental
- Información biográfica, números de pasaporte, información del programa de fidelización, datos de la tarjeta de pago e itinerarios de viaje es un atractivo creciente para los ciberdelincuentes que buscan rastrear a los viajeros con interés de monetizar la información
- Logística es un objetivo preciado por los ciberdelincuentes por el efecto dominó potencial en los demás rubros

Fuente: IBM X-Force Threat Intelligence Index 2020

# Ransomware

Es una pieza de software malicioso que se instala en una computadora o servidor informático, encripta la información disponible en dicho equipo para luego pedir rescate por su devolución.

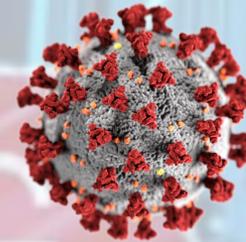
INGENIERIA SOCIAL

FACTOR MIEDO O URGENCIA

VULNERABILIDADES

CONTRASEÑAS

35%



# Incidentes de ciberseguridad en la actividad logística

2 REI GIIM'S DODT DE ANTWERP HACKED

No San Diego port hit by ransomware attack

Co \$2

© 28 Septemb



The Port of S



El Puerto de Barcelona sufre un ciberataque de mercaderías

• Los puertos y la actividad en ciberseguridad



Una imagen del Puerto

Cosco July 2 comp report  
La Autoridad Portuaria de Barcelona sufrió un ciberataque que afectó a la entrega y recepción de mercancías en la entidad.

U.S. MSC confirms malware attack, site threatened

Aug 15, 2019



- A
- J
- A
- V

At the :  
for ves:  
this re:  
Gulf, St  
commu



Infiltrate the system, masked and moved, undetected

This  
In Jur  
Europ  
Molle  
Opera  
causir

# Los nuevos desafíos de ciberseguridad

- El principal objetivo de ataque es la interrupción operativa
- Se demora en promedio 95 días en descubrir un ataque
- Los equipos de trabajo internos no podrán abordar la problemática
- No estábamos preparados para abordar la problemática COVID.

Todo es AHORA

- Sufriremos más ataques desde sistemas de terceros , incluyendo nuestros colaboradores
- El mundo será más digital y más conectado
- No se puede definir claramente el borde
- Todo será Paperless
- Todo será contactless



OEA

Más derechos para más gente



NACIONES UNIDAS

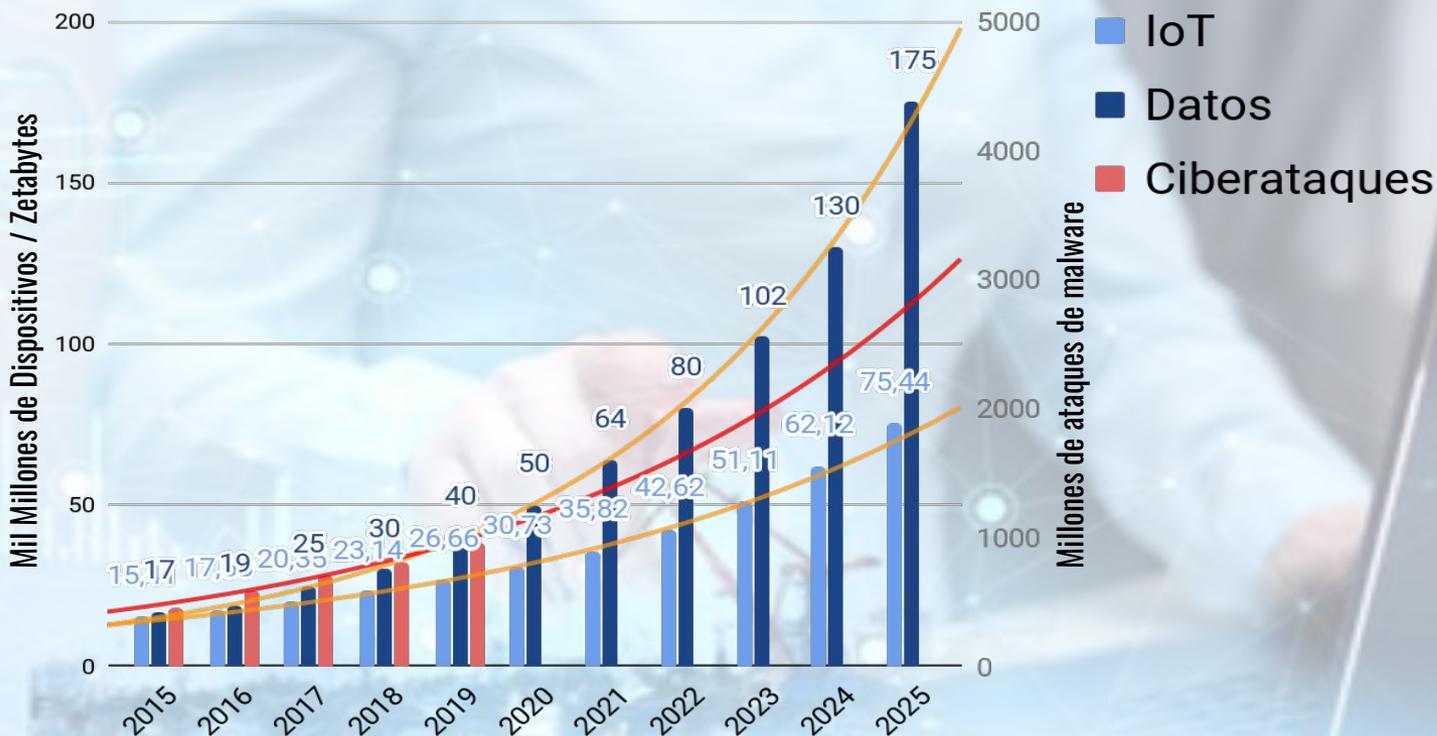
CEPAL



CIP

Comisión Interamericana de Puertos

# Evolución del uso de la tecnología



Fuente : IDC

# Los acciones de ciberseguridad

- **Crear un plan integral de defensa sin demoras. Todos los servicios de ciberseguridad pueden hacerse de manera remota**
  - **Procesos - Compromiso de la dirección**
    - Políticas y Procedimientos
    - Desarrollar y probar con frecuencia el plan de contingencia
    - Someterse a pruebas de stress de terceros
  - **Tecnológico**
    - Revisar estándares con especialistas
    - Software y hardware con soporte del fabricante vigente
    - Herramientas de análisis avanzado de eventos con alertas on line
    - Tecnologías intrínsecamente seguras
  - **Personas**
    - Entrenar a todo nuestro personal para construir cibercultura
    - Hacer conciencia de ciberinmunidad



**OEA**

Más derechos para más gente



NACIONES UNIDAS

**CEPAL**



**CIP**

Comisión  
Interamericana de Puertos

**Rodrigo M. Díaz - CISSP**  
**diaz.rodrico.m@gmail.com**

