CLAIN 2018

XXII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos PANAMA, 17-18 de Mayo 2018

ASOCIACION BANCARIA DE PANAMA

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

"Era Digital: Nuevo Reto para la Transformacion de la Auditoria Interna"

Regulaciones y Requerimientos de Ciberseguridad para el Sector Financiero

¿Y qué es Ciberseguridad?

¿Y qué es Ciberseguridad?

KASPERSKY lab

"Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos"

ISACA®
Trust in, and value from, information systems

"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados"

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

"El proceso para proteger información a través de prevenir, detectar y responder a ataques informáticos"

Ejemplo de un ciberataque masivo

Tipo de ataque: Ciberataque basado en Ransomware

Fecha: 12 de mayo de 2017

Plataforma: principalmente Windows 7 y WinServer 2003

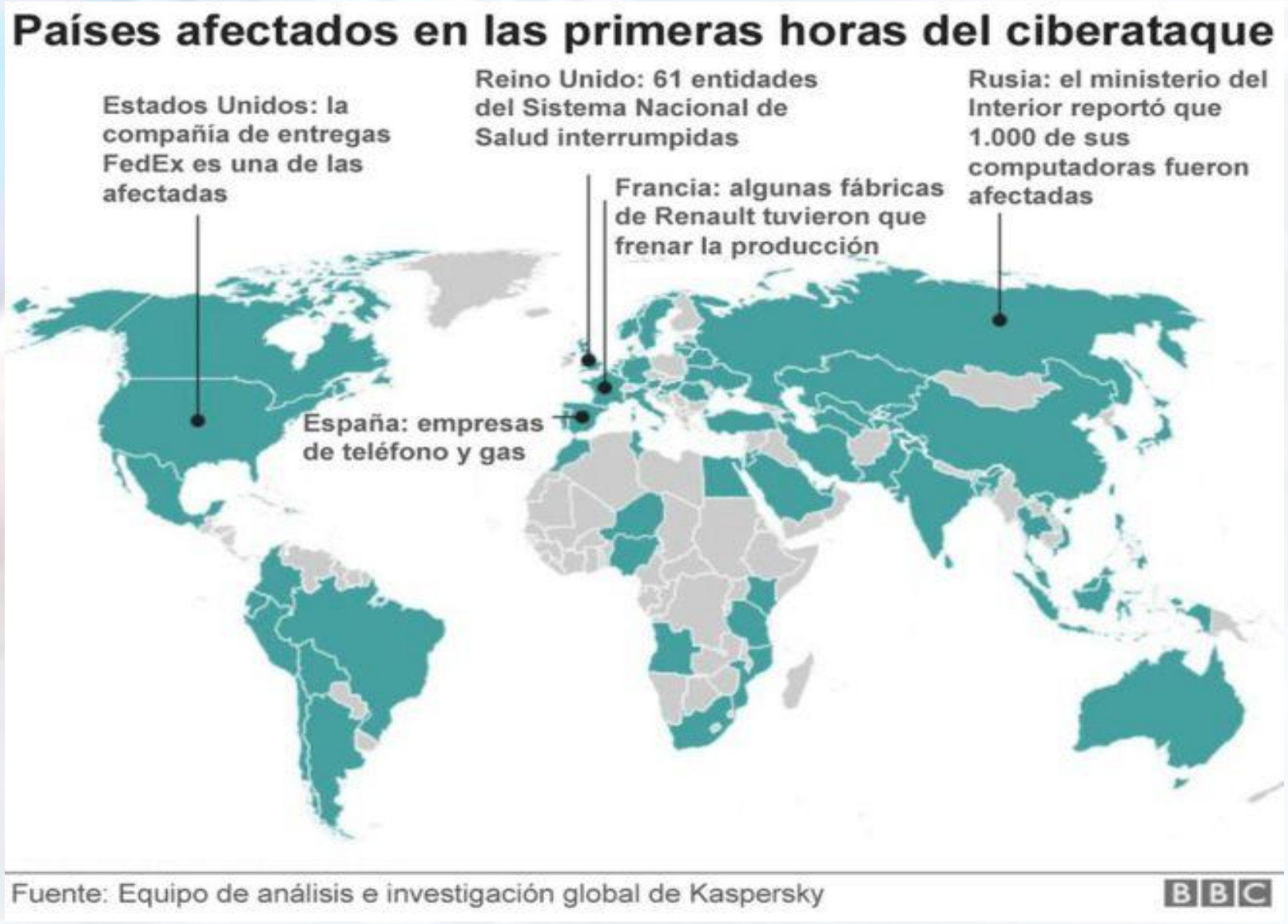
 # de computadoras: ~ 200K – 230K

 # de países: >150

Pago: $300 USD en bitcoins

Fuente: The Guardian& Financial Times

Ejemplo de un ciberataque masivo



Otros ataques relevantes

- Equifax – 143 millones de registros
- Gmail – 1 millón de cuentas comprometidas
- eBay – 145 millones de usuario
- Sony – 5 Películas y 50,000 registros de sus empleados
- J.P. Morgan Chase – 76 millones de clientes y 7 millones de PYMES
- Home Depot – 60 millones de TC y 53 millones de correos electrónicos
- Apple – Brecha de seguridad en iCloud – fotos de famosos se hacen públicas
- Target – 40 millones de TC y 110 millones de correos y direcciones

¿Cómo nos estamos preparando en América Latina?

- CSIRTs han sido creados en la mayoría de los países
- En algunos países de la región ya se empiezan a desarrollar regulaciones o estrategias orientadas a la ciberseguridad

Fuente: OEA

- Decreto 533: CREA COMITÉ INTERMINISTERIAL SOBRE CIBERSEGURIDAD
- Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022
- Circular: Seguridad de la Información y Ciberseguridad. Enfatiza la necesidad de tomar medidas de control

- Medidas mínimas de seguridad para las entidades del sistema financiero
- LA LEY GENERAL DEL SISTEMA FINANCIERO Y DEL SISTEMA DE SEGUROS Y ORGANICA DE LA SUPERINTENDENCIA DE BANCA Y SEGUROS
- REGLAMENTO DE LA GESTIÓN INTEGRAL DE RIESGOS
- REGLAMENTO DE TARJETAS DE CRÉDITO Y DÉBITO
- CIRCULAR N° G-164 – 2012 Reporte de eventos de interrupción significativa de operaciones
- CIRCULAR Nº G- 139 -2009 Gestión de la continuidad del negocio

POLÍTICA NACIONAL DE SEGURIDAD DIGITAL, Contiene referencias a otras regulaciones como:

- Ley 527 de 1999 (Comercio Electrónico)
- Ley 594 de 2000 (Ley General de Archivos)
- Ley 599 de 2000 (Código Penal)
- Ley 600 de 2000 (Código de Procedimiento Penal)

- Reglamento de la LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES (LFPDPPP)
- DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS
- INSTITUCIONES DE CRÉDITO

- FFIEC – Information Technology Examination Handbook (USA – 2004)
- Cybersecurity Framework de NIST

- Convenio sobre la Ciberdelincuencia
- Budapest 23-nov-2001

Requerimientos de seguridad

•**Identificar (Identify):** Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.

•**Proteger (Protect):** Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.

•**Detectar (Detect):** Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua.

•**Responder (Respond):** Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.

•**Recuperar (Recover):** Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

Requerimientos de seguridad

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Preguntas


thanks
Dank
merciBeaucoup
grazas
grazieMille
GRACIAS
gracias
esker
gràcies


scotiabank