
infosecurity®
MEXICO
Presenting
DARKTRACE
22 - 23 mayo de 2019
EVENTO LÍDER EN
CYBERSEGURIDAD
Part of
infosecurity
GROUP
Organized by
Reed Exhibitions®

Ciber Seguridad

¿Por qué nos Hackearon?, si hemos invertido mucho dinero…

infosecurity MEXICO

Algunos incidentes Cibernéticos…

BELL CANADA
Exposición de datos de 100,000 clientes

BANCOMEXT SWIFT
Extracción 100 millones

UNDER ARMOR MyFitnessPal
150 millones de registros filtrados

BANCO DE CHILE SWIFT
Robo de 10 millones de dólares

BANCO DE MEXICO SPEI

SINGHEALTH Singapore
1.5 millones de registros robados

FACEBOOK
Exposición de 50 millones de cuentas de usuarios

BRITISH AIRWAYS
Fuga de 380 mil tarjetas de crédito

MEGACABLE
Encriptan Servidores

US Postal Service
60 millones de usuarios expuestos

ene · feb · mar · abr · may · jun · jul · ago · sep · oct · nov · dic

CI BANCO
Ataque con Malware en equipos

BANCO DE MEXICO SPEI
400 millones de pesos

TicketFly (EventBrite)
Hacker Roba 26 millones de emails y direcciones de casas

Google
Filtrado 500,000 cuentas "Derriban el servicio"

US MEDICARE & MEDICAL SERVICES
Filtrado de 75,000 registros de personas

AXA
XML Injection

MARRIOT
500 millones de registros robados

2018

CUMPLIMIENTO REGULATORIO 01

AMENAZAS INTERNAS 02

AMENAZAS EXTERNAS 03

Vulnerabilidad en tus aplicaciones y los servicios

- Inseguros
- Fallas / Incompletos

Problemas en tus controles / Procesos / Políticas

- Falla en la ejecución
- Falta de Cumplimiento
- Débiles
- Ausencia de

Gestión de servicios inadecuada

- Falta de Parches y Actualización
- Falta de Respaldos
- Falla en las Operaciones

Personas

- Disgustadas
- Malintencionadas
- Curiosas
- Falta de Cultura de Seguridad / Sensibilización
- Errores Inadvertidos

CUMPLIMIENTO REGULATORIO 01

AMENAZAS INTERNAS 02

AMENAZAS EXTERNAS 03

AMENAZAS

TROYANOS

CIBER CRIMEN

SECUESTRO DE SESIÓN

PHARMING

ROOTKIT

MALWARE

CIBER ESPIONAJE

DNS POISONING

ARP SPOOFING

SPAM

ADWARE

PHISHING

GUSANOS

ROBO DE IDENTIDAD

CIBERGUERRA

ROBO PROPIEDAD INTELECTUAL

IoT BOTNET

RANSOMWARE

SQL INJECTION

APT

DDOS

SPYWARE

CROSS SITE SCRIPTING

VIRUS

Crypto Mining

VULNERABILIDAD

RAT

FUGA DE INFORMACIÓN

FILTRACIÓN DE DATOS

infosecurity MEXICO

Vulnerabilidad en tus aplicaciones y los servicios

- Inseguros
- Fallas / Incompletos

Problemas en tus controles / Procesos / Políticas

- Falla en la ejecución
- Falta de Cumplimiento
- Débiles
- Ausencia de

Gestión de servicios inadecuada

- Falta de Parches y Actualización
- Falta de Respaldos
- Falla en las Operaciones

Personas

- Disgustadas
- Malintencionadas
- Curiosas
- Falta de Cultura de Seguridad / Sensibilización
- Errores Inadvertidos

Ejemplos de Ataques Cibernéticos…

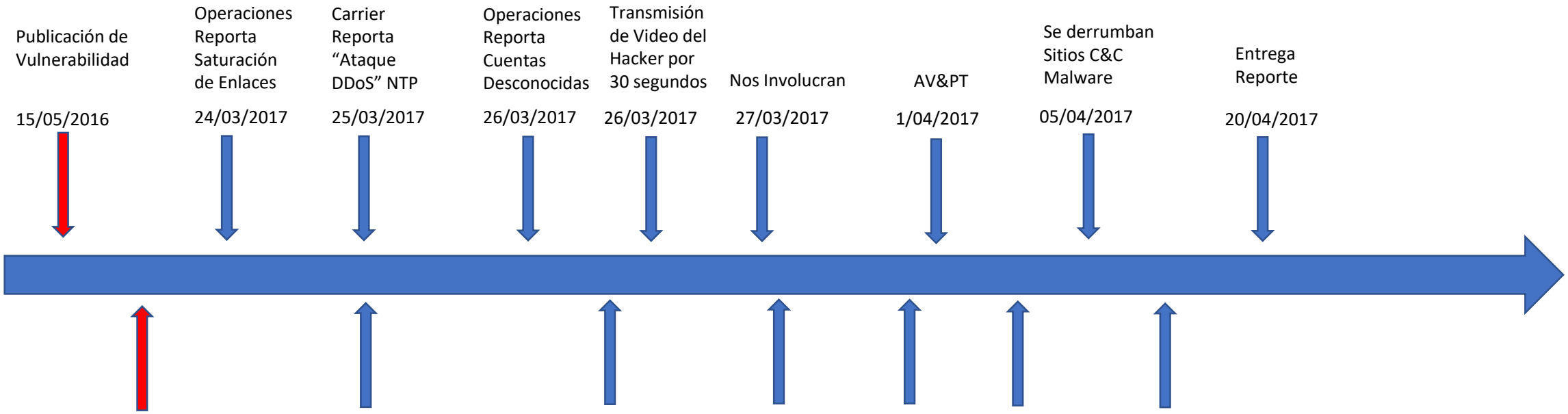
Compartir Experiencia

Las fechas han sido modificadas

Los hechos son reales

Los nombres de los clientes no son divulgados

Robo "PI" en Televisora por Internet



Participantes:

- Integrador
- Empresa de Medios
- Empresa de Producción

Impacto:

- Intrusión de Hacker en Red
- Transmisión de Video por 30 segundos no relacionado con la televisora
- Robo de Propiedad Intelectual (Lanzamiento de Nuevo Contenido)
- 1M USD en pérdidas por difusión de Contenido

¿Por qué nos Hackearon?, si hemos invertido mucho dinero…

Informe a CEO / CFO:

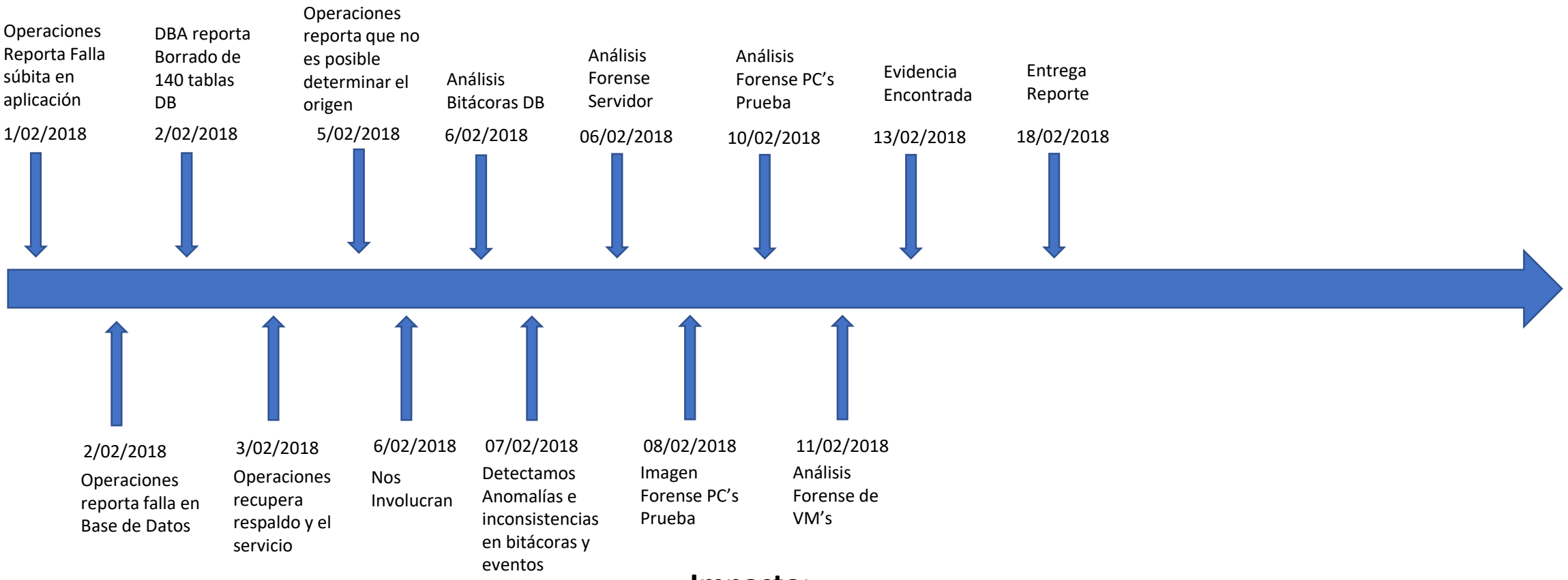
- **Falta de Debida Diligencia**
- **Falta del Debido Cuidado**
- **Falta de Cumplimiento**
- **Falla en las Operaciones**
- **Administración Inadecuada**
- **Falta de Capacidad para Responder**

Informe a CIO

- **Vulnerabilidades de Sistema Operativo y Base de Datos**
- **Fallas:**
  - **Administración de vulnerabilidades**
  - **Monitoreo de Servicios**
  - **Gestión de servicios**
  - **Control de ejecución de programas**
  - **Administración de cambios en las configuraciones**

El Ataque y la transmisión de Video solo fue un distractor mientras el hacker ya estaba conectado y ejecutando, su objetivo que era robar los videos. Se considero un ataque dirigido

Sabotaje empresa Farmacéutica



Participantes:

- Integrador de Servicios
- Fabrica de Software

Impacto:

- Operación detenida por un día
- No se facturo 24 horas
- Eliminación de 140 Tablas de Base de Datos
- 24 horas para restaurar la operación
- 20 Personas dedicadas para el incidente

¿Por qué nos Hackearon?, si hemos invertido mucho dinero…

Informe a CEO / CFO:

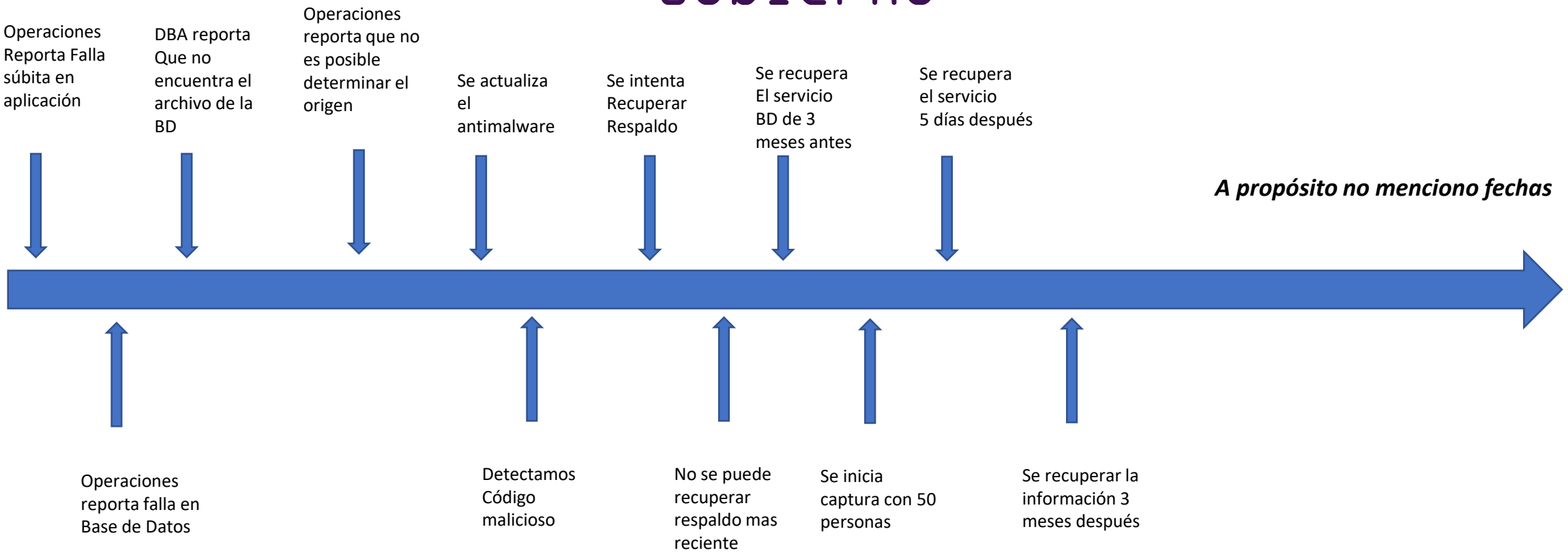
- **Falta de Debida Diligencia**
- **Falta del Debido Cuidado**
- **Falta de Cumplimiento**
- **Falla en las Operaciones**
- **Administración Inadecuada**
- **Falta de Capacidad para Responder**

Informe a CIO

- **Passwords Débiles**
- **Proceso inadecuado de Baja de Empleado**
- **Fallas en la administración de usuarios privilegiados**
- **Falta de controles en las máquinas de los desarrolladores**
- **Uso de Tabla de Passwords, sin protección y compartida sin control**
- **Uso de máquina de pruebas sin protección ni control, ni supervisión**
- **Uso de Máquina Virtual en los equipos de pruebas**

El Ataque fue un sabotaje de un ex empleado de la fábrica de software, usando una máquina de pruebas que conocía, usando contraseñas y cuentas, que no fueron eliminadas después de su salida de la empresa.

Ataque Cibernético - Entidad Gobierno



Participantes:

- Cliente – Entidad de Gobierno

Impacto:

- Operación detenida por una semana
- Perdida total de la Base de Datos en SQL Server
- 3 Meses para recuperar la información y 50 Personas dedicadas a capturar del papel las transacciones

¿Por qué nos Hackearon?, si hemos invertido mucho dinero…

Informe a CEO / CFO:

- **Falta de Debida Diligencia**
- **Falta del Debido Cuidado**
- **Falta de Cumplimiento**
- **Falla en las Operaciones**
- **Administración Inadecuada**
- **Falta de Capacidad para Responder**

Informe a CIO

- **Explotación de una vulnerabilidad**
- **Portal Web mal configurado**
- **Firewall configurado inadecuadamente**
- **Uso de Network Shares**
- **Antimalware no actualizado**

El respaldo no se pudo recuperar

Ataque Cibernético - Entidad Gobierno

¿Por qué nos Hackearon?, si hemos invertido mucho dinero…

- El ataque fue el 18 de septiembre del 2001 (hace 17 años)
- El malware fue el gusano “Nimda” (admin al revés)

¿Por qué desde hace 17 años seguimos teniendo los mismos problemas?

¿Por qué desde hace 17 años seguimos teniendo los mismos problemas?

Factor Humano

- **Negligencia / Descuido**
- Falta de Tiempo
- Falta de Capacitación
- **Falta de Personal**
- Cargas de Trabajo Excesivas
- Fama / Dinero

Factor Empresa

- Falta de Procesos, Políticas, Controles, Normas
- Falta de Cumplimiento
- Competencia / Propiedad Intelectual
- **Falta de Presupuesto**

Factor Tecnológico

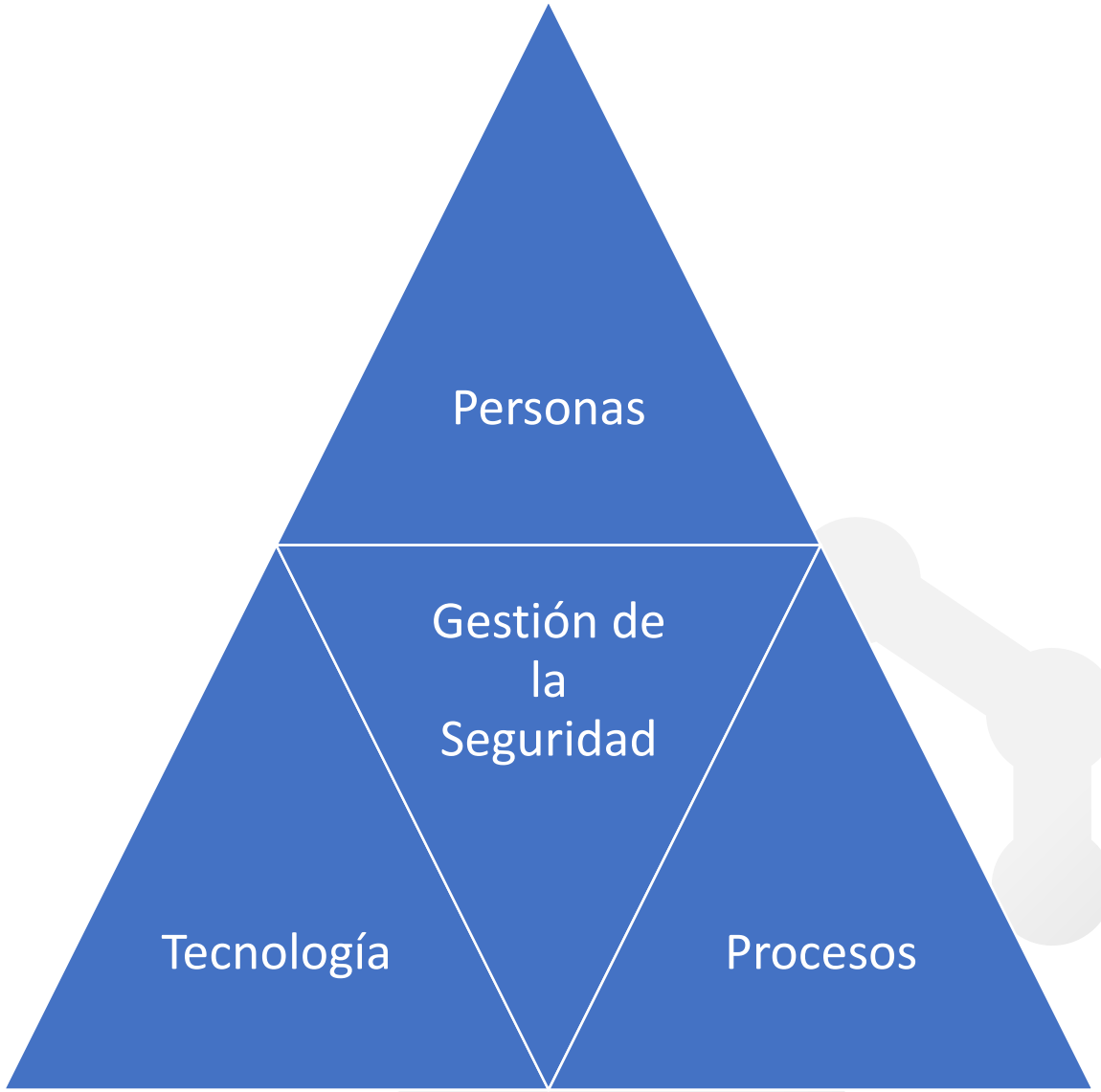
- Saltos Tecnológicos
- Falla en la Ejecución
- Industria del Malware
- **Tecnología Vulnerable**

Globalización

- Ciber Guerra
- Espionaje Industrial
- **Presencia en Internet**
- Hackers / Vandalismo
- Gobierno en Búsqueda de Fondos
- Riesgos / Amenazas
- Delincuencia Organizada

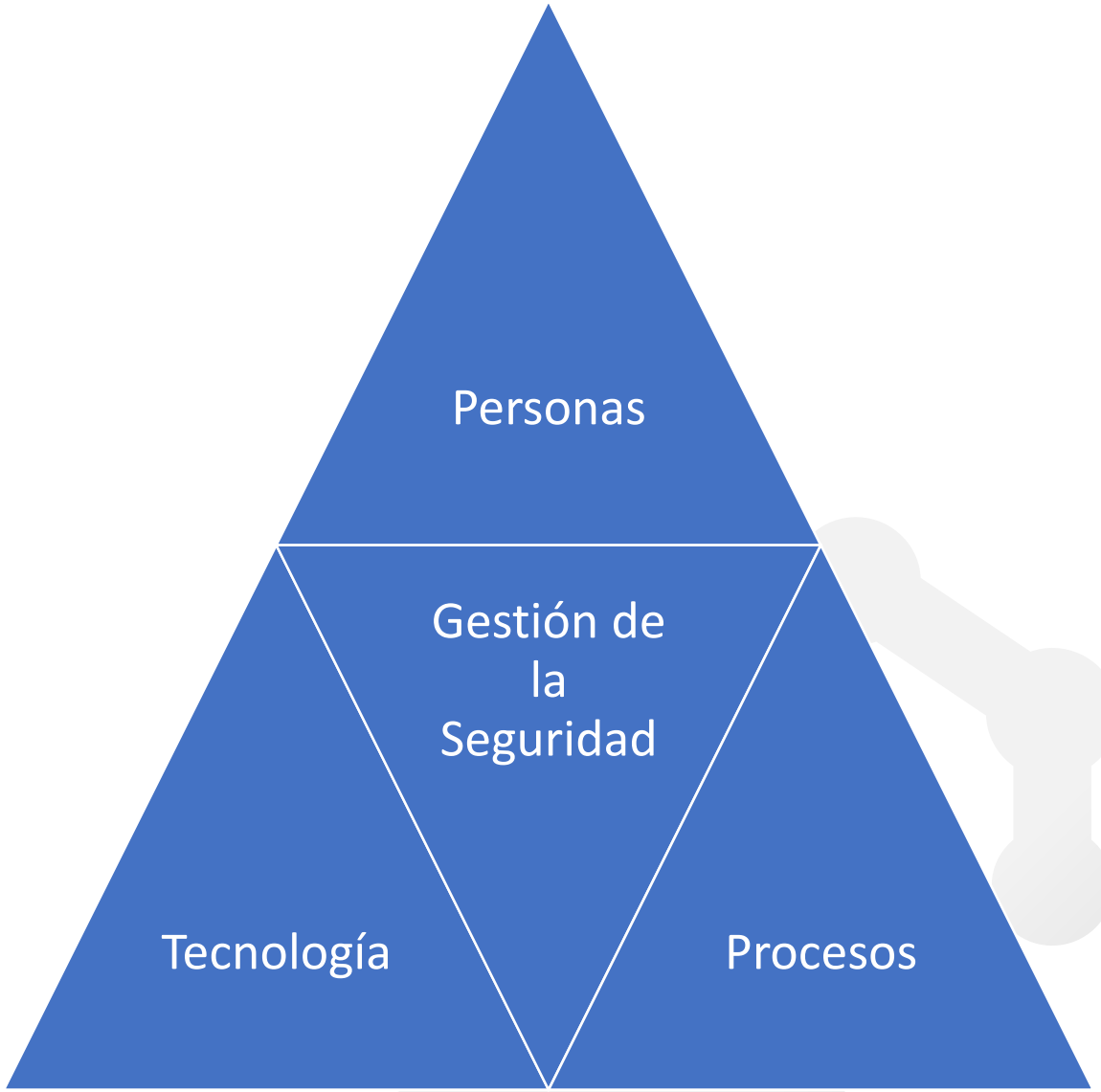
Factores a mejorar

- Posicionar Ciber Seguridad a nivel Estratégico
- Plan y Estrategia de Seguridad
- Ejecutar Análisis de Riesgos de Negocio / Tecnológico
- Establecer Procesos, Controles, Políticas, Estándares
- Cultura / Sensibilización
- Capacitación
- Contratar un Seguro que cubra Incidentes Cibernéticos



Factores a mejorar

- Establecer Normatividad / Reglas
- Asignar Presupuesto
- Tercerizar lo Operativo
- Gestión Continua de la Seguridad (Servicio Administrado)
- Capacidad de Respuesta a Incidentes



¡Muchas Gracias!

AXITY EN AMÉRICA:

USA: New York y Dallas

MEXICO: Ciudad de México, Monterrey y Guadalajara

COLOMBIA: Bogotá, Medellín y Cali

PERU: Lima

CHILE: Santiago de Chile

ARGENTINA: Buenos Aires

conectados@axity.com