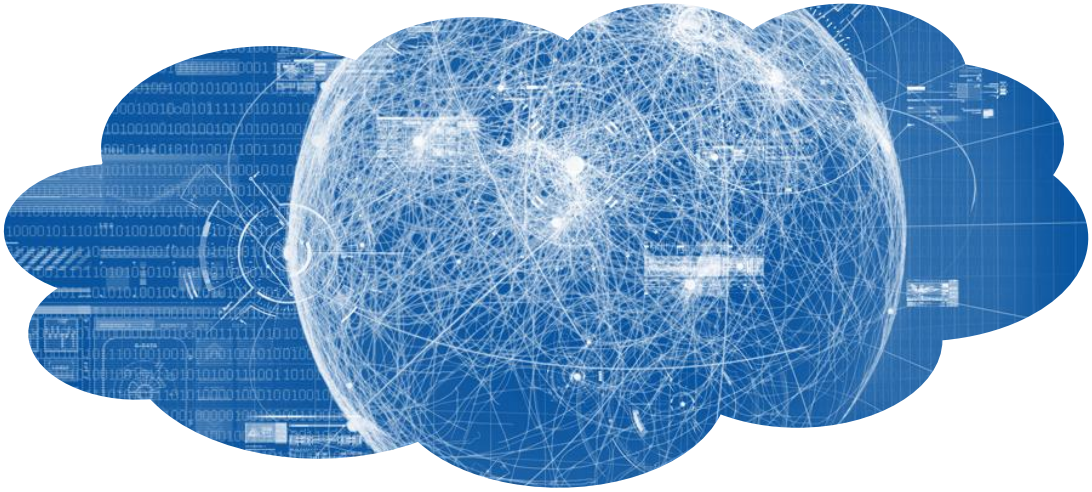
BBVA



Nuevos retos de Ciberseguridad en la transformación digital del sector financiero

Octubre 2016

1 Introducción a la ciberseguridad

2 Cómo gestionar la ciberseguridad

3 Principales riesgos de ciberseguridad

4 Casos relevantes en la industria

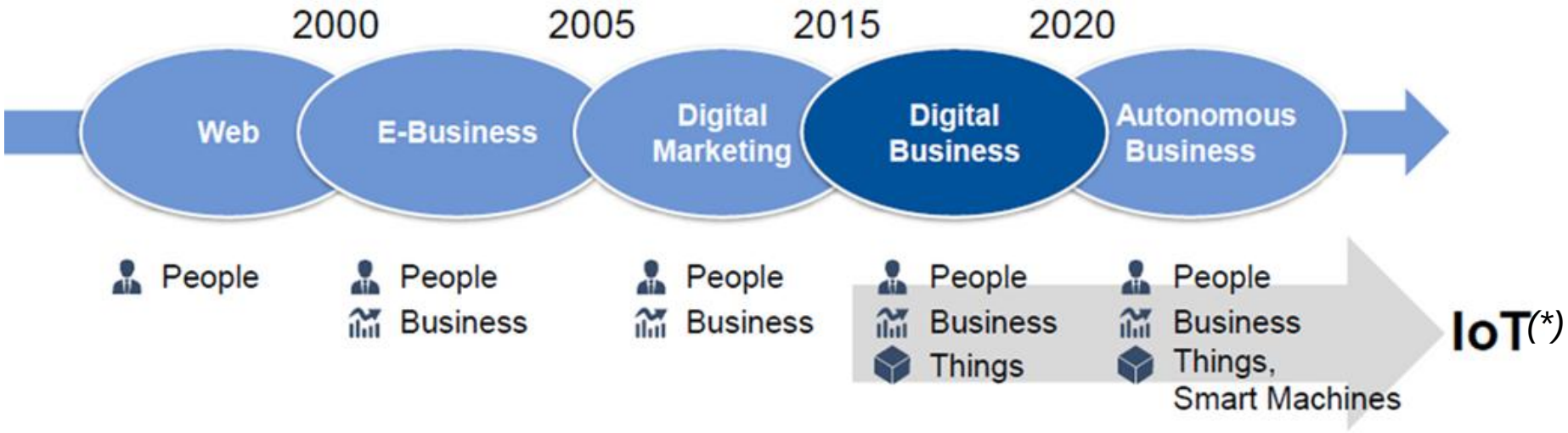
5 Conclusiones

1

Introducción a la ciberseguridad

Las etapas del Negocio Digital

La característica evolución del negocio en base a las fases tecnológicas

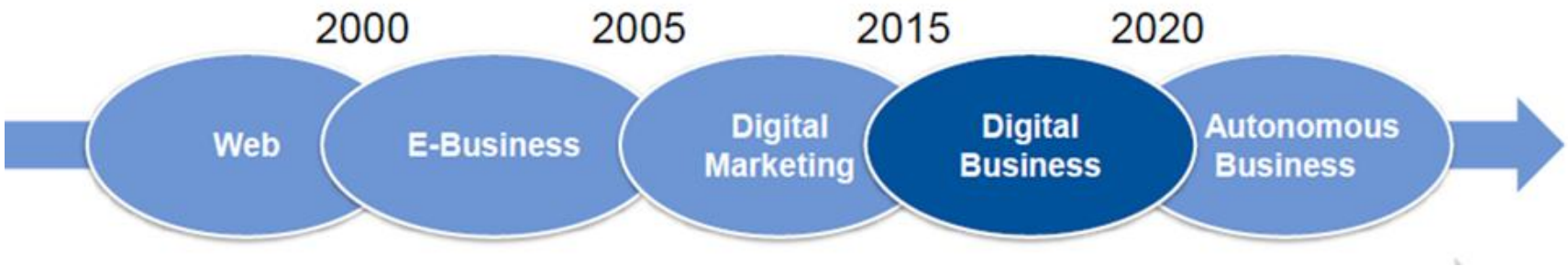


Fuente: Gartner

** Internet of Things*

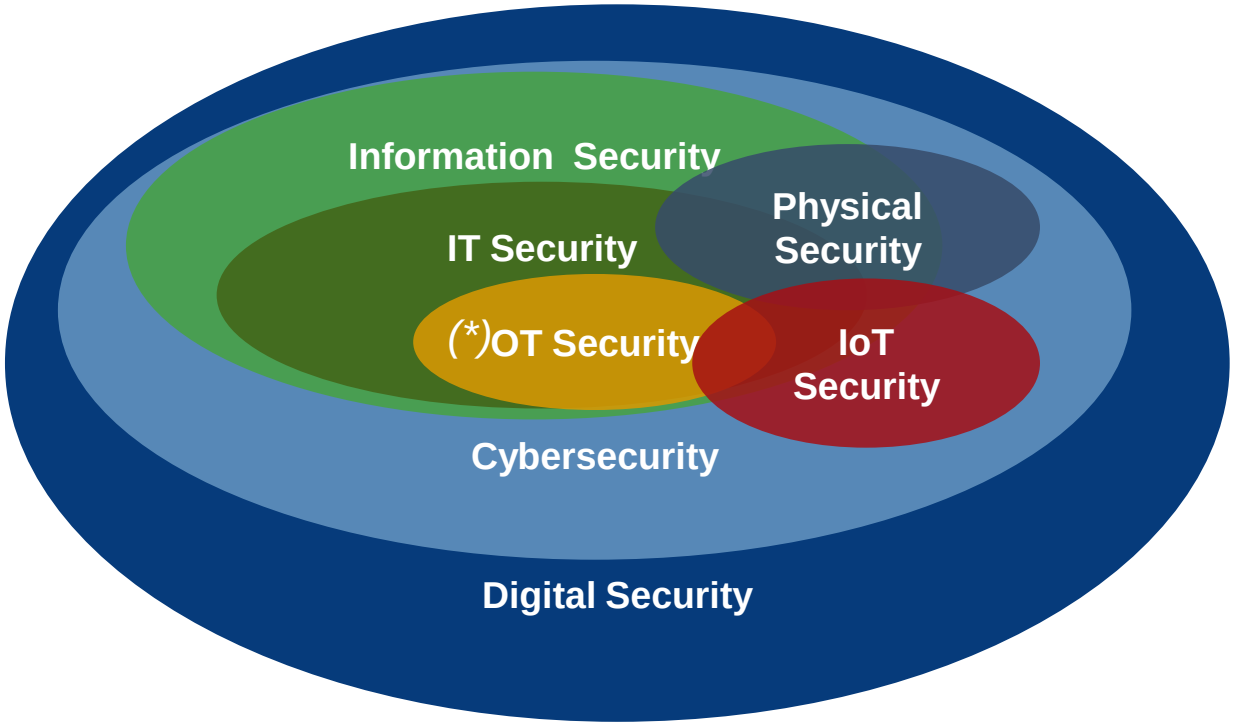
Las etapas de la protección de la Información

La evolución del modelo de Seguridad de BBVA ha sido paralela a la evolución del Negocio Digital.



Ámbitos de la Ciberseguridad

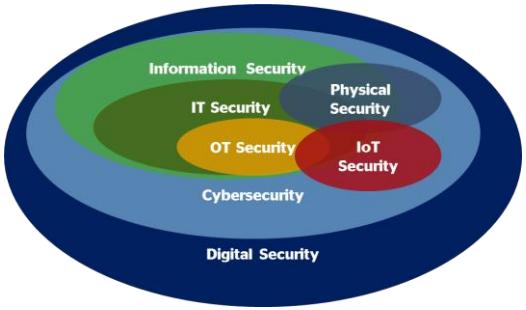
Nuevo enfoque y definición de la Ciberseguridad y Seguridad Digital



Fuente: Gartner

** Operational Technology Security*

Ámbitos de la Ciberseguridad



	Riesgos de Procesos Tecnológicos *Gestión de Cambios*	Riesgos de Plataforma Tecnológica *Virus y vulnerabilidades*	Riesgos de la Información *Robo de información*	Riesgos de operar en Internet *DDoS, APT's*	Riesgos del entorno digital *Digital trust*
OT Security	✓				
IT Security	✓	✓			
Information Security	✓	✓	✓		
Cybersecurity	✓	✓	✓	✓	
Digital Security	✓	✓	✓	✓	✓

Earl Perkins, Gartner Group VP Research

“La Seguridad Digital es la expansión y extensión, orientada por el riesgo, de prácticas de seguridad y riesgos existentes que protegen los activos digitales en todos los tipos de negocio digital, y garantizan que las relaciones entre esos activos sean confiables.”

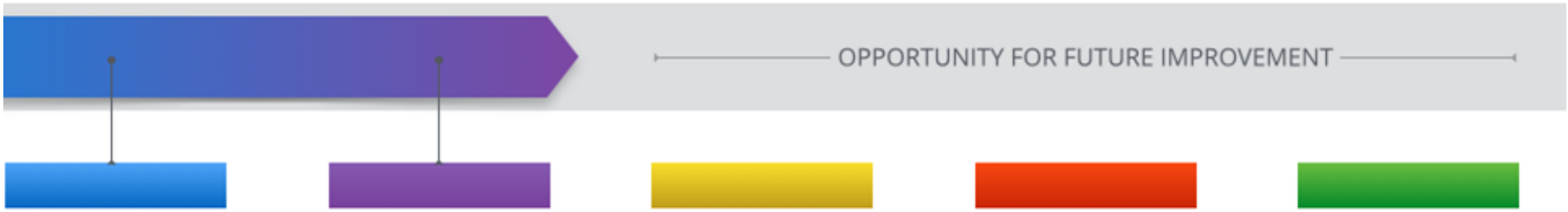
2

Cómo gestionar la ciberseguridad

Marco de Referencia de la Ciberseguridad

El NIST Cybersecurity Framework 1.0 se está empleando como referencia por el BCE en su proceso de valoración del riesgo de ciber seguridad de las entidades financieras europeas.

5	Dominios
22	Subdominios
98	Indicadores



IDENTIFY (24)

- Asset management (6)
- Business environment (5)
- Governance (4)
- Risk assessment (6)
- Risk management strategy (3)

PROTECT (35)

- Access control (5)
- Awareness and training (5)
- Data security (7)
- Information protection and procedures (12)
- Maintenance (2)
- Protective technology (4)

DETECT (18)

- Anomalies and events (5)
- Security continuous monitoring (8)
- Detection process (5)

RESPOND (15)

- Response planning (1)
- Communications (5)
- Analysis (4)
- Mitigation (3)
- Improvements (2)

RECOVER (6)

- Recover planning (1)
- Improvements (2)
- Communications (3)

(#) Número de indicadores del modelo

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

Modelo de Madurez del Marco de Referencia

Modelo

IDENTIFICAR	PROTEGER	DETECTAR	RESPONDER	RECUPERAR
Gestión de activos	Control de acceso	Anomalías y eventos	Planificación de respuesta	Planificación de la recuperación
Entorno de Negocio	Concienciación y entrenamiento	Monitorización continua de seguridad	Comunicación	Mejoras
Governance	Seguridad de datos	Proceso de detección	Análisis	Comunicación
Evaluación riesgo	Protección de la información y procedimientos		Mitigación	
Estrategia de gestión de riesgo	Mantenimiento		Mejoras	
	Tecnología de protección			

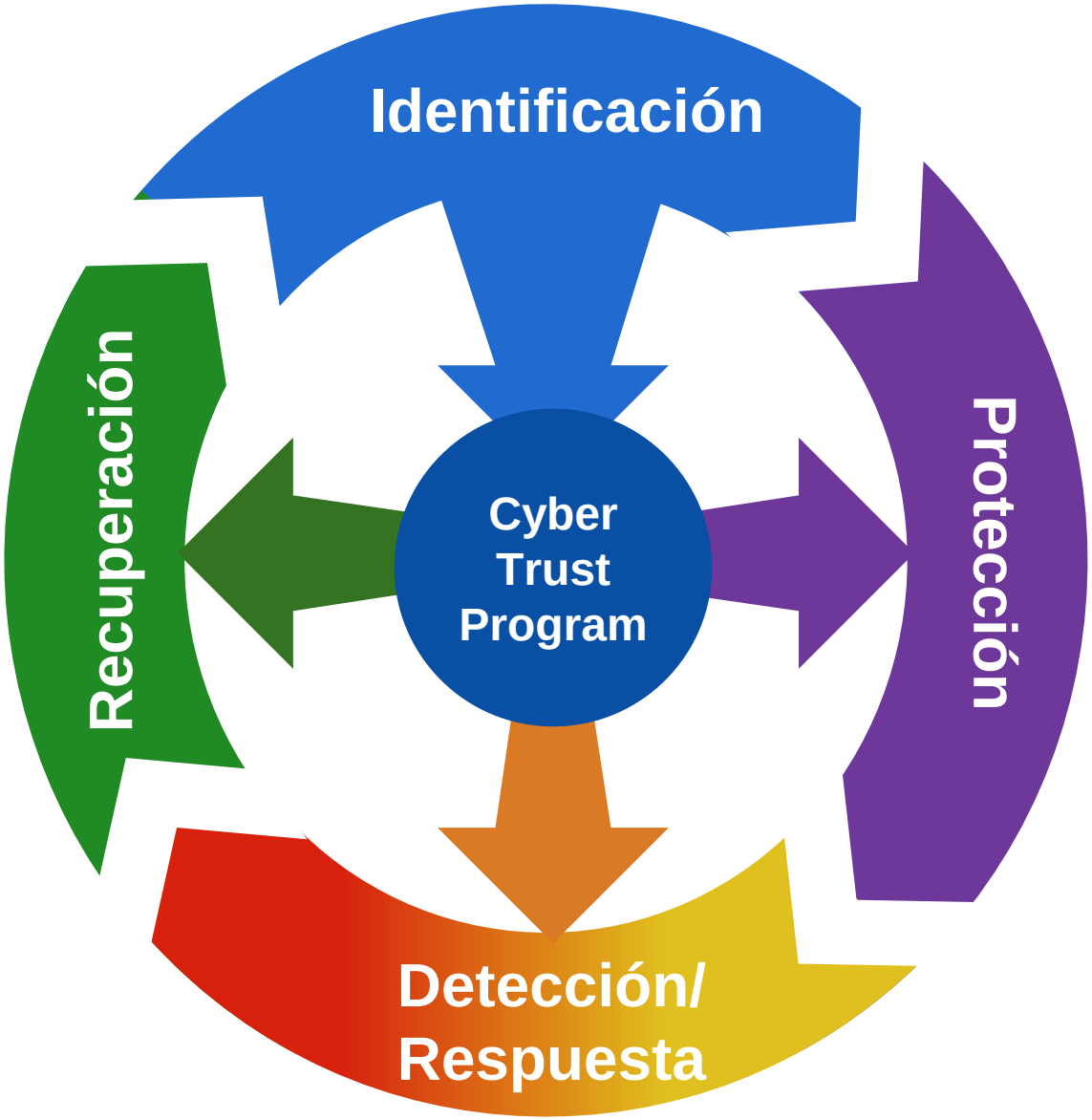
Indicadores

PR.PT-1: Se han definido, documentado, implantado y revisado trazas y registros de actividad / auditoria, de acuerdo a una política.
PR.PT-2: Los soportes extraíbles están protegidos y su uso está restringido de acuerdo a una política.
PR.PT-3: El acceso a los sistemas y activos está controlado, incorporando el principio de necesidad de acceso.
PR.PT-4: Las comunicaciones y redes de control están protegidas.

Madurez

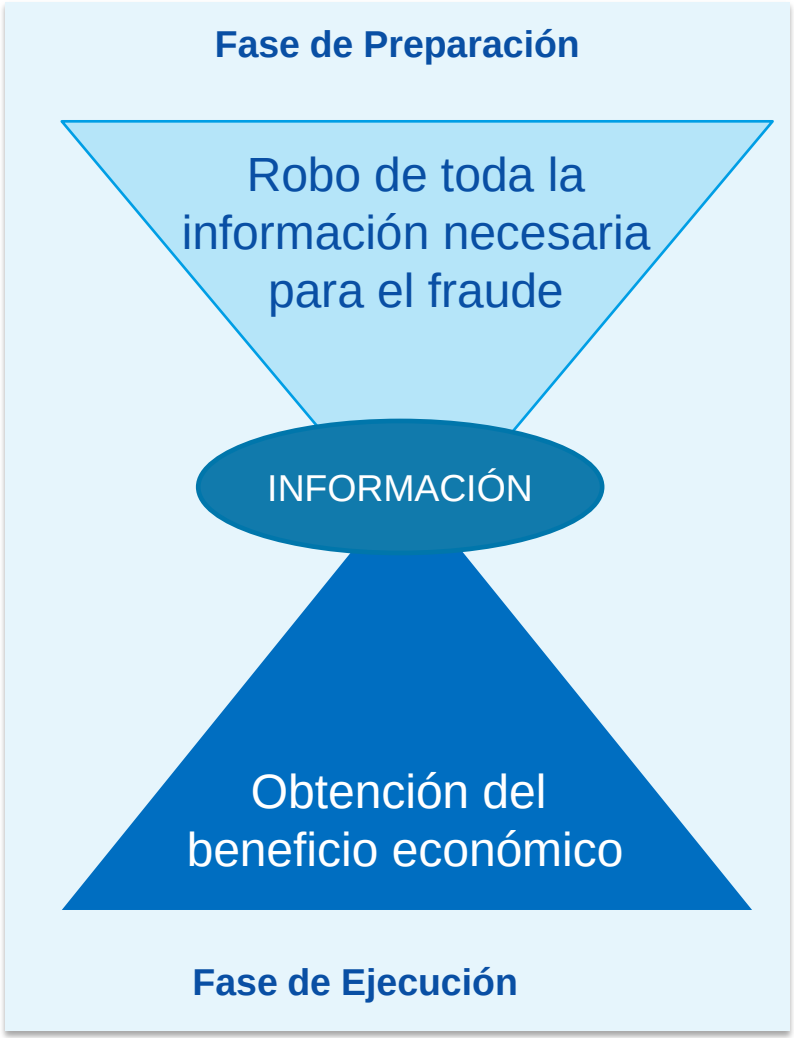
1. Existen registros y trazas de actividad en sistemas y aplicaciones.
2. Los registros están normalizados y se recuperan periódicamente.
3. Los registros se recuperan de forma continua en un sistema estructurado para ser analizados mediante procedimientos definidos.
4. Existe un sistema de gestión y análisis continuo de registros que facilita correlación y seguimiento de actividades, y facilita alarmas.
5. Se realizan procesos continuos de análisis y mejora sobre la gestión de registros, con enfoque hacia la eficiencia y aportación de valor.

Ciclo de Gestión de las Amenazas



Gestión Integral del Riesgo

Cadena de valor de la delincuencia organizada



Medidas de mitigación

Evitar los robos de Información

Medidas de Protección de la Información

Evitar la monetización de la Información

Servicios de Prevención de Fraude

¿Por dónde empezar?

1. Priorizar los activos de información por riesgos de negocio
2. Integrar profundamente la seguridad en el entorno tecnológico
3. Diferenciar la protección por la importancia de los activos
4. Desplegar defensas activas para descubrir ataques de forma proactiva
5. Probar continuamente los planes de respuesta para mejorarlos
6. Involucrar al personal de primera línea para que entiendan el valor de los activos de información
7. Incorporar la ciber-resiliencia en los procesos de gobierno y gestión de riesgo en toda la Entidad

Fuente: Gartner

3 Principales riesgos de ciberseguridad

Tendencias de Ciberseguridad 2016 - 2017

Aplicaciones, Datos, Sistemas

- Hardening y aislamiento de datos y aplicaciones
- Protección y auditoría centrada en los datos
- Preparación para la seguridad definida por software y el Internet of Things

Monitorización, Defensa, Verificación e Inteligencia

- Defensa avanzada ante amenazas
- Inteligencia de Seguridad
- Foco de la prevención a la detección
- Patrones y “Machine Learning”

Red, Movilidad, Cloud

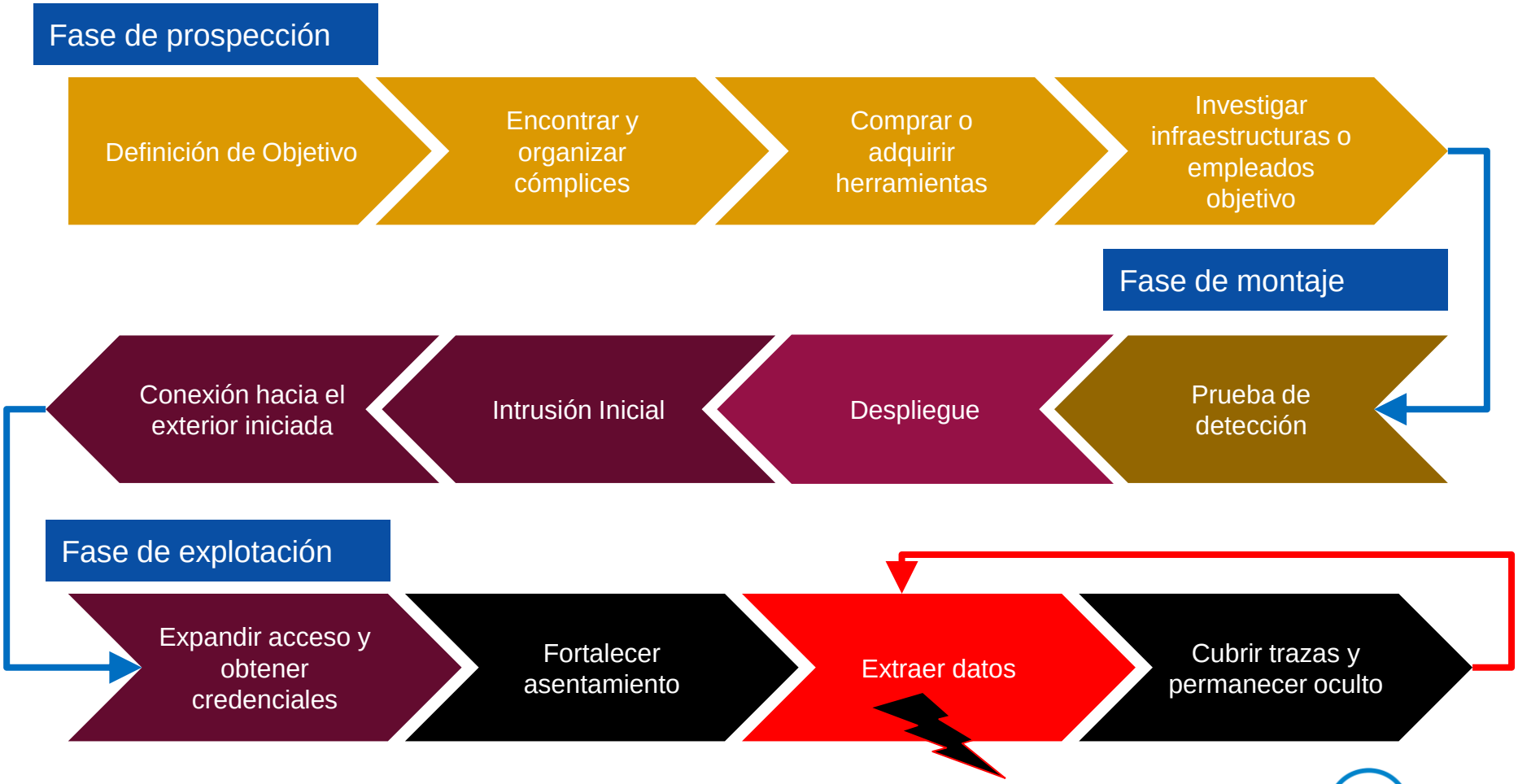
- Servicios de intermediación de Seguridad
- Protección de brechas de seguridad en dispositivos móviles
- “Espectro de confianza” de los dispositivos móviles
- Movimientos de la seguridad al chip
- Expansión de la Seguridad Cloud

Identidad y Gestión de Accesos

- La identidad de las cosas
- Acceso adaptativo
- Gestión de Identidades y Accesos bimodal
- Seguridad centrada en las personas

Fuente Gartner

Ciclo de una amenaza persistente



Fuente:

Tipos de Amenazas

Amenazas externas

Infecciones de Malware por email

- Descargas
- Adjuntos
- Compartición de archivos
- Software pirata
- “Spear Phising”
- Modificaciones de Rutas y DNS

Infecciones de Malware Físicas

- Memorias USB infectadas
- CDs y DVDs infectados
- Tarjetas SD infectadas
- Dispositivos varios infectados
- Equipos IT con puertas traseras

Explotación externa

- Hacking Profesional
- Exploits de vulnerabilidades
- Penetración en cloud
- Penetración Wi-Fi maliciosa
- Puente por smartphone

Amenazas internas

Amenaza de Insider

- Empleado desleal
- Subcontratista malicioso
- Experto en ingeniería social
- Personal infiltrado
- Incidente criminal (acceso, robo, etc.)
- Instalación de Software de doble uso

Conexiones confiables

- Robo de credenciales VPN
- Servidores de itinerancia secuestrados
- Escucha en conexiones B2B
- Brechas en sistemas de proveedores
- Brechas en sistemas alojados externamente
- Equipamiento de red del mercado

Fuente: DAMBALLA

4 Casos relevantes de la industria (tipos)

Casos relevantes (tipos)

Tipos

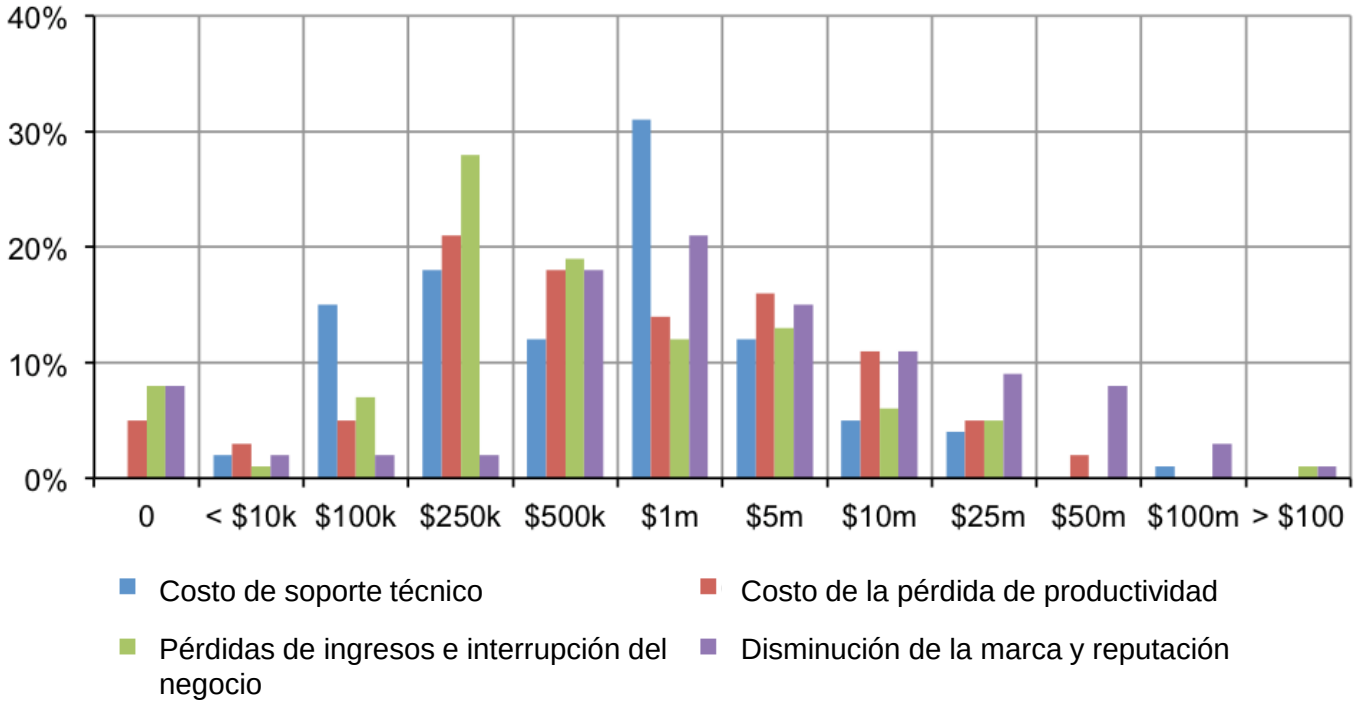
- Fraude Interno – Robo de información de clientes
- Fraude externo – Adulteración de ATMs y POS
- Debilidades en el modelo de Seguridad – ATP y VTS (0-Day)
- Negligencia – Pérdida de información sensible

Impacto

- Reparación – Pérdida económica sustancial (varios $MM)
- Negocio – Disminución, detenimiento del ingreso, “efecto sorpresa”
- Productividad – Detenimiento del servicio
- Marca – Impacto directo en la imagen (publicaciones)
- Despidos – Cese de actividad de altos cargos Ejecutivos

Costo de las APT

Distribución en 4 categorías de costos estimados asociados con APT / incidentes relacionados



Sponsored by IBM

Fuente: Independently conducted by Ponemon Institute LLC
Publication Date: May 2014

Panorama de amenazas a futuro

Ciber espionaje

Transición desde el robo o desvío de dinero a la recopilación de conocimiento

Internet de las cosas

50 millones de dispositivos de múltiples tipos, con información personal y un elevado grado de vulnerabilidad

Privacidad

La información personal será más codiciada por la delincuencia y la normativa será cada vez más exigente.

Ramsonware

Aumento exponencial de variantes de software de secuestro y expansión hacia los móviles y la nube.

Movilidad

La expansión del malware, la utilización como herramienta de pago (NFC) y el uso de las monedas virtuales convertirán la movilidad en un objetivo futuro de la delincuencia organizada.

Malware Windows

El malware para Windows afectará de forma masiva a múltiples tipos de dispositivos, no solo PC's y sirven para lanzar otros ataques.

Fuente: Threats Predictions McAfee Labs

Ciber Espionaje

Incremento de la frecuencia de ataques de ciber espionaje

Recopilación de Conocimiento

Los infiltrados de larga duración son recopiladores de información que pasan desapercibidos.
Los cibercriminales sofisticados cambiarán de ataques rápidos a recopilar información de manera eficiente.

Robo de dinero

Los recién llegados buscarán formas de robar dinero y anular a sus adversarios.

En 2013, hubo un total de 551 incidentes de ciber espionaje, incluyendo 306 con filtración de información confirmada.

87%	11%	1%	1%
Afiliados a un estado	Crimen Organizado	Competencia	Empleado desleal

Internet of Things

Los ataques a la Internet of Things se incrementarán rápidamente debido al hipercrecimiento del número de objetos conectados, la débil aplicación de la seguridad y el valor de la información contenida en dichos dispositivos.

50.000 millones de dispositivos

Número de dispositivos conectados a Internet en el mundo previstos en 2019.

Dispositivos IoT

Los ataques a los dispositivos IoT ya son algo habitual.

- Cámaras IP
- Contadores inteligentes
- Dispositivos de salud
- Dispositivos SCADA

Un reciente estudio de HP sobre IoT pone en cuestión la seguridad de 10 dispositivos muy populares:

70%	25	80%	90%	70%
Eran vulnerables	Fallos que comprometían la red	Contraseñas débiles	Contenían datos personales	Permitían identificar usuarios

Privacidad

La privacidad se mantendrá bajo amenaza en tanto los gobiernos y organizaciones sigan en los límites de los permitido en cuanto al acceso autorizado a la información personal.

110 millones de personas

Alrededor de 110 millones de ciudadanos de EEUU han visto comprometidos sus datos de alguna forma el año 2013.

Contraseñas

Los anticuados sistemas basados en roles y esquemas de contraseñas serán anulados por los atacantes malintencionados.

Regulaciones

Se va a producir un incremento en el alcance de las regulaciones y estándares sobre datos personales.

Biometría

La Biometría y la identificación en este contexto serán áreas de innovación y posiblemente los mejores indicadores de presencia.

Ransomware

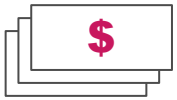
El Ransomware evolucionará en sus métodos de propagación, cifrado y objetivos.

2 millones de muestras

El número total de muestras de ransomware en los laboratorios de McAfee superó los 2 millones en el Q3 de 2014.

Almacenamiento en la nube

El Ransomware pasará a centrarse en servicios de almacenamiento en la nube, intentando acceder a las credenciales de forma que pueda infectar los datos.



$255,000 robados

Se identificó el robo de $225,000 en un solo mes en una única instancia de CryptoLocker.

Espacio móvil

Se prevé que las técnicas de Ransomware dirigidas a la copia de seguridad en cloud se extiendan a los dispositivos móviles.

Movilidad

Los ataques continuarán creciendo como la superficie de ataque de las nuevas tecnologías, y en tanto existan tiendas de aplicaciones móviles vulnerables.

Pagos Digitales

La adopción de tecnologías de pago por proximidad (NFC) para dispositivos móviles atraerá a los ciberladrones.

Malvertising

Las tiendas de App no confiables serán una fuente de malware móvil, facilitado por el “malvertising”

5MM muestras de malware 2014

Crecimiento malware móvil

16%

Q3 2014

112%

Q4 2013 –Q3 2014

Monedas virtuales

Se espera un incremento del Ransomware dirigido a dispostivos móviles utilizando las monedas virtuales como forma de pago del secuestro.

Kits de Malware para Móviles

La capacidad de crecimiento de los kits y código fuente de generación de malware hará más fácil a los cibercriminales atacar los dispositivos móviles.

Malware Windows

La vulnerabilidad Shellshock va a extenderlos ataques de malware a sistemas no Windows en el futuro.

22,487 IP's Atacantes

En los primeros 4 días después del anuncio de Shellshock, se detectaron 22,487 direcciones IP atacantes.

Shellshock

Los atacantes van a basarse en Shellshock para exfiltrar información, secuestrar sistemas corporativos, y asimilar spam bots.

Dispositivos

Dispositivos tales como routers, TV's, controladores industriales, sistemas de navegación, e infraestructuras críticas pueden contener esta vulnerabilidad.

Peligroso

Clasificado como 10/10 de severidad por la base de datos de vulnerabilidades de los EEUU.

5 Conclusiones

Conclusiones

La ciberseguridad es un riesgo relevante a considerar en todos los ámbitos de cada Organización.

Aspectos clave para la gestión de la ciberseguridad:

- Implicación de la Alta Dirección
- Vigilancia por los Supervisores y por los Mercados
- Tendencia natural a subestimar los impactos
- Programa de seguridad para mitigar los riesgos principales
- Verificación continua de las capacidades de ciberseguridad
- Seguimiento constante del mercado
- Revisión periódica del programa

¿ Preguntas ?

BBVA

Muchas Gracias !