Fuga de Información en los Siglos XIX y XXI

75.17 - IMPLANTACIÓN DE SISTEMAS
75.56 - ORGANIZACIÓN DE LA IMPLANTACIÓN Y EL MANTENIMIENTO

Grupo N°: 2

Integrantes:

- Stephanie Zurita
- Santiago Maraggi
- Yi Cheng Zhang
- Miguel Angel Schmidt
- María Inés Parnisari

Año y cuatrimestre: 2014 2°C

Introducción

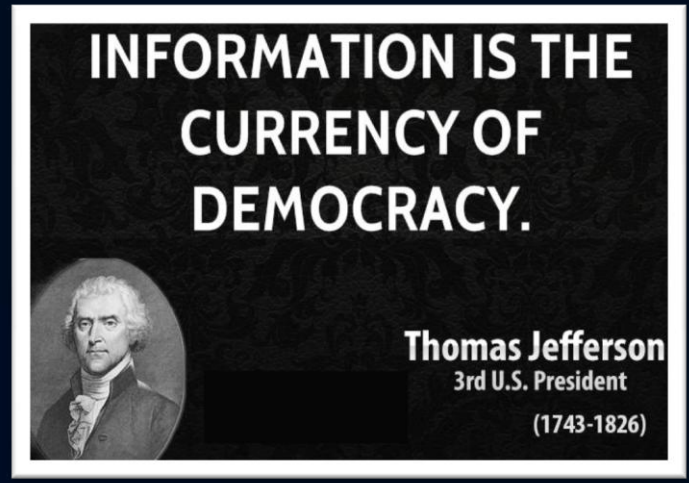
- La información como activo intangible de las organizaciones
- Fuga de información
- Riesgos existentes
- Tipos de controles

El activo más valioso de las organizaciones

- Activos tangibles (antiguamente)
- Activos intangibles (actualmente)

- La **información** se ha convertido en el activo más importante que posee cualquier organización → **protección de la información**

- Existen dos conceptos asociados a información:
  - ❑ **Confidencialidad** → autorización
  - ❑ **Privacidad** → garantía



La fuga de información (I)

- **Fuga de información** ocurre cuando algún dato que tiene valor para una organización pasa a manos ajenas, perdiendo la cualidad de confidencialidad que le fue asignada

- Las principales **causas** de fugas de información son:
  - ❑ Negligencia o desconocimiento
  - ❑ Ataques internos
  - ❑ Delincuentes informáticos

La fuga de información (II)

- Los **sistemas de información** capturan, procesan y almacenan información en una gran variedad de dispositivos

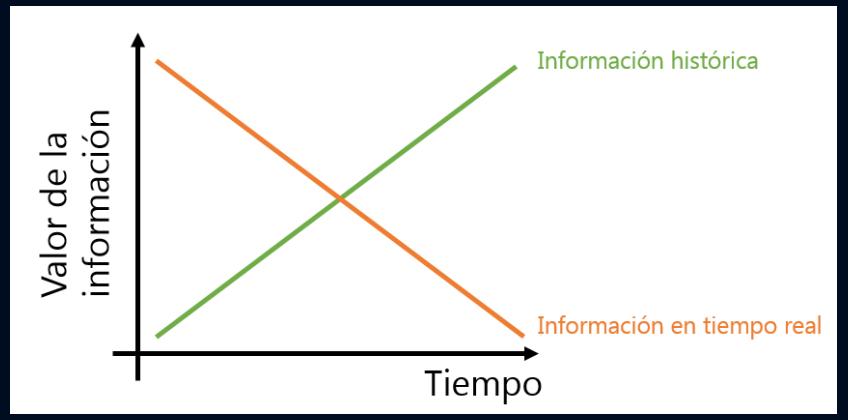
- Tipos de dispositivos:
  - ❑ Físicos
  - ❑ Electrónicos

- La clave para decidir cómo manejar la información:
  - ❑ Tipo de información
  - ❑ Nivel de confidencialidad
  - ❑ Dónde está almacenada

Se debe categorizar la información

La fuga de información (III)

- La información **pierde valor** a medida que pasa el tiempo



- Las organizaciones no desean almacenar información irrelevante

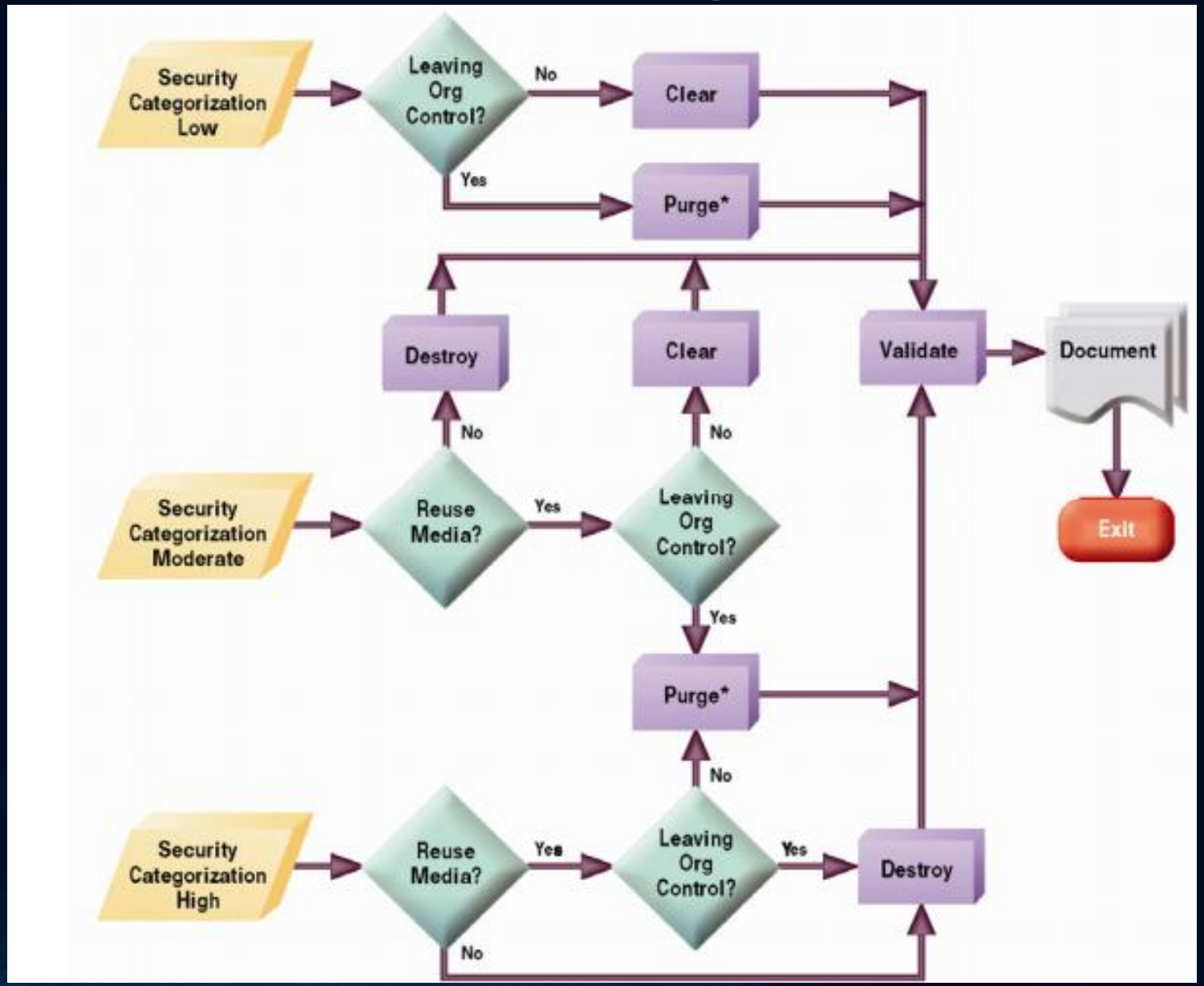
- *¿Cómo deshacerse de información de poco valor?*
  → Poco valor para nosotros
  → Mucho valor para otras personas / empresas

Cómo deshacerse de forma segura de información (I)

Existen cuatro categorías de mecanismos para deshacerse de información:

- **Desecho**: la información se elimina sin ningún tipo de tratamiento.
- **Limpieza**: la información se elimina de tal forma que se impide su recuperación mediante herramientas de recuperación de datos.
- **Purga**: la confidencialidad de la información se protege contra ataques de laboratorio.
- **Destrucción**: la información se elimina físicamente.

Cómo deshacerse de forma segura de información (II)

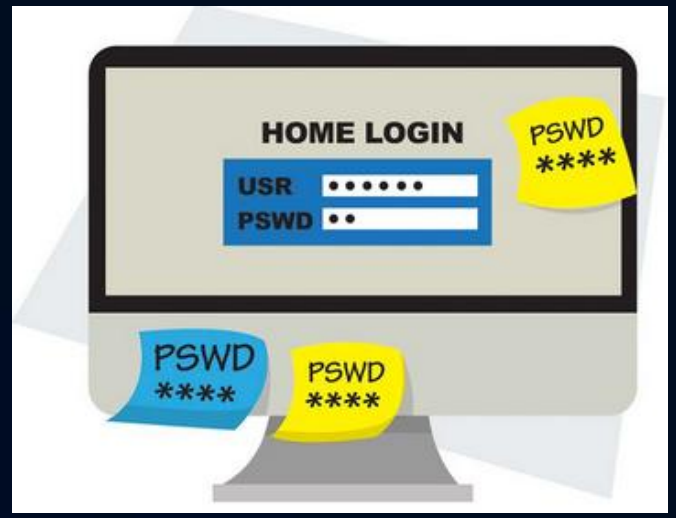


Riesgos existentes

Tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad

El riesgo tecnológico puede verse desde tres aspectos:

1. A nivel de la **infraestructura tecnológica** (hardware o nivel físico)
2. A nivel **lógico** (riesgos asociados a software, sistemas de información e información)
3. Riesgos derivados del **mal uso** de los anteriores factores, que corresponde al factor humano como un tercer nivel.



Tipos de controles para mitigar riesgos

Existen distintos tipos de controles, a saber:

- **Preventivos**: identifican el riesgo antes de que se produzca.
- **Detectivos**: se utilizan para detectar riesgos luego de que se materializan.
- **Correctivos**: ayudan a la investigación y corrección de las causas del riesgo.

Siglo XIX

LA INFORMACIÓN ENTRE MOSQUETES Y BAYONETAS

Introducción

- Revolución Industrial
- Innovación productiva, relevancia del inventor
- Política
  - Europa
  - América
  - África
- Administración de la propiedad intelectual
  - Cédulas Reales de Privilegio de Invención
  - Patentes de Invención
  - Propiedad Industrial

Revolución Industrial

Iniciada a mediados del Siglo XVIII

- Importancia de la técnica productiva
- Centralización poblacional
- Burguesía Industrial
- Ordenamiento social
- Liberalismo
- Iluminismo

Innovación productiva: El Inventor

De la sabiduría a la invención

- Búsqueda de mayor productividad en la producción de bienes industriales
- Revalorización del conocimiento técnico
- Creciente demanda por un mayor incentivo a la actividad de la invención
- Sofisticación y formalización del conocimiento técnico
- Rédito del inventor

Política

“Lo relativo al ordenamiento de la ciudad”.

- Propagación de estructuras e ideas de la Revolución Francesa
- Instauraciones de Repúblicas como Estados Nacionales
- Desintegración del Reino de Indias e independencia de regiones administrativas divididas en provincias
- Colonización de África. Expediciones científicas europeas y repartición de territorios continentales (Conferencia de Berlín)
- Doctrinas materialistas: liberalismo y socialismo

Administración de la Propiedad Intelectual

Entre la libertad y la privacidad

- Cédulas Reales de Privilegio de Invención
- Patente de Invención (principios S. XIX)
- Convenio de París (1883). Protección internacional de la Propiedad Industrial.
- Convenio de Berna (1886). Protección de los Derechos de Autor de obras literarias y artísticas (Dumas).

Mecanismos de Protección

- Esteganografía
- Criptografía
- Patentes de invención
- Cajas de seguridad

Esteganografía

Canal de información oculto

- Grecia, narraciones de Herodoto:
  - Tablilla grabada recubierta con cera
  - Mensaje en cabeza de esclavo rapado con pelo crecido.
- Antigua China: mensajes en seda, envueltos en cera y tragado por mensajeros.
- Giambattista della Porta S. XVI, mensaje en el huevo duro.
- Uso de tinta invisible sensible al calor (imperios griego y romano).

Criptografía

Significado del mensaje oculto.

- Método de la varilla (Escítala). Esparta, Imperio griego, siglo V, AC
- Máquina de rodillos de Thomas Jefferson (10 cilindros con el alfabeto coaxiales)
- Método Playfair, 1854 de Wheatsone. Método digráfico (caracter por caracter)
- Étienne Bazeries, 1890, variante de la máquina de Thomas Jefferson

Patentes de Invención

Este conocimiento es mío.

- Cédula Real de Privilegio de Invención
  - Otorgada por autoridad monárquica
  - Privilegio concedido
  - A criterio de la autoridad, entrega ocasional
- Opositores a la propiedad intelectual en el siglo XVIII (Thomas Jefferson y Benjamin Franklin) superados por coyuntura industrial
- Patente de Invención (1820) por presión de sectores liberales
- Convenio de París 1883 (Propiedad Industrial internacionalizada)
- Convenio de Berna 1886 (Derechos de Autor)

Cajas de Seguridad

La llave es la clave. Obstrucción física al elemento protegido.

- Los activos más importantes eran siempre tangibles
- El conocimiento tenía soportes físicos
- Utilización desde la época del imperio romano (cajas de hierro)
- Evolución técnica de cerrajes y blindajes durante el Siglo XIX
- Debilidad: factor humano y administración de las llaves
- Servicios tercerizados de guarda de bienes. Explosión del negocio a partir de la segunda mitad del siglo XIX

Siglo XIX – Riesgos (I)

- Riesgo a que otro patente el activo propio
- Comercialización de activo propio por parte de otras organizaciones
- Copia de patentes en el extranjero
- Robo de documentación

Siglo XIX – Riesgos (II)

- Información clave en manos del enemigo
- Pérdida de información
  - Siniestros

Siglo XIX – Casos reales (I)

- Guerra Civil Americana
  - Unión – Sustitución + Transposición
  - Confederados - Vigenère
- Cola-Cola – 1886
  - 2 únicos directivos tienen acceso a la fórmula

Siglo XIX – Casos reales (II)

- Automóvil
  - Auto moderno – 1885 – Henry Ford o Karl Benz?
- Radiografía
- Filmaciones o Imágenes en Movimiento
- Teléfono

Siglo XIX – Casos reales (III)

- Bombilla Eléctrica
- Telegrama Zimmermann
  - Interceptado y descifrado por criptógrafos

Siglo XXI

LA INFORMACIÓN COMO ACTIVO PRIMORDIAL

Introducción

- Economía basada en la información
  - Nuevos desafíos: manejar y procesar información de diversa índole, en grandes cantidades, a alta velocidad
- Información disponible de forma electrónica
  - Información personal, datos médicos, datos financieros
  - Espionaje informático

Eventos

- 2001: Nace **Wikipedia**
- 2004: Nacen **Gmail** y **Facebook**
- 2005: Nace **YouTube**
- 2006: Nace **WikiLeaks**
- 2007: Apple lanza el teléfono **iPhone**
- 2013: Se publican secretos de varios programas de la NSA (*National Security Agency*)

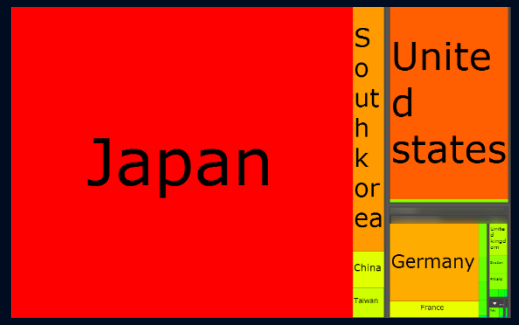
- 2014: **Divulgación de fotos privadas** de 26 celebridades mediante la plataforma iCloud de Apple.
  - La vulnerabilidad “Heart Bleed” encontrada en la librería OpenSSL, que podía ser utilizada para obtener datos sensibles como contraseñas.

Amenazas

- Usuarios y accesos no autorizados
- Programas maliciosos que roban información
- Errores de programación
- Desastres no previstos, catástrofes naturales, fallos de hardware
- Robo de información

Mecanismos de defensa

- Registro de patentes



- Controles informáticos
  - Software desarrollado siguiendo estándares de seguridad (criptografía)
  - Controles físicos sobre el hardware
  - Políticas de contraseñas y perfiles de usuario
  - Monitoreo de tráfico en las redes
  - Uso de software de protección
  - Creación de *backups* periódicos

Mecanismos de defensa (cont.)

- Auditoría de operaciones
- Normas de control
  - Normas ISO 27000, especialmente dedicada a seguridad de la información
- Uso de nombres en clave para los proyectos

Siglo XXI – Riesgos (I)

- Personal deshonesto con autorizaciones de acceso sensibles
- Robo, alteración y/o pérdida de información (políticas inapropiadas)
- Espionaje industrial
- Dependencia de los sistemas informáticos

Siglo XXI – Riesgos (II)

- Mal administración de perfiles de usuarios y/o contraseñas
- Dependencia de empleados claves
- Generación de información residual
- Siniestro del soporte físico de la información

Siglo XXI – Casos reales (I)

- 2001: espionaje industrial de la década: implicó a dos empresas rivales en bienes de consumo, “Unilever” y “Procter & Gamble”.

- 2002: Este caso muestra como el espionaje industrial puede convertirse en un problema de seguridad nacional. La compañía sueca Ericsson se vio envuelta por sorpresa en un incidente diplomático.

Siglo XXI – Casos reales (II)

- 2004: se descubrió el primer caso de violación a la ley HIPAA (Health Insurance Portability and Accountability Act), cuando un empleado de una asociación de enfermos de cáncer utilizó información de pacientes para obtener tarjetas de crédito.

- 2005: empleados de un hospital fueron descubiertos mientras obtenían información de la internación por maternidad de la cantante pop Britney Spears.

Siglo XXI – Casos reales (III)

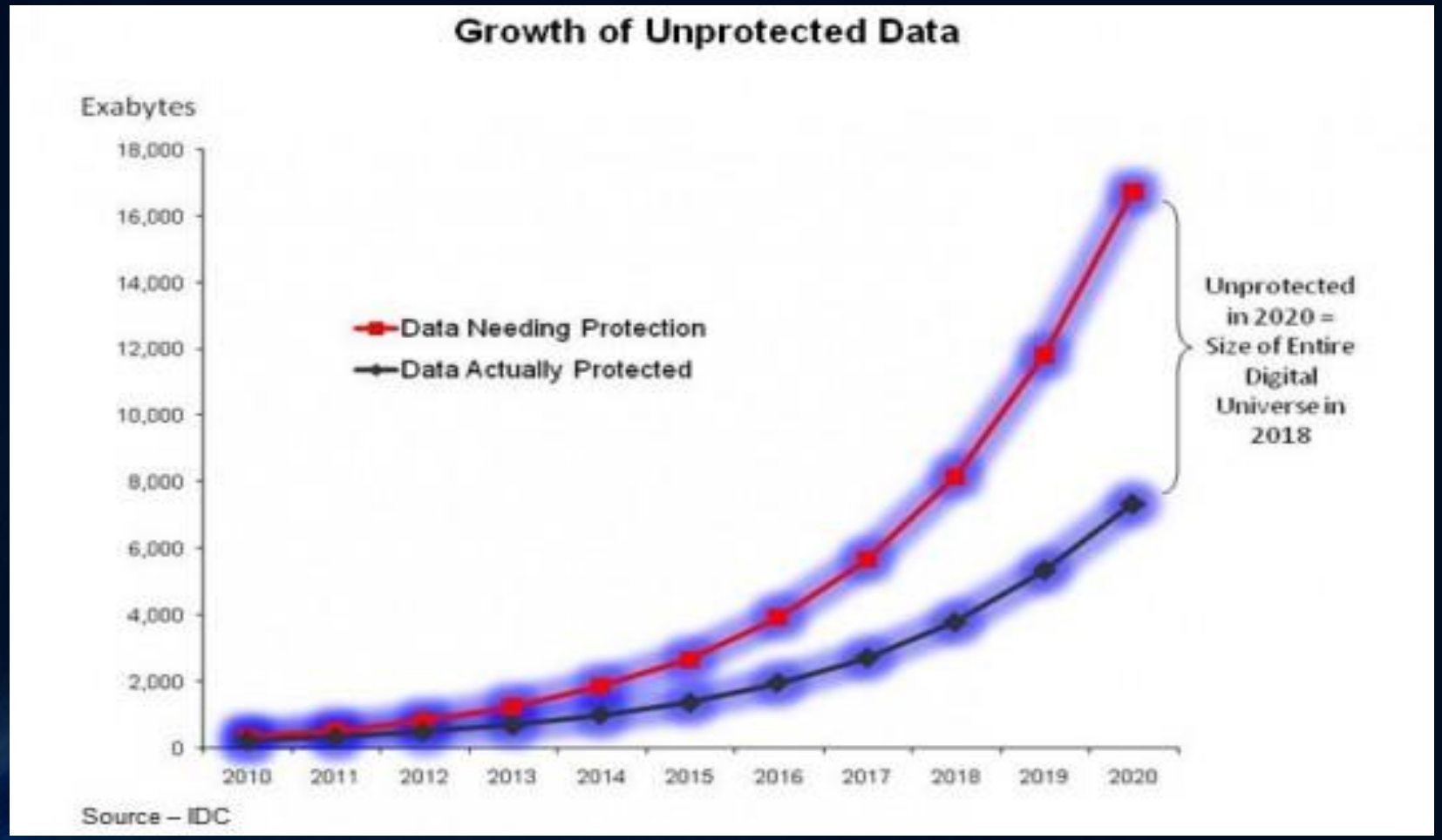
- 2005: se produjo la fuga de información confidencial sobre centrales nucleares en Japón, a través de Internet desde un ordenador infectado por un virus.

- 2007: el sitio global de búsquedas laborales Monster sufrió el robo de 1,6 millones de datos con información personal de los usuarios registrados. Los atacantes ingresaron a las bases de datos con contraseñas que habían sido obtenidas previamente mediante un troyano.

Siglo XXI – Casos reales (IV)

- 2009: la red social Tuenti fue afectada por el robo de 4.000 cuentas de usuario y sus contraseñas, por parte de un atacante enojado con la empresa.
- 2010: Google detectó que había sido víctima de un ataque desde China, que robó información de su propiedad intelectual.
- 2014: Edward Snowden revela cómo la Casa Blanca y sus organismos espían las comunicaciones en Internet.

Siglo XXI – Información sin protección



Conclusiones

Conclusiones

- La amenaza más grande para las organizaciones probablemente no sean los ataques de terceros, ni los empleados maliciosos, sino los empleados descuidados que de forma inintencionada divulgan información sensible
- Una combinación de protección tecnológica, políticas y procedimientos actualizados, y educación de los usuarios deberían contribuir a paliar los efectos que causan estas fugas

Conclusiones (cont.)

- Procedimiento básico para desarrollar una estrategia de protección:
  - ✓ Clasificar la información a proteger
  - ✓ Entender los datos que se manejan
  - ✓ Establecer políticas sobre el manejo de la información
  - ✓ Capacitar al personal en las herramientas
  - ✓ Implementar seguridad a nivel físico
- No debe olvidarse de ejecutar revisiones periódicas, para mantener las políticas actualizadas y en conformidad con los requisitos y las tendencias tecnológicas

Conclusiones (cont.)

- A pesar de que los ataques maliciosos son una minoría, no deberían ser ignorados
- Existen múltiples vías de escape de información que deben ser monitoreadas
- No existen soluciones que protejan los activos intangibles de forma 100% segura, se puede minimizar la probabilidad de que ocurran pérdidas mediante la aplicación de varios métodos complementarios

Fin

¿Preguntas?

Muchas gracias !!!