IBM Data Governance

Consideraciones y Regulaciones de Seguridad

Índice

- **Amenazas y Riesgos para los Datos**
- **Normativas, Regulaciones y Buenas Prácticas**
- **5 Acciones Clave para Proteger los Datos**

Índice

- **Amenazas y Riesgos para los Datos**
- **Normativas, Regulaciones y Buenas Prácticas**
- **5 Acciones Clave para Proteger los Datos**

Amenazas y Riesgos para los Datos

- Existe mucha literatura sobre el hacking y los hackers presentando en múltiples una visión glamorosa o “buenista” sobre los mismos.
- Múltiples denominaciones (en muchos casos ficticias o confusas): Hackers, Crackers, piratas informáticos, lamers, script kiddies, phreakers, etc.

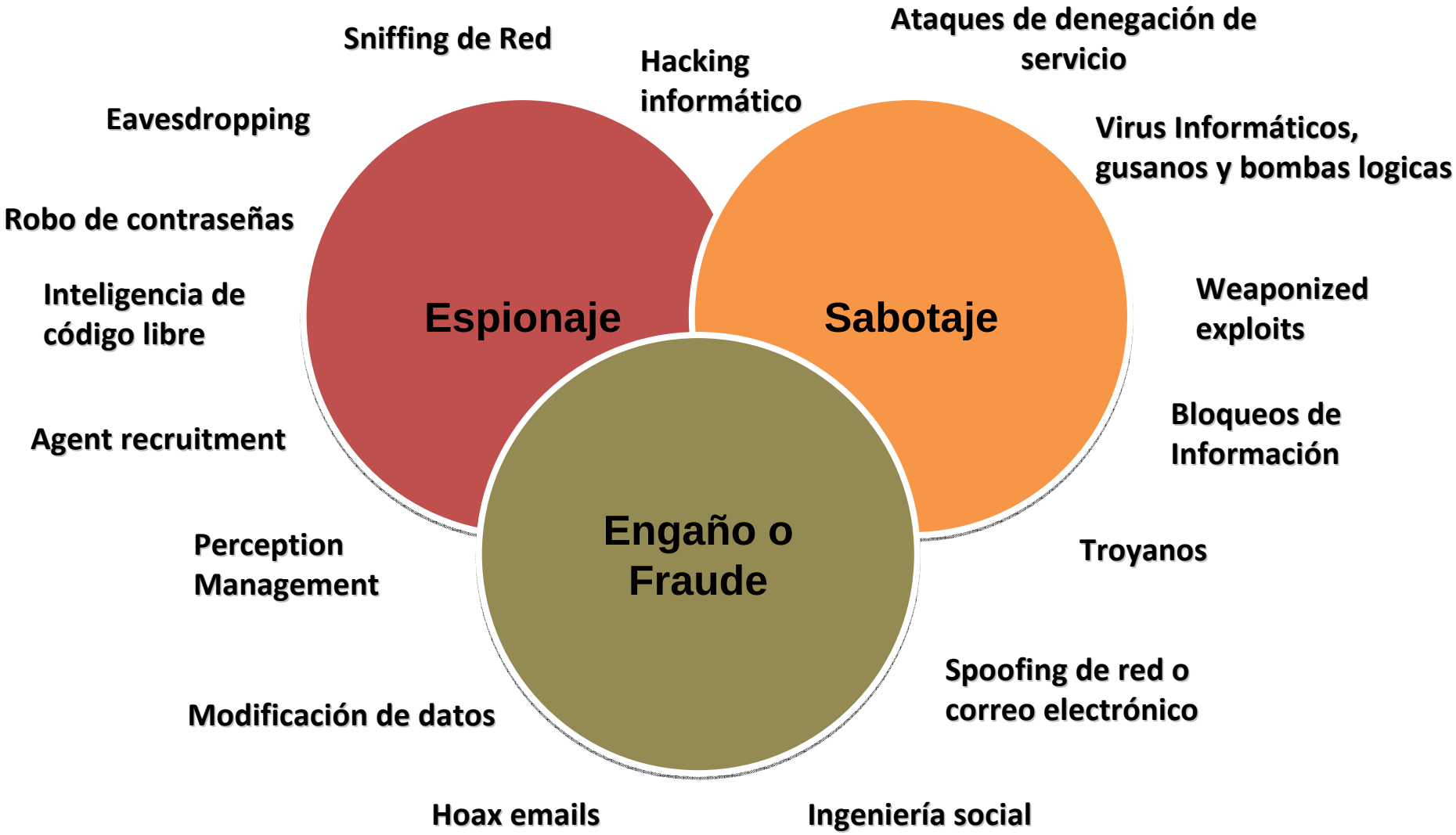
Amenazas y Riesgos para los Datos

- En la actualidad, a parte de los perfiles “clásicos” de atacantes, la principal preocupación son delincuentes informáticos, en muchos casos organizados en mafias que utilizan las técnicas de hacking para cometer delitos como robos, fraudes, etc.
- Además, se ha “profesionalizado” en negocio del crimen informático pudiendo “subcontratar” estas actividades.
- Disponen cada vez de mas y mejores herramientas.

Amenazas y Riesgos para los Datos

- Por último, no nos olvidemos de la causa mas frecuente de incidentes: El error humano.

Amenazas y Riesgos para los Datos



Amenazas y Riesgos para los Datos

- **Cadena de tiendas americana.**
- **En 2007 se publica el incidente, pero lo primeros robos de información se producen en 2003!!.**
- **Características del Incidente:**
  - 95.000.000 millones de usuarios afectados.
  - 45.000.000 millones de tarjetas de crédito robadas.
  - Usuarios de Estados Unidos, Puerto Rico, Canadá, Reino Unido e Irlanda.
  - Números de Tarjetas de Crédito, números de carné de conducir, números de identificación entre otros.
- **Se contrata a IBM para la confirmación del incidente así como para establecer e implementar un plan de seguridad en la compañía.**
- **Consecuencias conocidas:**
  - Disculpa pública del presidente a los clientes.
  - Apertura de numerosas causas judiciales contra la compañía y necesidad de llegar a un acuerdo con todos los afectados.
  - Establecimiento de líneas de atención a los clientes específicas para gestionar el incidente
  - Contratación de mas de 50 expertos en seguridad dedicados al estudio del incidente y a la definición e implementación de nuevas medidas de seguridad.
  - La cadena se ve obligada a recomendar a todos los clientes afectados la necesidad de revisar sus cuentas en busca de posibles movimientos fraudulentos.
  - Daños a la imagen de la marca, Prensa.
  - Pago de Monitorización de Tarjetas.
  - Multa de $800.000
  - ¿Compensación a los Bancos por re-emisión de tarjetas?
- **En Resumen:**
  - **Problemas con Clientes, Justicia, Accionistas, Bancos, Marcas.**
  - **Algunas fuentes hablan de $1.000.000.000 de impacto**

Amenazas y Riesgos para los Datos

Índice

- **Amenazas y Riesgos para los Datos**
- **Normativas, Regulaciones y Buenas Prácticas**
- **5 Acciones Clave para Proteger los Datos**

Normativas Regulaciones y Buenas Prácticas

Normativas, Regulaciones y Buenas Prácticas
PCI-DSS

- Estándar de la Industria de medios de pago, elaborado por el PCI Standards Council (www.pcisecuritystandards.org) fundado por American Express, Discover Financial Services, JCB, MasterCard Worldwide y Visa International.

- PCI DSS se compone de 12 requerimientos agrupados en 6 grupos denominados “Objetivos de Control”. A su vez, cada uno de los 12 requerimientos se descompone en sub-requerimientos de mayor detalle.
- Debe distinguirse entre el estándar y el programa

- Desarrollar y Mantener una Red Segura
- Proteger los Datos de los Tarjetahabientes
- Mantener un Programa de Gestión de Vulnerabilidades
- Implementar Medidas Sólidas de Control de Acceso
- Monitorizar y Probar Regularmente las Redes
- Mantener una Política de Seguridad de la Información

Normativas, Regulaciones y Buenas Prácticas
LOPD

- Clasifica los Datos en tres niveles:
  - Bajo: Nombre, dirección, …
  - Medio: infracciones administrativas o penales, administraciones tributarias, seguridad social, personalidad del individuo, morosidad.
  - Alto: violencia de genero, sexo, religión, salud, ideas políticas, religiosas, afiliación sindical, creencias, pruebas policiales recabadas sin consentimiento.
- Y para cada nivel establece una serie de controles que deben ser implementados:
  - Bajo: identificación inequívoca, cambio de contraseña antes de un año, gestión de soportes, control de acceso lógico con perfiles, documento de seguridad, definición de funciones del personal.
  - Medio: registro de incidencias, control de acceso físico, bloqueo ante intento reiterado de acceso, inventario y gestión de soportes (sin cifrar cuando salen de la oficina), auditoria bianual y un responsable de seguridad.
  - Alto: Cifrado en las comunicaciones publicas o inalámbricas, registro de acceso durante dos años y con informes, copias de respaldo fuera de la ubicación, gestión y distribución de soportes cifrando cuando salen de la oficina,
- Pueden suponer cuantiosas sanciones:
  - Leves: no atender la solicitud de un interesado, no inscribir un fichero, etc → 600€ a 60.000€
  - Graves: Engañar en la finalidad, negativa a facilitar información al interesado → 60.000€ a 300.000€
  - Muy graves: La recogida de datos de forma engañosa y fraudulenta, cesión de datos no permitidas, no cesar en el tratamiento después de un aviso → 300.000€ a 600.000€

Normativas, Regulaciones y Buenas Prácticas
SOXs

- Aplica a todas las empresas que coticen el la bolsa americana y sus filiales en el mundo.
- Responsabilidad a los gestores de la veracidad de los estados contables de la empresa.
- Aplica verificando que los procesos relativos a los estados contables son correctos: autenticación individualizada/personal, registros de accesos, etc…

Normativas, Regulaciones y Buenas Prácticas Protección de las Infraestructuras Críticas

- El Plan Nacional de Protección de Infraestructuras Críticas define como Infraestructuras Críticas:

"Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".

- El Plan Nacional de Protección de Infraestructuras Críticas contempla la inclusión de éstas, en 12 Sectores estratégicos, subdivididos a su vez en Subsectores, Ámbitos y Segmentos:

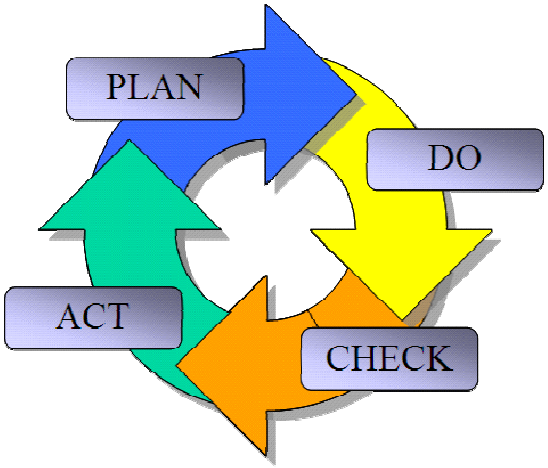
Administración
Alimentación
Energía
Espacio
Sistema Financiero y Tributario
Agua
Industria Nuclear
Industria Química
Instalaciones de Investigación
Salud
Tecnologías de la Información y las Comunicaciones
Transporte

Normativas, Regulaciones y Buenas Prácticas ISO 27002 y 27001

ISO/IEC 27002:2005

International Organization for Standardization

International Electrotechnical Commission



ISO/IEC 27001:2005

Índice

- **Amenazas y Riesgos para los Datos**
- **Normativas, Regulaciones y Buenas Prácticas**
- **5 Acciones Clave para Proteger los Datos**

5 Acciones Clave para Proteger los Datos

Descubrir la Ubicación de los Datos Sensibles y Clasificarlos

Aplicar Máscaras a los Datos en Entornos de no Producción

Eliminar Datos no Estructurados Sensibles de Documentos

Cifrar las Bases de Datos

Monitorizar la Base de Datos y Analizar las Vulnerabilidades

Cumplimiento, Normativa y Buenas Prácticas

5 Acciones Clave para Proteger los Datos

Descubrir la Ubicación de los Datos Sensibles y Clasificarlos

- ✓*La organización debe tener un inventario completo de los datos sensibles, sus repositorios, sus flujos de comunicación y las aplicaciones que los procesan.*
- ✓*La información deberá ser clasificada conforme a la normativa interna de seguridad. De igual forma deberán conocerse y documentarse las regulaciones que aplican a dichos datos.*
- ✓*Debe establecerse una normativa de clasificación interna que cubra en la medida de lo posible la mayor parte de requerimientos regulatorios.*
- ✓*En el proceso de búsqueda de la información sensible podemos apoyarnos en herramientas que automatizan el proceso y permiten encontrar relaciones entre los datos.*

InfoSphere Discovery

5 Acciones Clave para Proteger los Datos

Aplicar Máscaras a los Datos en Entornos de no Producción

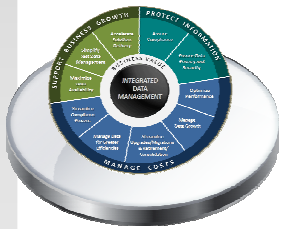
- ✓*Es muy frecuente encontrar datos reales o de producción en entornos no productivos, esto supone un riesgo serio dado que a estos entornos acceden un número mucho mayor de personal interno y externo y no suelen estar dotados de las mismas de protección que los entornos de producción.*
- ✓*Estos entornos han proliferado mucho en los últimos tiempos encontrándose entornos de desarrollo, pruebas, pre-producción, formación, certificación, etc, lo que complica significativamente el problema.*
- ✓*La mejor protección es que los datos de estos entornos no sean datos reales, por lo que deben aplicarse procesos de desnaturalización/disociación/enmascaramiento de los datos de producción para garantizar la seguridad.*
- ✓*Para automatizar este proceso y garantizar la integridad referencial se pueden emplear herramientas.*

Optim Data Privacy

5 Acciones Clave para Proteger los Datos

Eliminar Datos no Estructurados Sensibles de Documentos

- ✓*Uno de los grandes problemas es la existencia de Información sensible no estructurada en documentos y ficheros ofimáticos.*
- ✓*Esto supone un gran riesgo de fuga, robo y pérdida accidental de información dado que estos ficheros no disponen de mecanismos de control de acceso, ni cifrado ni registro.*
- ✓*Los accesos a los datos deben realizarse siempre através de las aplicaciones no permitiéndose ni las "queries" directas a la BBDD ni las exportaciones de datos a ficheros locales.*
- ✓*Para aquellos casos donde haya una justificación de negocio pueden emplearse herramientas para eliminar la información sensible de los documentos.*



Optim Data Redaction

5 Acciones Clave para Proteger los Datos

Cifrar las Bases de Datos

- ✓*La protección de las BBDD de producción es una medida clave para mitigar los riesgos de seguridad asociados a los datos y cumplir con varias de las regulaciones existentes.*
- ✓*La criptografía debe ser robusta basada en algoritmos de cifrado de clave simétrica o asimétricas y altamente contrastados.*

Database Encryption Expert

5 Acciones Clave para Proteger los Datos

Monitorizar la Base de Datos y Analizar las Vulnerabilidades

✓*El registro de acceso a las bases de datos y a cualquier tipo de datos sensibles es un medida fundamental para cumplir con las regulaciones existentes, exigir responsabilidades, disuadir a atacantes internos (insiders) y poder tomar acciones legales en caso de ataque contra la organización.*

✓*Para ello es imprescindible implementar una política de usuarios personales, es decir no genéricos ni compartidos, que permita identificar unívocamente a los usuarios.*

✓*Los registros de acceso deberán ser adecuadamente protegidos y el acceso a los mismos debe ser estrictamente limitado a las personas imprescindibles.*

Guardium®
SAFEGUARDING DATABASES™