GOBERNANZA Y GESTIÓN SEGURA DE LOS DATOS

OWASP LATAM 2016 LATIN AMERICA TOUR

Honduras, 04/04/2016

Fredis Dubal Medina Escoto
fredis.medina@owasp.org
Skype: fredis.medina

¿Qué es la gobernanza delos datos?

Definiciones:

1. Se refiere a la **gestión global de la disponibilidad**, **facilidad de uso**, **la integridad** y la **seguridad de los datos** empleados en una empresa.

   No se refiere a la **gestión táctica de los datos**, ni es un área restringida al departamento de IT.

2. La práctica de **organizar e implementar políticas**, procedimientos y normas para el uso eficaz **de los activos informacionales**, ya sean estructurados o no estructurados, de una organización.

¿Qué es la gobernanza delos datos?

3. El **proceso de toma de decisiones** que **prioriza las inversiones**, **asigna recursos**, y **mide los resultados** para asegurar que los **datos se gestionan y despliegan en la forma adecuada** para dar apoyo a las necesidades del negocio.

¿Requisitos de una gobernanza de datos?

A. **Accesible:** tiene que garantizar que las personas pueden acceder a los datos que necesitan en el momento preciso, encontrándolos en condiciones de formato adecuadas.

B. **Seguro:** debe ser posible garantizar que sólo las personas autorizadas pueden acceder a los datos, mientras que el resto no tiene esta posibilidad en ningún momento ni bajo ninguna circunstancia.

C. **Consistente:** con datos sin duplicidades, libres de redundancias y en condiciones de racionalización de cada versión de los mismos existente.

¿Requisitos de una gobernanza de datos?

D. **De calidad:** en términos no sólo de exactitud, sino también de conformidad con las normas acordadas.

E. **Auditable:** capaz de explicar el origen de los datos y de aportar información suficiente sobre su uso y propósito.

¿Porqué se deben proteger los datos?

Los personales:

1. **Declaración Universal de Derechos Humanos, desde 1948; artículo 12:**

   "*Nadie será objeto de* ***injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia****, ni de ataques a su honra o a su reputación. Toda persona tiene* ***derecho a la protección de la ley contra tales injerencias o ataques***"

http://www.un.org/es/documents/udhr/

¿Porqué se deben proteger los datos?

2. **La OCDE publicó las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales; desde 1980.**

   …"**Principio de salvaguardia de la seguridad:**
   Se **emplearán salvaguardias razonables de seguridad para proteger los datos personales** contra riesgos, tales como **pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos**"...

Organización para la Cooperación y Desarrollo Económicos
http://www.oecd.org/

Según OWASP Top 10 – 2013:

"**A6–Exposición de datos sensibles:**

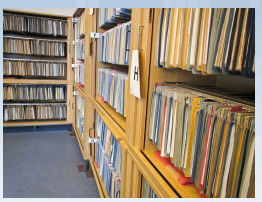
Muchas aplicaciones web **no protegen adecuadamente datos sensibles** tales como números de tarjetas de crédito o credenciales de autenticación.

Los atacantes pueden robar o modificar tales datos para llevar a cabo fraudes, robos de identidad u otros delitos. **Los datos sensibles requieren de métodos de protección adicionales** tales como el **cifrado de datos**, así como también de **precauciones especiales en un intercambio de datos con el navegador**."

¿El antes y presente de la gestión de los datos?

Antes:

1. **Diversas fuentes con controles físicos.**
2. **No podían ser accedidos en línea.**
3. **La versión en papel quizá ofrecía "mayor seguridad".**



Presente:

1. **La digitalización de datos, la computación en nube, movilidad y la globalización ha aumentado los riesgos para los datos.**
2. **Se requieren mecanismos y estrategias para garantizar la seguridad de los datos.**

OWASP Open Web Application Security Project

Gobierno y Gestión

Dos disciplinas que engloban **diferentes tipos de actividades**, requieren **diferentes estructuras organizativas** y sirven a **diferentes propósitos**:

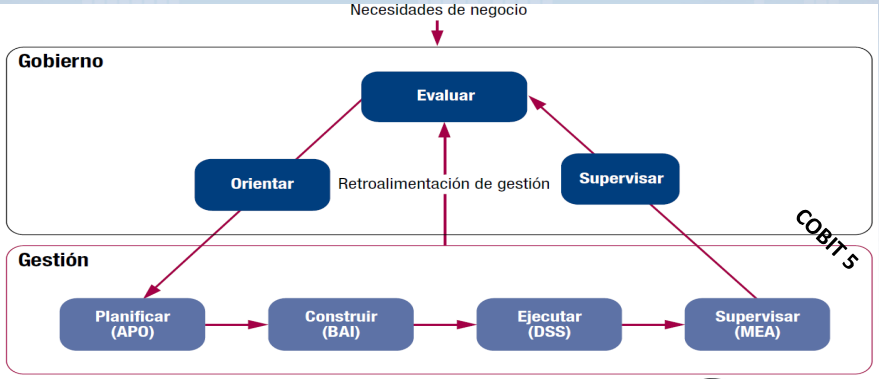
- **Gobierno:** Asegura que se evalúan las **necesidades, condiciones y opciones de las partes interesadas** para determinar que se **alcanzan las metas corporativas equilibradas y acordadas**; estableciendo la **dirección a través de la priorización** y la **toma de decisiones**; y **midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas**.

5. Separar el Gobierno de la Gestión
COBIT 5

OWASP Open Web Application Security Project

Gobierno y Gestión

- **Gestión:** Planifica, construye, ejecuta y controla actividades **sincronizadas con la dirección establecida** por el cuerpo de gobierno para alcanzar las **metas** empresariales.



OWASP Open Web Application Security Project

¿Que debe hacer el gobierno para proteger los datos?

No todas las instituciones tienen un sistema de Gestión de Seguridad de la Información como lo establece el ISO 27000; http://iso27000.es/iso27002.html

¿Porqué?

1. No hay regulación en el país.
2. No han tenido impactos (financieros, imagen, etc.)
3. No han sido sancionadas.
4. No han sufrido ataques.

OWASP Open Web Application Security Project

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

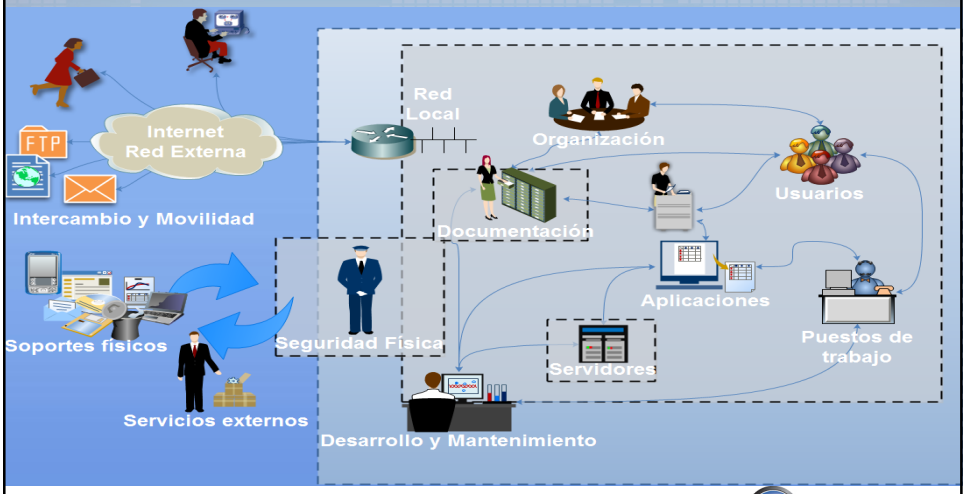
¿Que debe hacer el gobierno para proteger los datos?

Datos que deben ser protegidos:

1. Los procesados y almacenados en computadoras y servidores.
2. Transmitidos por medios electrónicos (correo, etc.).
3. Contraseñas, números de tarjetas de crédito, registros médicos, e información personal.
4. Impresos o escrito en papel.
5. Enviados por fax.
6. Almacenados en cintas, discos ópticos y magnéticos.
7. Almacenados en dispositivos móviles.
8. Hablados en conversaciones.

OWASP Open Web Application Security Project

¿Que debe hacer el gobierno para proteger los datos?

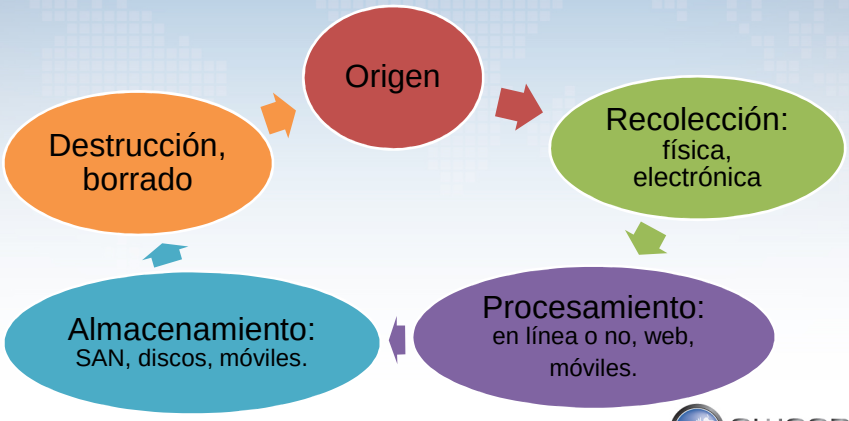


http://www.iso27002.es/

OWASP Open Web Application Security Project

¿Que debe hacer el gobierno para proteger los datos?

Ciclo de Vida de los Datos:



OWASP Open Web Application Security Project

Corresponde al gobierno

Establecer:

1. Políticas sobre seguridad y riesgos de los datos.
2. Marcos de referencias para la gobernanza.
3. Entrega de valor a las partes interesadas.
4. Disponer los recursos (Financieros, Información, RRHH, Infraestructura) necesarios.
5. Transparencia y ética con las partes interesadas.
6. Principios.

OWASP Open Web Application Security Project

Corresponde al gobierno

¿Por qué una Política de Seguridad de la Información de Alto Nivel?

- ✓Garantizar la continuidad de los negocios de una organización, a través de la preservación de los tres dominios de una información:
  - ✓ Confidencialidad
  - ✓ Integridad
  - ✓ Disponibilidad

OWASP Open Web Application Security Project

Corresponde al gobierno

¿Por qué una Política de Seguridad de la Información de Alto Nivel?

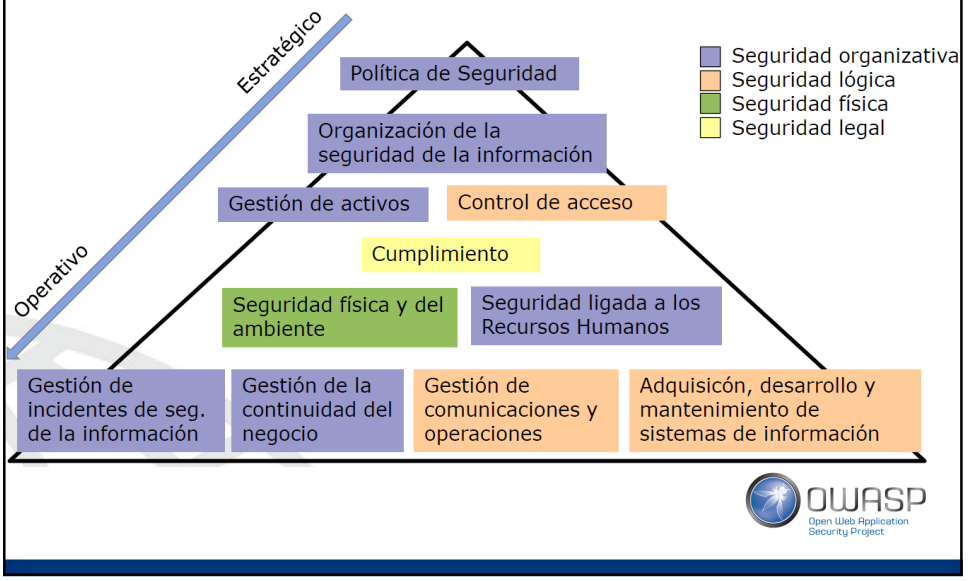
Principales amenazas:

- ✓ Acceso no autorizado.
- ✓ Usuarios desleales.
- ✓ Espionaje industrial.
- ✓ "Hackers".
- ✓ Fraude.
- ✓ Persecución y observación de empleados clave.
- ✓ Robo de notebooks, Smartphone.
- ✓ etc.

OWASP Open Web Application Security Project

Corresponde al gobierno

Norma ISO de Seguridad



OWASP Open Web Application Security Project

¿Que corresponde gestionar para proteger los datos?

Según el ISO 27002:

- ✓ **Dominio: 18. Cumplimiento;**
- ✓ **Objetivo: 18.1 Cumplimiento de los requisitos legales y contractuales;**
- ✓ **Actividades de control del riesgo:**

18.1.3 Protección de los registros de la organización: **Los registros se deberían proteger** contra **pérdidas**, **destrucción**, **falsificación, accesos y publicación no autorizados** de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

18.1.4 Protección de datos y privacidad de la información personal: **Se debería garantizar la privacidad y la protección de la información personal identificable** según requiere la legislación y las normativas pertinentes aplicables que correspondan.

18.1.5 Regulación de los controles criptográficos: **Se deberían utilizar controles de cifrado de la información** en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

OWASP Open Web Application Security Project

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

¿Que corresponde gestionar para proteger los datos?

Minimizar fuga de datos:

1. Datos en reposo (almacenada).
2. Datos en movimiento (red).
3. Datos en uso (equipo de usuario).

Uso de soluciones del tipo DLP (Data Loss Prevention)

Prevenciones: Según Owasp Top 10.

1. Considerar las amenazas de **atacante interno o usuario externo**; **cifrando los datos sensibles almacenados o en tráfico**.
2. **No almacene datos sensibles innecesariamente**. Descártelos apenas sea posible. Datos que no se poseen no pueden ser robados.

OWASP Open Web Application Security Project

¿Que corresponde gestionar para proteger los datos?

Prevenciones: Según Owasp Top 10.

3. Aplicar **algoritmos de cifrado fuertes y estándar**, así como **claves fuertes y gestiónelas de forma segura**.
4. Asegúrese que las **claves se almacenan con un algoritmo especialmente diseñado para protegerlas**.
5. **Deshabilite el autocompletar en los formularios que recolectan datos sensibles**. Deshabilite también el **cacheado de páginas que contengan datos sensibles**.

OWASP Open Web Application Security Project

Corresponde a la gestión

Alinear, Planificar y Organizar

- **APO01** Gestionar el Marco de Gestión de TI
- **APO02** Gestionar la Estrategia
- **APO03** Gestionar la Arquitectura Empresarial
- **APO08** Gestionar las Relaciones
- **APO09** Gestionar los Acuerdos de Servicio
- **APO10** Gestionar los Proveedores

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Alinear, Planificar y Organizar

- **APO04** Gestionar la Innovación
- **APO05** Gestionar Portafolio
- **APO06** Gestionar el Presupuesto y los Costes
- **APO07** Gestionar los Recursos Humanos
- **APO11** Gestionar la Calidad
- **APO12** Gestionar el Riesgo
- **APO13** Gestionar la Seguridad

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Construir, Adquirir e Implementar

- **BAI01** Gestionar los Programas y Proyectos
- **BAI02** Gestionar la Definición de Requisitos
- **BAI03** Gestionar la Identificación y la Construcción de Soluciones
- **BAI08** Gestionar el Conocimiento
- **BAI09** Gestionar los Activos
- **BAI010** Gestionar la Configuración

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Construir, Adquirir e Implementar

- **BAI04** Gestionar la Disponibilidad y la Capacidad
- **BAI05** Gestionar la Introducción de Cambios Organizativos
- **BAI06** Gestionar los Cambios
- **BAI07** Gestionar la Aceptación del Cambio y de la Transición

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Según COBIT 5

OWASP Open Web Application Security Project

Corresponde a la gestión

Mejora Continua a la Seguridad de los Datos

OWASP Open Web Application Security Project

Corresponde a la gestión

Finalmente: Lista de chequeo de la gestión de datos

1. **Autoridad de la toma de decisiones y definición de políticas y procedimientos:** **asignar niveles apropiados de autoridad a los administradores de datos**, definiendo el alcance y las limitaciones de esa autoridad de forma proactiva.

2. **Estándares:** adoptar y hacer cumplir las políticas y procedimientos encuadradas en un plan de gestión de datos, que debe recogerse por escrito para asegurar que todo el **mundo entiende la importancia de la calidad de los datos y la preservación de su seguridad**.

3. **Inventarios de datos:** inventariar **todos los datos que requieren de protección, manteniendo este inventario actualizado con información sobre todos los registros sensibles y sistemas de datos, previamente clasificados en función de su prioridad y criticidad**.

OWASP Open Web Application Security Project

Corresponde a la gestión

Finalmente: Lista de chequeo de la gestión de datos

4. **Gestión del contenido de los datos:** gestionar el contenido de los datos para justificar la recopilación de datos sensibles, optimizar los procesos de gestión de datos **y asegurar el cumplimiento con las regulaciones estatales y locales**.

5. **Gestión de registros de datos:** especificar las actividades de gestión y de usuario adecuados relacionados con el manejo de datos para proporcionar a **los administradores de datos y usuarios las herramientas adecuadas para el cumplimiento de las políticas de seguridad de la organización**.

6. **Calidad de datos:** asegurarse de que los datos son exactos, relevantes, consistentes, actualizados y completos para los fines previstos. La clave para el mantenimiento de datos de alta calidad es un enfoque proactivo de la gestión de los mismos, que **requiere del establecimiento y actualización periódica de las estrategias para la prevención, detección y corrección de errores y mal uso de los datos.**

Corresponde a la gestión

Finalmente: Lista de chequeo de la gestión de datos

7. **Acceso de datos:** **definir y asignar niveles diferenciados de acceso a los datos a las personas según sus funciones y responsabilidades**. Resulta fundamental para evitar el acceso no autorizado y minimizar el riesgo de violaciones de datos.

8. **Seguridad de datos y gestión de riesgos:** garantizar **la seguridad de los datos confidenciales y personales identificables y mitigar los riesgos de la divulgación no autorizada de estos datos.** Este aspecto debe considerarse como altamente prioritario para la consecución de un plan de gobierno de datos eficaz.

Corresponde a la gestión

Sin tiempo para planear

"Deprisa… tenemos un plazo apretado. No hay tiempo para planear, sólo comenzar a escavar"

OWASP Open Web Application Security Project

¡¡¡Muchas gracias por su atención!!!

OWASP Open Web Application Security Project