Auditorías de Seguridad: revisión como método de prevención

Vicente Aguilera Díaz
Internet Security Auditors, S.L.

CONTENIDO

1. Protección de la información

2. Auditorías de seguridad

3. Implantación de un SGSI

1. PROTECCIÓN DE LA INFORMACIÓN

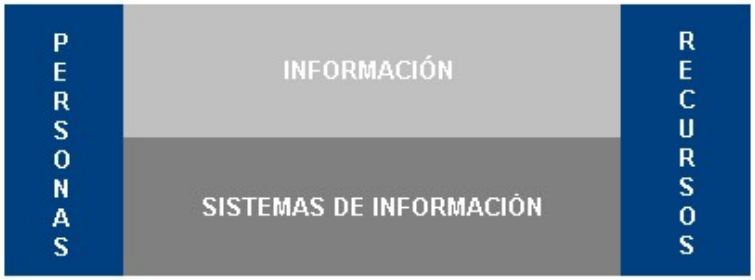
Auditorías de seguridad como método de prevención

Motivos que pueden evitar tomar esta decisión:

- Miedo
- Coste
- Inconsciencia
- Despreocupación
- Desconocimiento

1. PROTECCIÓN DE LA INFORMACIÓN

Negocio



La información es el eje del negocio.

1. PROTECCIÓN DE LA INFORMACIÓN

Ataques al Negocio

¿De dónde provienen?

1. PROTECCIÓN DE LA INFORMACIÓN

¿Qué podemos hacer?

- Nada
- Tomar una actitud reactiva
- Tomar una actitud proactiva

2. AUDITORÍAS DE SEGURIDAD

¿Qué son?

- La comprobación de las medidas de seguridad adoptadas por la empresa
- La revisión o testeo exhaustivo de los Sistemas de Información de la empresa.
- El análisis objetivo de que las normas de seguridad implementadas son suficientes o no.
- Las herramientas para descubrir qué se está haciendo incorrectamente, qué correctamente y qué se puede mejorar dentro de la seguridad.

2. AUDITORÍAS DE SEGURIDAD

Beneficios

- Identifican problemas de seguridad en:
  - Sistemas de protección:
    Routers / Firewalls, IDS / IPS
  - Servidores:
    Sistemas Operativos / Servicios, Aplicaciones
- Permiten detectar fugas de información útil para atacar los sistemas de la empresa.
- Permiten emplear mecanismos estandarizados para la implementación de medidas de seguridad.
- Generan confianza dentro y fuera de la empresa sobre la seguridad.

2. AUDITORÍAS DE SEGURIDAD

Clasificación

Técnicas	Organizativas	Legales
Externas - Test de Intrusión - Auditoría Aplicaciones - ... Internas - Auditoría Intrusiva - Auditoría de Seguridad - ...	Políticas y procedimientos - 1995. BS7799 - 1998. BS7799-2 - 2000. ISO/IEC 17799 - 2002. UNE 17799 - 2004. UNE 71502 - ISO 27000 series BS7799 – 27001 ISO17799 – 27002 - ...	- LOPD - LSSICE - Sarbanes-Oxley - Gramm-Leach-Billey - HIPA - ...

¿Por dónde empezar?

2. AUDITORÍAS DE SEGURIDAD

Una correcta Auditoría de Seguridad requiere:

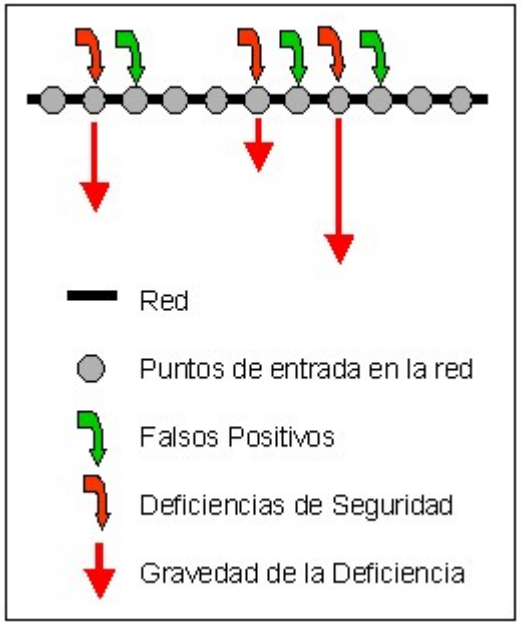
- Objetividad
- Independencia
- Conocimientos
- Uso de metodologías “reconocidas”
  - OSSTMM (Open Source Security Testing Methodology Manual)
  - ISSAF (Information Systems Security Assessment Framework)
  - OWASP (Open Web Application Security Project)

Es necesario revisar periódicamente la seguridad.

2. AUDITORÍAS DE SEGURIDAD

Test de Intrusión

- Es mucho más que un escaneo de vulnerabilidades.
- Consiste en ataques controlados de forma remota a los sistemas de la empresa visibles en Internet.
- Evalúa la seguridad de los sistemas de protección perimetral (routers, firewalls, detectores de intrusos, antivirus, etc.).
- Se emplean las mismas técnicas y herramientas que usa un hacker, pero de forma Ética: Ethical Hacking.



2. AUDITORÍAS DE SEGURIDAD

Test de Intrusión, según la OSSTMM...

- Sondeo de red.
- Escáner de puertos, identificación de servicios y Sistemas Operativos.
- Test Automático de Vulnerabilidades
- Password Cracking.
- Document Grinding.
- Test de Antivirus.
- Test de Firewall y ACLs.
- Test de Medidas de Contención.
- Revisión de la Política de Privacidad.
- Test de los sistemas de confianza.
- Test y Verificación Manual de vulnerabilidades.
- Test del Sistema de Detección de Intrusos (IDS).
- Test de Aplicaciones No Privilegiado.

2. AUDITORÍAS DE SEGURIDAD

Auditoría de Aplicaciones

- Evalúa las buenas prácticas en el desarrollo de aplicaciones
- Consiste en ataques controlados a la aplicación llevados a cabo de forma remota
- Requiere gran parte de búsqueda “manual” de vulnerabilidades
- Dos modos de auditoría: privilegiada/no privilegiada
- Visión externa y objetiva de la seguridad

2. AUDITORÍAS DE SEGURIDAD

Auditoría de Aplicaciones, basadas en la OWASP...

Si no se han tenido en cuenta unas “buenas formas” durante el desarrollo de aplicaciones, tenemos los puntos débiles a explotar.

La auditoría cubre todos los aspectos de la seguridad en las aplicaciones:

- Validación de entradas
- Canonización de URLs
- Manipulación de Parámetros
- Autenticación y Gestión de Sesiones
- Overflows
- Fugas de Información
- Criptografía
- Configuraciones

2. AUDITORÍAS DE SEGURIDAD

Auditorías Internas

Pueden tener dos objetivos diferenciados claramente: Intrusivas o de Seguridad.

- Auditorías Intrusivas:

  Permiten conocer qué puede llegar a hacer un usuario malicioso dentro de nuestra red.

  Se emplean las mismas técnicas (Hacking Ético) que en las Auditorías Externas pero aplicadas a redes locales.

- Auditorías de Seguridad:

  Implica una revisión técnica completa de los SI: arquitectura de red, dispositivos, sistemas de Protección (FW, AV, IDS, etc.), Servidores, Servicios, ordenadores de usuario, VoIP, WiFi, etc.

  Añade una revisión de la documentación disponible (Política de Seguridad, desarrollo, continuidad, etc.) siguiendo los controles de la ISO17799.

3. IMPLANTACIÓN DE UN SGSI

Niveles de seguridad

- Nivel 0: Medidas mínimas legales
- Nivel 1: Auditorías de Seguridad
- Nivel 2: Implantación de un SGSI

3. IMPLANTACIÓN DE UN SGSI

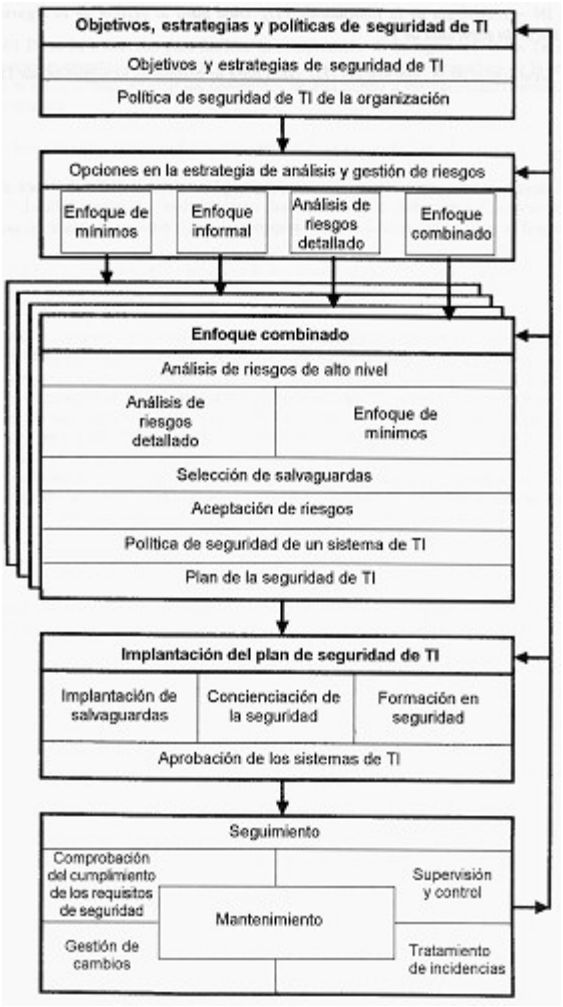
Niveles de seguridad

3. IMPLANTACIÓN DE UN SGSI

Dónde estamos/dónde queremos llegar

- Debemos conocer el nivel de seguridad en el que nos encontramos.
- Debemos conocer el nivel de seguridad requerido en nuestro tipo de negocio.
- Debemos plantearnos el nivel de seguridad que pretendemos alcanzar.
- A partir de todos estos parámetros hay que planificar un desarrollo de la seguridad en la empresa a corto, medio y largo plazo para alcanzar el nivel de seguridad deseado.

3. IMPLANTACIÓN DE UN SGSI



Implantación de un SGSI según la UNE 71502:2004:

La implantación de un SGSI comienza definiendo cuales son los objetivos en seguridad de la empresa.

Continua con un Análisis de Riesgos (AR)según estos requerimientos.

Tras el AR es necesario decidir qué medidas de seguridad tomar para corregir el riesgo no asumible y aceptar o trasladar el riesgo asumible.

El paso siguiente será implantar las medidas que se han decidido.

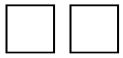
Finalmente es necesario realizar el mantenimiento y seguimiento de todos los aspectos anteriores periódicamente.

3. IMPLANTACIÓN DE UN SGSI

Beneficios de un SGSI

- Los controles del Nivel 1 nos dan confianza a nosotros y la seguridad que estamos empleando mecanismos y sistemas de protección de forma correcta (o en su defecto, se detectaran las deficiencias), pero no implican ningún "sello" de calidad frente a nuestros clientes o proveedores.
- Las certificaciones oficiales aumentan la credibilidad, dan confianza y por tanto facilita la incorporación y posterior fidelización de los clientes.
- Facilita el acceso a mercados exteriores que pueden tener requerimientos específicos de certificación.
- Ofrece calidad implícita y evita la cuestionabilidad de los productos o servicios ofrecidos.
- Elemento diferenciador frente a la competencia.

Gracias por su atención



Vicente Aguilera Díaz
vaguilera@isecauditors.com
Internet Security Auditors, S.L.