*[Adecuación al Esquema Nacional de Seguridad: Un Enfoque Integral]

Autor: Vanesa Gil Laredo
Responsable Consultoría S21Sec
CISA, CISM, CGEIT, Lead Auditor, QSA

Fecha: 2 Junio 2011

S21sec
Unidad de Servicios Globales de Seguridad

Índice

Servicio Integral Adecuación ENS

DESARROLLO DEL PLAN DE ADECUACIÓN

Análisis de Servicios y Sistemas
Categorización de Sistemas
Análisis Situación Actual Cumplimiento
Desarrollo Plan de Adecuación

IMPLANTACION DE MEDIDAS DEL ENS

Necesidades Tecnológicas
Proyectos Cumplimiento ENS
Auditorías Técnicas
Proyectos Internos

MANTENIMIENTO Y MEJORA CONTINUA

Gobierno de la Seguridad

Auditorías Periódicas

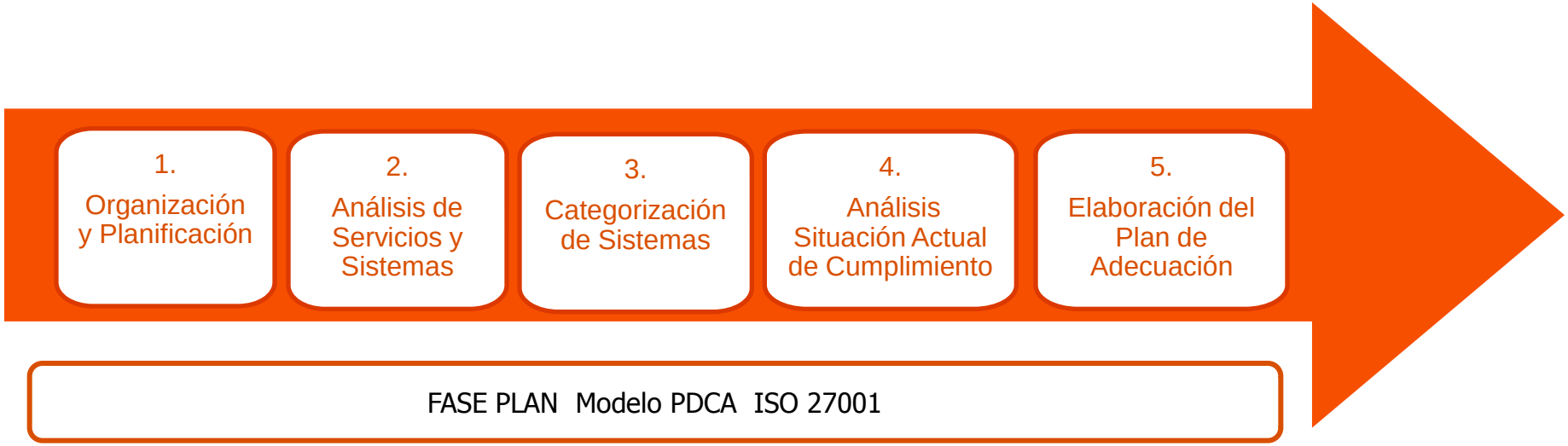
Formación y Concienciación

SERVICIO INTEGRAL ADECUACIÓN ENS

S21sec

Plan de Adecuación ENS

La metodología empleada para el desarrollo del Plan de Adecuación al ENS es la que se detalla a continuación:



Plan de Adecuación ENS

S21sec

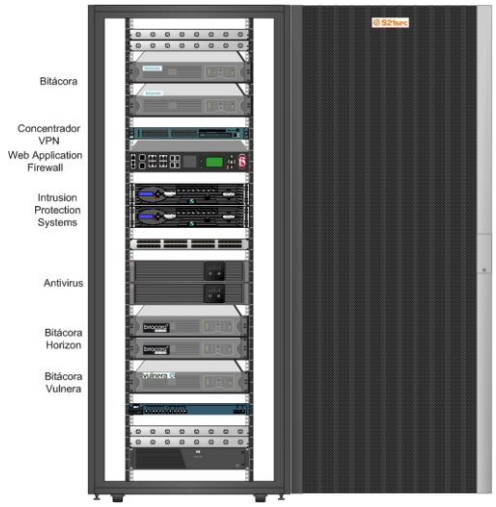
Implantación del ENS

- Una vez que ha sido desarrollado el Plan de Adecuación, es necesario proceder a la implantación de los proyectos que lo constituyen.
- S21Sec propone un enfoque de carácter global, considerando la seguridad desde un punto de vista integral.
- Las acciones y proyectos que resulta necesario implantar para garantizar la adecuación al Esquema Nacional de Seguridad se pueden agrupar en las siguientes categorías:

1. **Necesidades Tecnológicas para Cumplimiento ENS.**
2. **Proyectos para el Cumplimiento ENS.**
3. **Auditorías Técnicas.**
4. **Proyectos Internos.**

Implantación del ENS
1. Necesidades Tecnológicas

- Solución de Monitorización y Gestión de Eventos de Seguridad
- Solución de IDS/IPS
- Software Antivirus
- Solución de Monitorización de Políticas y Seguridad de Servidores
- Solución de Cifrado de Datos



Implantación del ENS
2. Proyectos para Cumplimiento ENS

- Desarrollo del Cuerpo Normativo
- Consultoría de Securización de Arquitectura de Red
- Guías de Securización de Sistemas
- Metodología de Programación Segura
- Estructura Organizativa de Seguridad
- Análisis de Riesgos
- Plan de Continuidad de Negocio
- Formación y Concienciación
- Oficina Técnica ENS

Implantación del ENS
3. Auditorías Técnicas

- Auditoría Bienal ENS
- Análisis de Vulnerabilidades
- Test de Intrusión
- Auditorías de Código de Aplicaciones

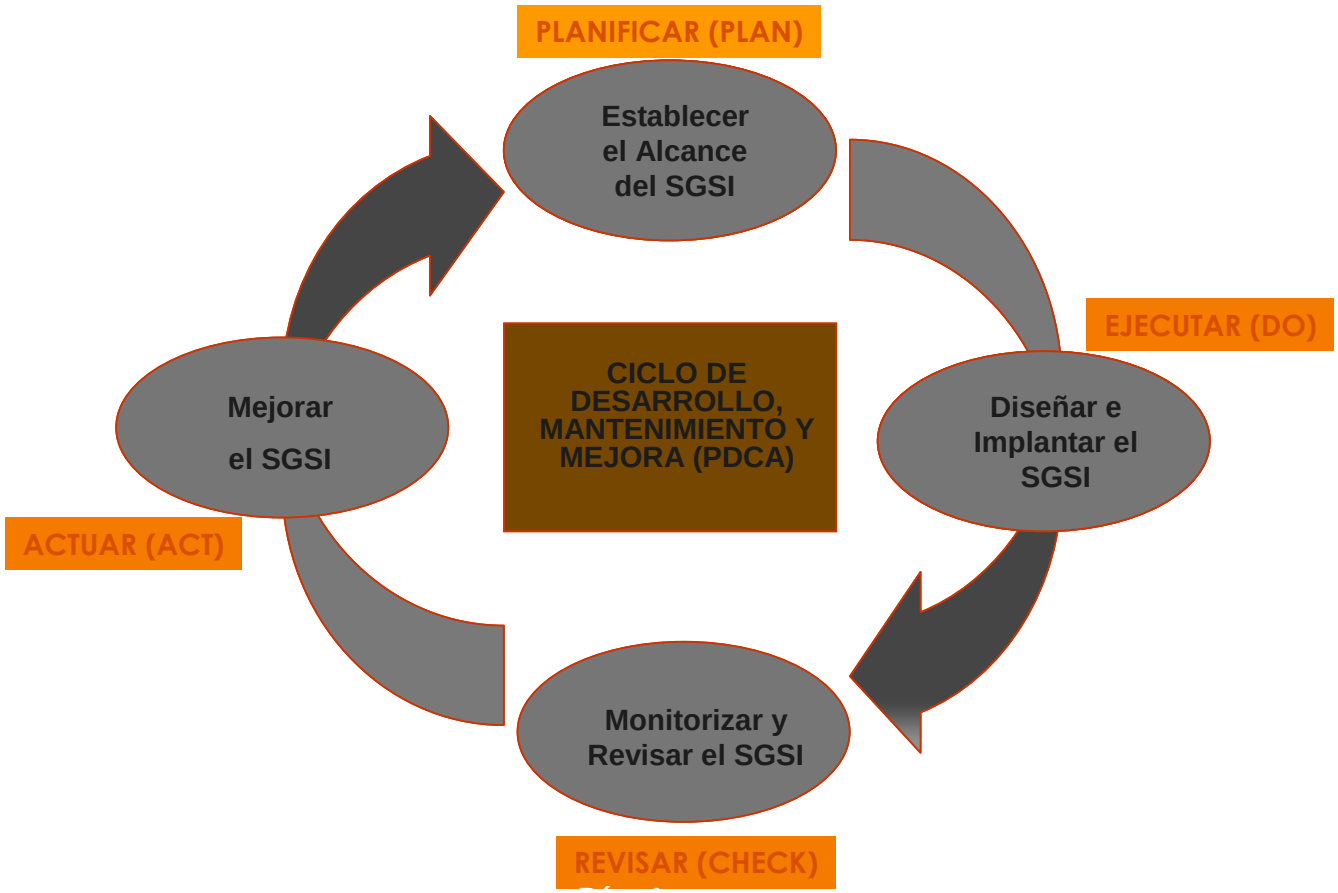
Implantación del ENS
4. Proyectos Internos

- **Implantación de Medidas de Seguridad ENS.**
  1. Implantación de medidas de control de acceso lógico.
  2. Implantación de medidas de control de acceso físico.
  3. Implantación de Guías de Securización de Sistemas.
  4. Implantación de medidas de desarrollo seguro de software.
  5. Implantación de normativas y procedimientos de seguridad
  6. Implantación de recomendaciones de auditorías periódicas.
  7. Otros

- **Mantenimiento de Logs de Sistemas (Registros de Auditoría).**
- **Segmentación y Securización de Arquitectura de Red.**
- **Implantación del Plan de Continuidad de Negocio.**

Mantenimiento y Mejora Continua

- Para garantizar la efectiva implantación del ENS es fundamental considerar el modelo conocido como PDCA (Plan-Do-Check-Act).



Mantenimiento y Mejora Continua
Cuadro de Mandos: Bitacora ENS

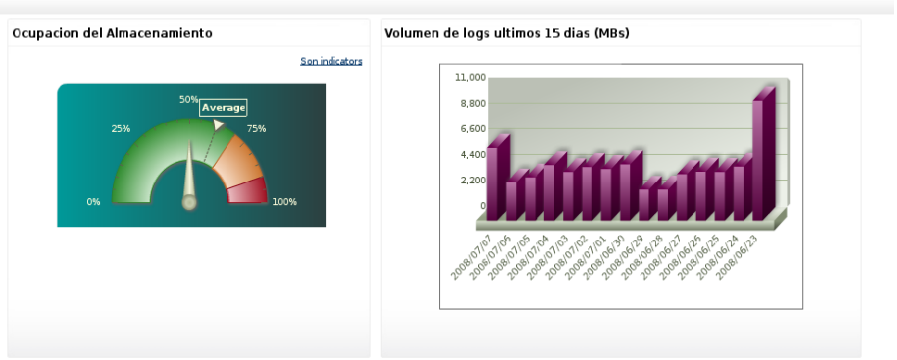
- Bitacora constituye una herramienta eficaz para ayudar al cumplimiento del ENS.

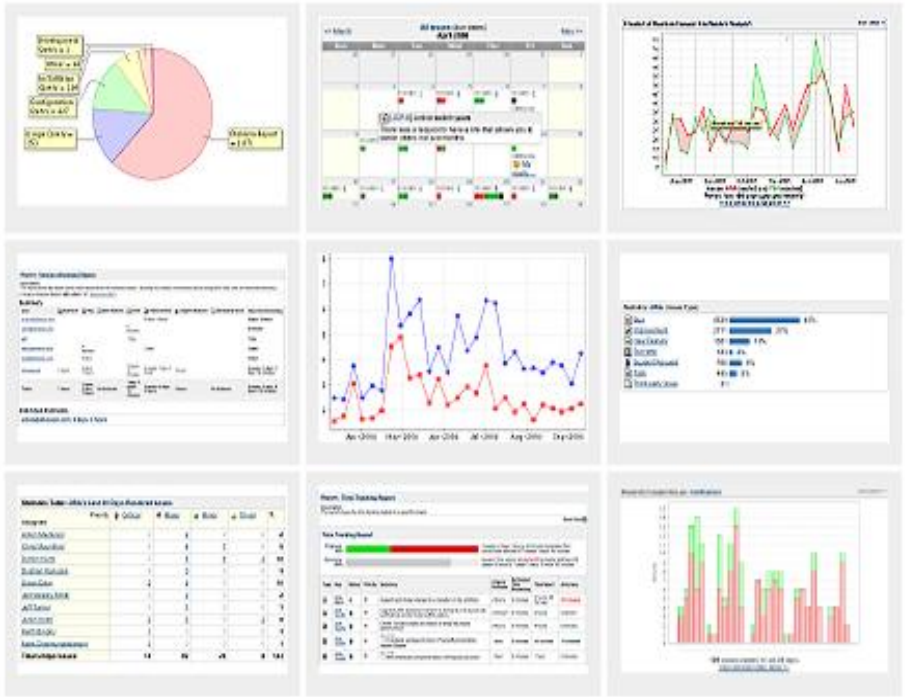
- Establecimiento de un cuadro de mandos que permite revisar y controlar, a través de los eventos monitorizados, el cumplimiento de:
  - Esquema Nacional de Seguridad.
  - Estándar PCI DSS
  - ISO 27001, ISO 27002,…
  - Legislación vigente de protección de datos de carácter personal (LOPD, RLOPD).

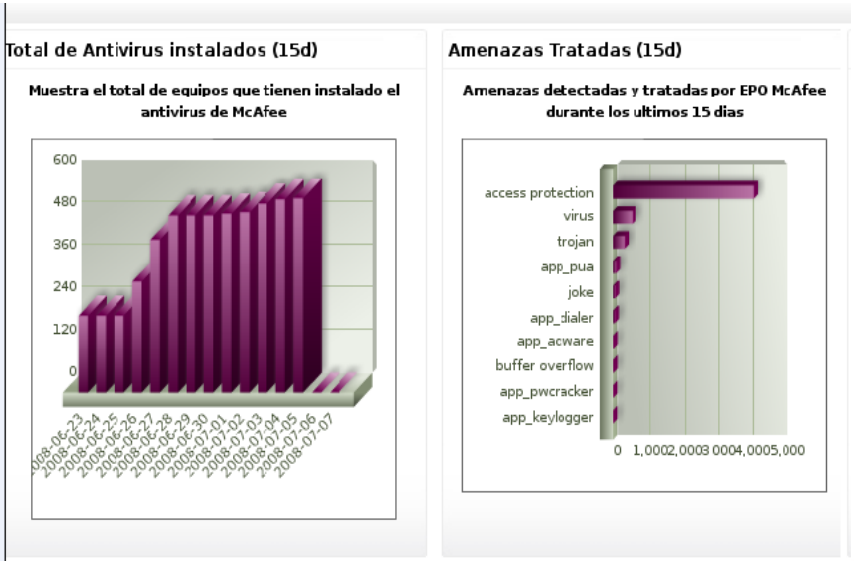
- Herramienta de gestión de logs de los sistemas incluidos en el alcance del ENS (host, firewalls, routers, servidores, bases de datos, aplicaciones,…).

- Permite disponer de indicadores, alertas y cuadros de mando en relación al cumplimiento, entre otras, de las siguientes medidas de seguridad establecidas por el ENS:
  - Control de Acceso Lógico (requisitos de acceso, mecanismos de autenticación, acceso local, acceso remoto…)
  - Protección frente a Código Malicioso.
  - Gestión de Incidencias.
  - Protección de las Comunicaciones.
  - Registro de Accesos.
  - Monitorización del sistema: Detección de Intrusión.
  - Inventario de Activos.

Mantenimiento y Mejora Continua
Cuadro de Mandos: Bitacora ENS







S21sec

Factores Críticos de Éxito

- Enfoque global de gestión de la seguridad de la información.
- Apoyo por parte de la Dirección.
- Aprobación de la Política de Seguridad y del Cuerpo Normativo de Seguridad.
- Establecimiento de una Estructura Organizativa de Seguridad responsable de garantizar la adecuación al ENS:
  - Creación de un Comité de Seguridad.
  - Asignación de roles y responsabilidades.
- Colaboración de todas las áreas implicadas.
- Formación y concienciación en materia de seguridad.
- Revisión y mejora continua del SGSI.
- Asesoramiento especializado.
- Consideración de las Guías del CCN-STIC.

El mayor equipo en España de Seguridad Digital: 200 especialistas

CISA · CISSP · OSSTMM · CISM · GCIA · GSEC

Microsoft Certified Partner | Security Solutions

SEI Partner

Un modelo de Gestión integral de la Seguridad 24 horas. CIS

NUESTRA DIFERENCIA

Desde los inicios, apostando por la innovación y el desarrollo de soluciones de vanguardia.
Primer centro I+D+i de Europa

S21sec labs
La seguridad digital del futuro, hoy

PCI Security Standards Council — APPROVED SCANNING VENDOR

PCI Security Standards Council — QUALIFIED SECURITY ASSESSOR

IQNet · AENOR ER Empresa Registrada UNE-EN ISO 9001 · AENOR ER Gestión I+D+i UNE 166002 · AENOR ER Capacidad Software 1 ISO/IEC 15504 · AENOR ER Seguridad Información UNE-ISO/IEC 27001

Y siempre, calidad y certificaciones

*[MUCHAS GRACIAS]

Contacto: vgil@s21sec.com

www.s21sec.com
info@s21sec.com
+34 902 222 521