Nextel S.A.
Ingeniería y Consultoría

Cómo acometer un proyecto de adecuación al ENS en tiempos de crisis

Joseba Enjuto
Responsable de Control Corporativo y Cumplimiento Legal

jenjuto@nextel.es

3/8/2012

ÍNDICE

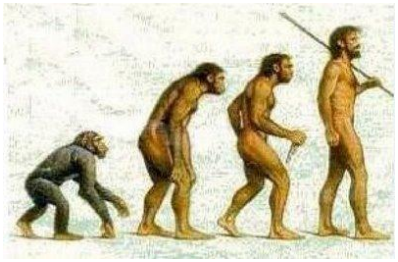
- Introducción
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

- **Introducción**
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

- www.nextel.es
- PYME – 100 personas
- País Vasco (Bilbao/Vitoria/Donostia) – Madrid – Sevilla
- Ingeniería y Consultoría
- Especialización en seguridad y gestión TI
  - ISO 27001
  - **ISO 20000**
  - LOPD
  - **ENS**
  - PIC (Protección de Infraestructuras Críticas)

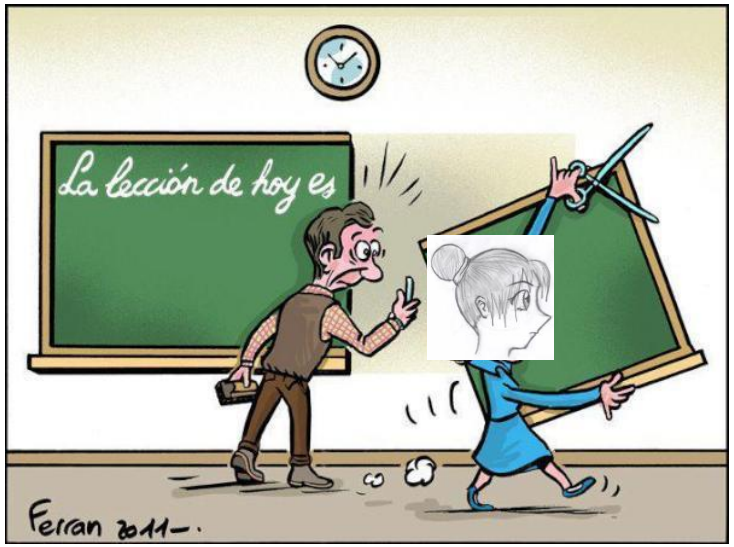
- Esquema Nacional de Seguridad: RD 3/2010
  - Principios básicos (6)
  - Requisitos mínimos (15)
  - Comunicaciones electrónicas
  - Auditoría de seguridad
  - Estado de seguridad de los sistemas (Informe)
  - Medidas de seguridad (Anexo)

- Adecuación al ENS
  - Sistemas nuevos: desde el inicio
  - Sistemas pre-existentes
    - Antes de 30/01/2011
    - Antes de 30/01/2014 si hay un Plan de Adecuación aprobado



Los tiempos de crisis

- Recortes presupuestarios



- Malestar labora'

ÍNDICE

- Introducción
- **ENS práctico**
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

Requisitos

- Proyecto de adecuación al ENS
  - Eficaz
  - Eficiente
  - Sencillo
  - Poco intrusivo
  - Económico

ÍNDICE

- Introducción
- ENS práctico
  - **El alcance**
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

Alcance

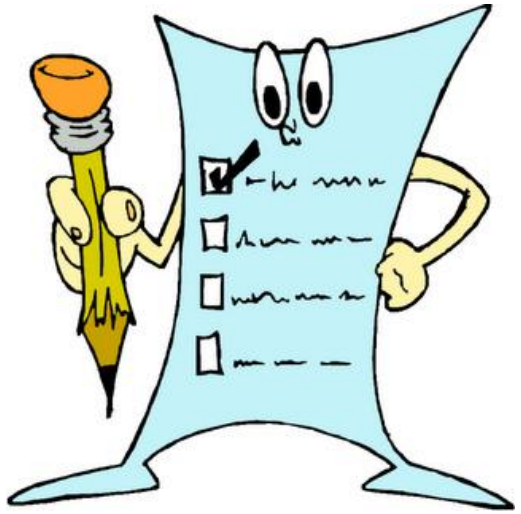
- **Limitar** alcance
  - Simplificación: Alcance inicial limitado
    - Mayor eficacia y eficiencia
    - Aprendizaje
    - Facilidad de ampliación

- **Seleccionar** alcance
  - Simplificación: Servicios principales
    - Mejor relación coste – beneficio

ÍNDICE

- Introducción
- ENS práctico
  - El alcance
  - **El análisis de riesgos**
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

- **Identificar** información / servicios
  - Simplificación: Servicio = información
    - Referencia única y conocida
    - Valoración única
- **Valorar** servicios
  - Simplificación: No usar el nivel Alto
    - Excluir el nivel alto justificadamente
    - Valoración: Despreciable / Normal / Importante
    - Usar gestión de riesgos como complemento
- **Evaluar medidas** de seguridad
  - Simplificación: Utilizar herramienta
    - Amigable para el usuario
    - Facilita mantenimiento
    - Ejemplos: PILAR, GesConsultor



ÍNDICE

- Introducción
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - **El Plan de Adecuación**
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- Conclusiones

Plan de Adecuación

- **NO PRESCINDIR** del Plan de Adecuación
  - Cumplimiento legal

- **Propiedades** del Plan de Adecuación
  - Modular
    - Por prioridad (impacto/urgencia)
    - Por bloques temáticos
  - Considerando costes completos
    - Externos
    - Internos
  - Realista en plazos
    - Carga de trabajo prevista
    - Presupuestos
  - Recursivo
    - Considerar ciclos en planes pluri-anuales

ÍNDICE

- **Política de Seguridad**
  - Simplificación: Política jerárquica y modular
    - Fácil de aprobar y mantener

- **Organización** de la Seguridad
  - Simplificación: Minimizar perfiles
    - Menor "ruido" interno
  - Simplificación: Roles != Funciones
    - Función de aprobación
    - Función de ejecución
  - Simplificación: Asignar función ejecutora a TIC
    - Perfiles funcionales poco preocupados por los servicios electrónicos

ÍNDICE

- Introducción
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - **Las medidas operativas**
  - Las medidas técnicas
- Conclusiones

Gestión de la seguridad

- Simplificación: Usar herramientas
  - Soporte tangible
  - Facilita mantenimiento
  - Ejemplos: ENSTool, GesConsultor

Gestión del ciclo de vida de los sistemas

- Simplificación: Proyecto(s) interno(s) de cambio
  - Menor resistencia al cambio

- Simplificación: Formación, concienciación y VENTA
  - Explica el por qué y el para qué
  - Convencer, no vencer

ÍNDICE

- Introducción
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - **Las medidas técnicas**
- Conclusiones

Herramientas

- Simplificación: "Exprimir" infraestructura existente
  - Equipamiento de red, VPN, Directorio Activo, Plataformas de firma, …
  - Menor coste
- Simplificación: Uso de software libre
  - Menor coste
  - Capacidad de complementar operativamente carencias técnicas
- Simplificación: Realismo
  - Limpieza de metadatos desasistida?
  - Gestión de infraestructura con certificados?

ÍNDICE

- Introducción
- ENS práctico
  - El alcance
  - El análisis de riesgos
  - El Plan de Adecuación
  - Las medidas organizativas
  - Las medidas operativas
  - Las medidas técnicas
- **Conclusiones**

- **Exigencias adaptables**
  - Coste dependiente de valoración
  - Coste principal: dedicación interna
- **Criterios de inversión**
  - Distribución temporal
  - Cumplimiento
  - Mantenibilidad
  - Gestionabilidad

Factor clave de éxito:

concienciación en seguridad de los órganos de gobierno

FIN

MUCHAS GRACIAS

Joseba Enjuto

Responsable de Control Corporativo y
Cumplimiento Legal

jenjuto@nextel.es