Nextel S.A.
Ingeniería y Consultoría

Sorteando obstáculos en el camino hacia la certificación

Joseba Enjuto
Director de Consultoría

@JosebaEnjuto

3/31/2016

ÍNDICE

- Presentación
- Introducción
- Sorteando obstáculos... fase por fase
  - Plan de Adecuación
  - Implantación
  - Despliegue
  - Mantenimiento
- Conclusiones

ÍNDICE

Nextel S.A.

- www.nextel.es
- PYME – 100 personas
- 27 años
- País Vasco (Bilbao/Vitoria/Donostia) – Madrid – Sevilla – Mexico DF
- Ingeniería y Consultoría
- Especializados en **Seguridad** y **Gestión TIC**

Tenemos un compromiso con la **mejora continua** para Alcanzar la **excelencia empresarial**

Q 2004

EFQM

AENOR ER Empresa Registrada ER - 0688/2/00

AENOR ER Seguridad Información UNE-ISO/IEC 27001

AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1

- **Consultoría**: Empresa de referencia en:
  - Esquema Nacional de Seguridad (**ENS**) – RD 3/2010
  - Gestión de servicios TI – **ISO 20000**
  - Continuidad de Negocio – **ISO 22301**
- **Ingeniería**: Empresa de referencia en:
  - Infraestructuras (**Red Hat**, sistemas hiper-convergentes, …)
  - Dispositivos de seguridad (**Check Point**, **Palo Alto**, **FireEye**, …)
- **Servicios especializados**: Empresa de referencia en:
  - Auditoría & Hacking (**PenTesting, peritaje**, …)
  - Seguridad gestionada (**SOC**, **MSSP**, …)

Joseba Enjuto

- Director de Consultoría de Nextel S.A.:
  - Consultor, auditor y formador
  - Múltiples certificaciones
    - Lead Auditor ISO 27001, ISO 20000, ISO 22301
    - Formador ISO 27001, ISO 20000, ISO 22301
    - Evaluador EFQM
    - ITIL Foundations
    - CISM
    - Experto en Evidencias Electrónicas
- Más de 12 años de experiencia como consultor
  - 6 años de experiencia con el ENS
- Director de itSMF Euskadi
- es.linkedin.com/in/josebaenjuto

ÍNDICE

- Presentación
- **Introducción**
- Sorteando obstáculos... fase por fase
  - Plan de Adecuación
  - Implantación
  - Despliegue
  - Mantenimiento
- Conclusiones

- **Esquema Nacional de Seguridad**: RD 3/2010 + RD 951/2015
  - Principios básicos (6)
  - Requisitos mínimos (15)
  - Mecanismo para cumplirlos
    - Medidas de seguridad (75) proporcionales a los riesgos
- Adecuación al ENS:
  - Plan de Adecuación
  - Implantación
  - Despliegue
  - Certificación
  - Mantenimiento

Cortesía de AENOR

ENS – Esquema Naciona de Seguridad

AENOR realiza actualmente la auditoría de certificación de conformidad del ENS de acuerdo a la **UNE-EN ISO/IEC 17021** para entidades de certificación.

AENOR esta considerando la UNE-EN ISO/IEC 17065 para la futura acreditación por ENAC. *(CCN-STIC-809 Declaración y Certificación de Conformidad del ENS)*

Además utiliza las guías del Centro Criptológico Nacional:

- ✓ **CCN-STIC-802,** ENS. Guía de Auditoría.
- ✓ **CCN-STIC 808,** Verificación del cumplimiento medidas ENS.
- ✓ **CCN-STIC-825**, ENS. CERTIFICACIONES 27001.

AENOR
conform

Los sistemas de información ó servicios del alcance siempre de acuerdo a **la categorización del sistema vigente.**

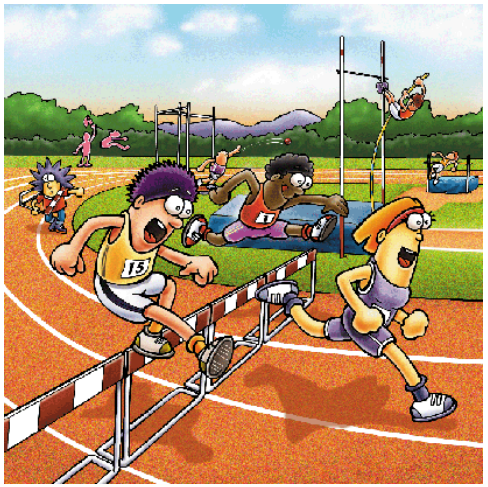
AENOR ha emitido más de 10 certificaciones de conformidad a Administraciones Públicas o entidades. *(**Consejo General de la Abogacía; Consejería de Castilla-La Mancha; KIO Networks**; ...)*

Cortesía de AENOR

Camino hacia la Certificación

- La certificación es una meta… **intermedia**
  - Plan de Adecuación
  - Implantación
  - Despliegue
  - **Certificación**
  - Mantenimiento
  - Mantenimiento
  - Mantenimiento
  - …

- Con algunos obstáculos en el camino



ÍNDICE

Obstáculos del Plan de Adecuación

- Planteamiento
  - Obstáculo: Entender el ENS como un proyecto TIC
- Alcance
  - Obstáculo: Alcance inicial excesivamente ambicioso
- Categorización de sistemas
  - Obstáculo: Valoraciones demasiado altas (perjuicio muy grave?)
    - Anulación de la capacidad de la organización para atender a obligaciones fundamentales.
    - Daño muy grave, o irreparable, por los activos de la organización.
    - Incumplimiento grave de alguna ley o regulación.
    - Perjuicio grave a algún individuo, de difícil o imposible reparación.

Obstáculos del Plan de Adecuación

- Análisis de riesgos
  - Obstáculo: Demasiado nivel de detalle
- Plan de adecuación
  - Obstáculo: Adecuación “de una sola vez”
  - Obstáculo: Adecuación demasiado rápida

ÍNDICE

- Presentación
- Introducción
- **Sorteando obstáculos… fase por fase**
  - Plan de Adecuación
  - **Implantación**
  - Despliegue
  - Mantenimiento
- Conclusiones

Obstáculos de la Implantación

- Articulado
  - Obstáculo: Olvidarse de implantar el proceso de seguridad
- Política
  - Obstáculo: Aprobación de la Política de Seguridad
  - Obstáculo: Entender la Política de Seguridad como una medida más
- Marco organizativo
  - Obstáculo: Centrarse en los procedimientos
- Medidas de protección
  - Obstáculo: Entender el proyecto como tecnológico

ÍNDICE

Obstáculos del despliegue

- Concienciación y difusión
  - Obstáculo: No centrarse en la visión del usuario

- Formación
  - Obstáculo: Formar sólo a parte de los afectados
  - Obstáculo: Olvidarse de la formación técnica

- Despliegue de las medidas de seguridad
  - Obstáculo: Olvidarse de la gestión del cambio

- Auditoría
  - Obstáculo: Olvidarse de la auditoría interna

ÍNDICE

Obstáculos del mantenimiento

- Gestión periódica
  - Obstáculo: Olvidarse de que la gestión de la seguridad es un proceso

- Gestión ágil
  - Obstáculo: Gestión “manual”

- Gestión eficaz
  - Obstáculo: No haber formalizado roles de administración de seguridad

ÍNDICE

- Presentación
- Introducción
- Sorteando obstáculos... fase por fase
  - Plan de Adecuación
  - Implantación
  - Despliegue
  - Mantenimiento
- **Conclusiones**

Conclusiones

- El ENS es una obligación
  - Puede convertirse en una oportunidad
- La certificación puede ser un factor diferencial
- Los obstáculos son sorteables
  - Pon un consultor para que te guíe!

¡Muchas Gracias!

Joseba Enjuto

jenjuto@nextel.es

Director de Cunsultoría

Socinfo

30/03/2016

¡Síguenos en
Redes Sociales!