sira

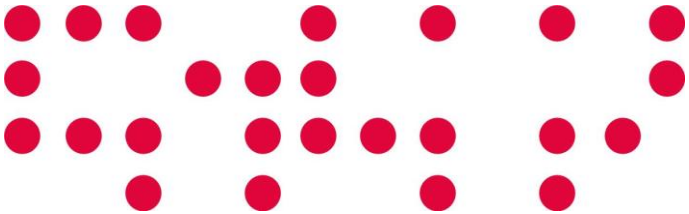
(Seguridad Informática en la Red Académica)

Javier García
Universidad de Murcia

Evangelino Valverde
Universidad de Castilla-La Mancha

Alcalá de Henares
Grupos de Trabajo RedIRIS 2008

1. Objeto de la presentación
2. Descripción de la iniciativa
3. Resumen
4. Debate



Objeto de la presentación

- Informar sobre la iniciativa **sira**
- Obtener vuestras opiniones sobre el enfoque del proyecto
- Captar voluntarios :-)

Cómo surge la iniciativa

- "¿Por qué no hacemos un RACE para seguridad?"

  Javier García en los GT de Valencia de 2008

- Qué es RACE (v2)
  - Red Avanzada de Correo Electrónico
  - Criterios de calidad evaluables y certificables
  - Puntuación por criterio
  - Asignación de nivel por puntuación (1, 2 o 3)
  - Criterios obligatorios (ej. filtrado del puerto 25)
  - Evaluador semiautomático

Actividad del grupo

- Grupo de voluntarios a través de IRIS-CERT

  Iñaki Ortega (**EHU**), Javier García y Jose Francisco Hidalgo (**UM**), Chelo Malagón y Diego López (**RedIRIS**), Jaime Lorenzo y Eduardo Bergasa (**UNIRIOJA**), Elena Galván (**UPC**), María Dolores de la Guía (**CSIC**), Toni Cortés (**URV**) y Evangelino Valverde (**UCLM**)

- Arranca en Junio de 2008
- Interacción 100% no presencial (correo, EVO, Doodle, Sharepoint)
- Documento de descripción de la iniciativa
- Primera reunión presencial en estos grupos

Objetivos y áreas a cubrir

- *"Fomentar las buenas prácticas en materia de seguridad informática dentro de las instituciones afiliadas a RedIRIS"*
- Cubre todos los aspectos de la seguridad informática de una institución
- Propuesta inicial de áreas:
  - Tantos enfoques distintos como miembros del grupo
  - Probablemente visiones sesgadas
  - Falta de consenso

Búsqueda de referencias

- "Los buenos artistas copian, los genios roban"

  Pablo Picasso

- No sé si somos genios pero vamos a robar ;-)
- Referencias
  - **ISO 27002** (a.k.a. ISO 17799:2005): Guía de buenas prácticas
  - **ISO 27001**: Requisitos para el sistema de gestión de la seguridad de la información (SGSI)
  - **ISO 27799**: Aplicación de la ISO 27002 en el sector sanitario

ISO 27001

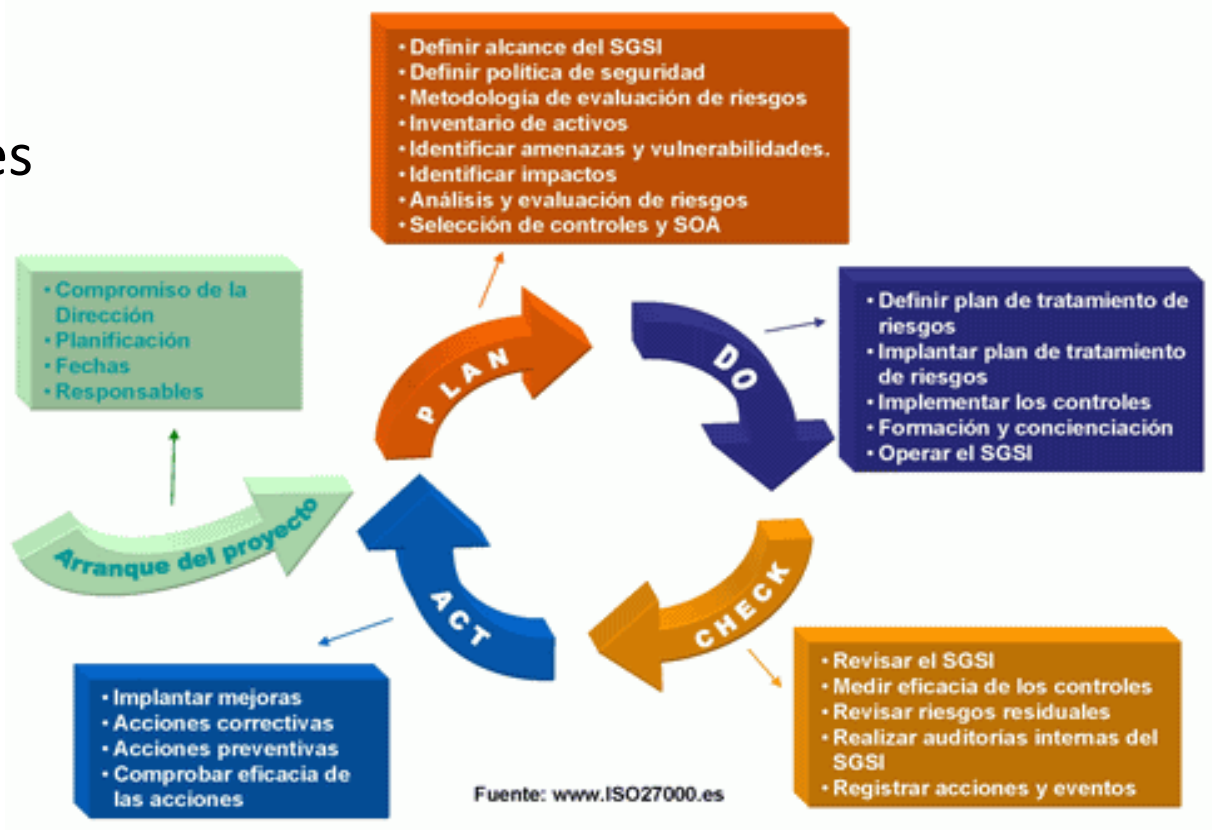
- Estándar aceptado internacionalmente para la administración de la seguridad de la información
- Aplicable a todo tipo de organizaciones
- No está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos
- Modelo(PDCA) *Plan-Do-Check-Act* para un SGSI

¿Qué es un SGSI?

- SGSI (Sistema de Gestión de Seguridad de la Información)
- La gestión de la seguridad de la información debería realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.
- Objetivo: que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma **documentada**, **sistemática**, **estructurada**, **repetible**, **eficiente** y adaptada a los cambios (**modelo de madurez**)

ISO 27001

- Certificable
- Conjunto controles
- Mejora continua



ISO 27002

- Guía de buenas prácticas
- describe los objetivos de control y controles recomendables
- 11 dominios, 39 objetivos de control y 133 controles
- Ejemplo:
  - **Dominio:** Gestión de Comunicaciones y Operaciones
  - **Objetivo de control:** Supervisión
  - **Control:** Sincronización del Reloj. Posibilita la obtención de registros de auditoría exactos y por tanto la investigación de incidentes.

ISO 27002: dominios

1. Política de seguridad
2. Aspectos organizativos de la seguridad de la información
3. Gestión de activos
4. Seguridad ligada a los recursos humanos
5. Seguridad física y ambiental
6. Gestión de comunicaciones y operaciones
7. Control de acceso
8. Adquisición, desarrollo y mantenimiento de los S.I.
9. Gestión de incidentes en la seguridad de la información
10. Gestión de la continuidad del negocio
11. Cumplimiento

¿Encaja la ISO 27002 en nuestros objetivos?

- ✚ Muy bien pensada y estructurada
- ✚ Muy completa
- ✚ Es un estándar (nos coloca en la dirección correcta)

- - Mala fama de las normas ISO: difícil de implantar
- - Percepción: mucho papeleo y poca medida técnica
- - Se centra en el qué pero no en cómo

Soluciones

- **No** proponemos una nueva metodología para SGSI
  - Si necesitas una, la ISO 27001 es una buena opción
- proponemos un conjunto de buenas prácticas
  - Que hace uso de la ISO 27002, como base pero no como objetivo
  - Extenderla allí donde podamos aportar algo
- proponemos una clasificación y selección de la misma por niveles de importancia (obligatorios, alta, media y baja)

Soluciones

- Proponemos una organización tipo para el desarrollo de guías:
  - Seleccionar sólo los controles más relevantes
  - Elaborar guías para indicar **cómo**
- Estudiaremos posibles mecanismos de evaluación / autoevaluación
- Nos apoyaremos en otras iniciativas y quizá proponer y promover nuevas:
  - Actual RACE para el correo
  - DNS, WEB, redes móviles (Eduroam), ...

Fases del proyecto (I)

- Fase I
  - Modelado de una organización tipo (estructura, activos, amenazas, etc.)
  - Selección de los controles ISO 27002 más relevantes para esa organización tipo
  - Clasificación de los controles por importancia (obligatorios, alta, media, baja)
- Fase II
  - Elaboración de recomendaciones/guías por control

Fases del proyecto (II)

- Fase III
  - Estudio/definición de un sistema de evaluación/autoevaluación
  - Elaboración guía de evaluación
    - Asignación de puntos por criterio
  - Evaluación de posible automatización
  - Certificados SIRA básico, medio y avanzado en función de:
    - Criterios de obligado cumplimiento
    - Puntuación obtenida

Fases del proyecto (III)

- Fase IV
  - Evaluación de resultados
  - Acciones correctivas
  - Implantar mejoras

Qué no es objetivo de la iniciativa sira

- Reinventar la rueda :-)
- Promover ni la implantación de la ISO 27001 ni su certificación
- Desarrollar guías de seguridad para servicios (DNS, Web, correo, etc.) que requerirían grupos de trabajo específicos

Resumen

- Objetivo: fomentar las buenas prácticas en S.I.
- Estrategia:
  - Utilizar un modelo de criterios/evaluación similar a RACE usando la ISO 27002 como base
- Fases:
  - Fase I: modelado y selección de controles
  - Fase II: elaboración de guías (cómo)
  - Fase III: sistema de evaluación
  - Fase IV: implantación de mejoras

Colabora

- Buscamos colaboradores. Apúntate en:

  http://listserv.rediris.es/wg-reqseg.html

Debate

- ¿Os parecen útiles los objetivos de esta iniciativa?
- ¿Cómo mejorarías la estrategia?
- ¿Veis valor en las certificaciones?
- ¿Otros enfoques?
- ¿Quién quiere colaborar?

Muchas gracias