SGSI
Poniendo orden a la seguridad

Eduardo Bergasa
eduardo.bergasa@unirioja.es

Introducción

”La seguridad sin control puede no ser efectiva”

Grados de madurez

- Grado 0. Sin preocupación por la seguridad
- Grado 1. Seguridad sin gestionar
- Grado 2. Seguridad algo gestionada
- Grado 3. Seguridad totalmente gestionada
- Grado 3+. Certificación ISO.

Grado 1

- Promovido por técnicos
- Sin instrucción por parte de la dirección
- Los técnicos deciden qué proteger y cómo hacerlo
- Implantando de controles **técnicos** de protección

Grado 1

- Antivirus de puesto
- Antivirus de correo
- Cortafuegos perimetral
- Cortafuegos internos
- IDS/IPS
- Antivirus perimetral, proxy
- ..

Grado 1

- La seguridad no son sólo medidas técnicas
  - La seguridad depende de las personas
  - También son medidas organizativas
- Las decisiones sobre la información a proteger no son técnicas
- Se pueden pasar por alto controles importante

Grado 2. Seguridad algo gestionada

En busca de estándares

En búsqueda de estándares: La serie ISO 27000

- ISO 27001. Sistema de Gestión de Seguridad de la Información
- ISO 27002. Conjunto de buenas prácticas y controles de seguridad que podrían tenerse en cuenta en una organización
- *ISO 27003. Guías de implantación de un SGSI*
- *ISO 27004. Métricas de seguridad*
- *ISO 27005. Gestión de riesgos*
- *ISO 27006. Acreditación de certificadores de SGSI*
- *ISO 27799. Adaptación de la ISO27002 para las particularidades del sector sanitario*

ISO 27002

- ISO 27002 == ISO 17799
- **Seguridad de la información**
  - La preservación de la confidencialidad, la integridad y la **disponibilidad** de la información, pudiendo además abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

ISO 27002

- Es una guía de buenas prácticas
- Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información
- No es certificable.
- Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios

Controles ISO 27002

- Política de Seguridad
- Aspectos organizativos de la Información
- Gestión de Activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los Sistemas de Información
- Gestión de Incidentes de Seguridad
- Gestión de Continuidad del negocio
- Cumplimiento normativo

5. Política de seguridad

- Existencia de una política que guíe todas las medidas de seguridad
- Política respaldada por la dirección
- Conocida por toda la organización
- Revisada y actualizada

6. Aspectos organizativos

- Organización interna
  - Coordinación de todas las actuaciones en materia de seguridad. Comité.
  - Definición de responsabilidades
  - Acuerdos de confidencialidad
  - Contactos con autoridades
- Terceras partes
  - Seguridad y riesgos en relaciones con clientes y proveedores

7. Gestión de activos

- Inventario y responsabilidad de activos
- Identificar propietarios
- Políticas de uso aceptable
- Clasificación de la información

8. Gestión de RRHH

- Aceptación de políticas y acuerdos de confidencialidad
- Formación, sensibilización
- Al finalizar el contrato
  - Devolución de activos
  - Retirada de autorización

9. Seguridad física

- Acceso físico a instalaciones
- Protección frente a amenazas del entorno
- Robos
- Suministro
- Cableado
- Destrucción/reutilización de equipos

10. Gestión de operaciones y comunicaciones

- Gestión de cambios
- Aceptación del sistema
- Código malicioso
- Copias de seguridad
- Controles de seguridad en la red
- Gestión de soportes
- Monitorización. Registros

11. Control de acceso

- Gestión de usuarios
- Gestión de privilegios
- Sistemas de identificación de usuarios
- Políticas de contraseñas
- Control de acceso y uso de la red y los sistemas
- Segregación de redes
- Seguridad en movilidad

12. Compras, desarrollo y mantenimiento

- Requisitos de seguridad de aplicaciones compradas o desarrolladas
- Revisión de aplicaciones tras cambios
- Acceso al código fuente
- Controles criptográficos
- Control de vulnerabilidades técnicas

13. Sistema de gestión de incidentes

- Funcionamiento del sistema de gestión de incidentes

14. Continuidad de negocio

- Planes de contingencia en caso de catástrofe

15. Cumplimiento normativo

- Cumplimiento de la legislación vigente
- LOPD
- LSSIC
- Propiedad intelectual

En qué se mejora con ISO27002

- Se tiene una visión global de la seguridad
- Con el checklist es más dificil 'olvidarse' algo
- Se incorporan medidas organizativas
- Se implica a la dirección

Grado 3. Seguridad gestionada

El sistema de gestión de seguridad

- ¿Sabemos nuestro nivel de seguridad?
- ¿Es suficiente para la información a proteger o demasido?
- ¿En qué nos basamos para hacer inversiones en seguridad?

- ¿Son efectivas nuestras medidas de seguridad?
- No disponemos de medidas del funcionamiento y evolución del sistema
- ¿Cómo saber si mejoramos o empeoramos?

SGSI: ISO 27001

- SGSI = Sistema de Gestión de Seguridad de la Información
- ISMS = Information Security Management System
- Herramienta para gestionar la seguridad
- Define un proceso sistemático, documentado y conocido por toda la organización para gestionar la seguridad desde un enfoque de *riesgo empresarial*

- La seguridad total no existe
- El objetivo de un SGSI es garantizar que los riesgos de la seguridad sean conocidos y gestionados de una forma sistemática y eficiente
- Es una herramienta para conocer nuestro nivel de riesgo y ayudarnos a minimizarlo a través de controles de seguridad o aceptarlo

Bisagra con la dirección

- Es una herramienta de gestión empresarial
- Habla el idioma de la dirección
- Similar a otros sistemas de gestión
- Compatible con ISO 9001 e ISO 14000
- Propósito de alinear la seguridad a las necesidades del negocio
- Aporta cuadro de mando con indicadores

Enfoque top-down

- Considera la información parte fundamental de la organización
- La seguridad de la información es un requisito de negocio
- Implicación de los altos mandos marcando las directrices

Las bases de un SGSI

- Definición del alcance
- Seguridad orientada a los procesos de negocio y dirigida por la dirección. Comité de seguridad.
- **Gestión de riesgos**
- Controles de seguridad
- Indicadores del funcionamiento del SGSI
- Proceso de mejora continuo

Gestión del riesgo

Identificación de activos

- Es importante saber qué es lo que queremos proteger
- Asignación de importancia o prioridades a los activos
- Clasificación de la información

Gestión de riesgos

- Identificar los riesgos en base a:
  - Activos
  - Amenazas
  - Vulnerabilidades
  - Impacto
- Riesgo: Pérdida que se produciría en nuestros activos en caso de que se materializase una amenaza aprovechando una vulnerabilidad

Gestión del riesgo

Gestión de Riesgos

- Identificar los riesgos que pueden afectar a nuestros activos
- Tratamiento sistemático del riesgo:
  - Evitarlo: Suprimir las causas del riesgo
  - Transferirlo: Outsourcing, seguros
  - Reducirlo
  - Asumirlo
- **Fijar los niveles de riesgo aceptables**

Selección de controles

- Basándos en el alcance, análisis de riesgos y la política de seguridad se seleccionan los controles de seguridad
- Declaración de aplicabilidad

SGSI: Ciclo de vida

Ciclo de vida

- PLAN
  - Evaluación de amenazas, riesgos e impacto
- DO
  - Se seleccionan e implementar los controles para reducir el riesgo a un nivel aceptable
- CHECK y ACT
  - Recogida de evidencias e indicadores que realimentan el sistema
  - Proceso de mejora del sistema

PLAN: Establecer el SGSI

- Definición del alcance
- Definir Política de Seguridad
- Definir Metodología de evaluación del riesgo

DO: Implementar y utilizar el SGSI

- Seleccionar los controles en base al análisis de riesgos
- Implantar los controles
- Definir sistema de métricas para saber la eficacia de los controles
- Formación y concienciación del personal

CHECK: Monitorizar y revisar el SGSI

- Comprobar la efectividad del SGSI y de los controles
- Revisar periódicamente las evaluaciones del riesgo
- Registrar acciones y eventos que puedan afectar a la efectividad del sistema

ACT: Mantener y mejorar

- Implantar mejoras identificadas en el paso anterior

Condiciones para el éxito

- COMPROMISO DE LA DIRECCIÓN
  - Definir política de seguridad
  - Establecer responsabilidades
  - Asignación de recursos
  - Formación y concienciación

Condiciones para el éxito

- COMPROMISO DE LA DIRECCIÓN
- Definición de alcance apropiada
- Evaluación de riesgos adecuada
- Compromiso de mejora
- Organización y comunicación
- Concienciación del personal
- Integración del SGSI en la organización

Pasos para implantar un SGSI

- Formación del personal
- Convencer a la dirección
- Elegir un alcance reducido
- Crecer poco a poco

Qué aporta el SGSI

- Los controles de seguridad se han fijado de acuerdo a las prioridades del negocio y a los riesgos
- El análisis de riesgos permite orientar las inversiones
- Podemos mejorar
- Conocemos y aceptamos nuestro nivel de seguridad

Qué aporta el SGSI

- Conocer la efectividad de nuestras medidas de seguridad
- Aporta calidad a la seguridad
- Concienciación y compromiso

Inconvenientes

- Excesiva burocracia
- Sobrecarga de trabajo
- Esfuerzo continuo para mantenerlo en marcha
- Necesidad de recursos: esfuerzo, tiempo y gasto

Grado 3+. Certificación del SGSI

¿Utilidad de la certificación?

- Para empresas es clara:
  - Diferenciación
  - Competitividad
  - No exclusión
- Para organizaciones RedIRIS:
  - Recompensa al trabajo de implantación
  - Imagen
  - Reconocimiento del funcionamiento del sistema por un externo
- El objetivo debería ser la certificación

¿Certificación = Inmunidad?

- La certificación es al sistema de gestión, no a la seguridad técnica.
- No es garantía de inmunidad

¿Es viable implantar y certificarse?

- Es dificil en una organización grande y con colectivos heterogeneos.
- Es viable certificarse reduciendo el alcance

SIRA

Seguridad **I**nformática en la **R**ed **A**cadémica

UNIVERSIDAD DE LA RIOJA

Eduardo Bergasa Balda – Ciudad Real Marzo 2009

SIRA

- Objetivos
  - Ayudar a las organizaciones a lograr el apoyo institucional necesario
  - Evaluación del nivel de seguridad en las organizaciones
  - Ayudar a que las organizaciones sepan cuáles sus puntos débiles y cómo mejorar

SIRA

- Medios
  - Encuesta de autoevaluación basada en ISO27002
  - Documentación de ayuda
- Objetivo a largo plazo, crear una certificación 'al estilo RACE'

SIRA: Participantes

- Universidad de Almería
- Universidad de Burgos
- Universidad de Castilla La Mancha
- CSIC
- Universidad de Murcia
- Universidad Pública de Navarra
- Universidad Pablo Olavide
- Universidad del País Vasco
- Universidad Politécnica de Cataluña – esCERT
- Universidad Politécnica de Cartagena
- Universidad de La Rioja
- Universidad Rovira i Virgili

SGSI
Poniendo orden a la seguridad

Eduardo Bergasa
eduardo.bergasa@unirioja.es

Más información

- Normas ISO 27001, ISO 27002
- www.iso27000.es