MINISTERIO
DE CIENCIA
E INNOVACIÓN

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

El largo camino de un Plan Director de Seguridad de la Información

Dolores de la Guía Martínez

Secretaría General Adjunta de Informática

CSIC

CSIC
Consejo Superior de Investigaciones Científicas

Presentación

1. Las expectativas
2. El pliego
3. El concurso
4. Los inicios
5. El desarrollo
6. Los resultados
7. El después
8. Y al final …¿qué?

1. Las expectativas. El idealismo

- Pregunta:

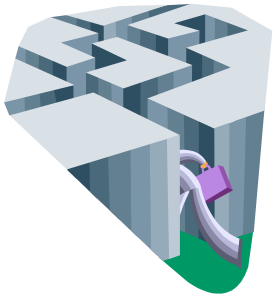
  ¿Qué esperamos de un PDSI?

- Respuesta:

  La solución de todos nuestros problemas

CSIC
Consejo Superior de Investigaciones Científicas

1. Las expectativas. La realidad

- Conviene ser realistas y definir unos objetivos razonables
  - Distinguir y acotar los puntos básicos de interés
  - Añadir algunos puntos secundarios
  - Delimitar el estudio a un período suficiente pero no demasiado largo
- … para obtener  y no 

CSIC
Consejo Superior de Investigaciones Científicas

2. El pliego

- Objetivo
  - Contratación de un servicio de consultoría para la definición y elaboración de un Plan Director de Seguridad de la Información (PDSI) que abarque la infraestructura física, lógica, de comunicaciones y la adecuación a la normativa legal vigente en materia de seguridad de la información en el CSIC
- Plazo de ejecución
  - 4 meses

2. El pliego

- Alcance
  - Básico
    - Auditoría para conocer con detalle el estado de seguridad en la Secretaría General Adjunta de Informática (SGAI) del CSIC
    - Proceso consultivo de las necesidades de los centros del CSIC en materia de seguridad en la medida que éstas trascendiesen los servicios prestados desde la SGAI
    - Elaboración de un plan de acción orientado a gestionar los riesgos detectados
  - Secundario
    - Desarrollo de una política de seguridad
    - Definición de la organización necesaria para gestionar la seguridad en el seno del CSIC
    - Módulo de concienciación de los usuarios sobre la seguridad

2. El pliego. Descripción detallada

- Condiciones del entorno de trabajo para la elaboración del PDSI
  - Metodología de Análisis de Riesgos MAGERIT v2 y la herramienta PILAR
    - Propias de la Administración Pública y gratuitas para los organismos e instituciones públicas
  - Dentro del marco de buenas prácticas de la norma ISO/IEC 27001:2007
    - Cuando se redactó el pliego aún no se conocía el Esquema Nacional de Seguridad

2. El pliego. Descripción detallada

- Aspectos de seguridad a considerar
  - Organizativos
    - Política y organización de la seguridad
    - Gestión de activos
    - Gestión de incidentes
  - Recursos humanos
    - Gestión de la continuidad de negocio
  - Legales
    - Conformidad con la legalidad vigente
  - Lógicos
    - Control de accesos
    - Adquisición, desarrollo y mantenimiento de sistemas
    - Integridad de datos y confidencialidad
  - Físicos

2. El pliego. Descripción detallada

- Fases
  - Análisis de la situación actual
  - Análisis de riesgos
  - Análisis de vulnerabilidades
  - Consultas sobre el estado de la seguridad en los centros del CSIC
  - Definición de la política y organización de la seguridad
  - Definición del plan de acción
  - Concienciación de la seguridad
- Listado detallado de todos los entregables

2. El pliego. Descripción detallada

- Análisis de la situación actual
  - Objetivo
    - Recopilar información necesaria a nivel físico y lógico de los sistemas, comunicaciones, servicios y medidas de seguridad existentes
  - Tareas
    - Recopilación de la documentación existente
    - Reuniones con usuarios finales y responsables de las unidades
    - Revisión de las plataformas tanto a nivel hardware como software
    - Revisión de la estructura de comunicaciones
    - Revisión de la política de seguridad previa
    - Revisión de la adecuación y cumplimiento de la legislación vigente

2. El pliego. Descripción detallada

- Análisis de riesgos
  - Objetivo
    - Análisis de riesgos cualitativo (y cuantitativo) en base a la información recopilada de los activos y procesos de la organización
    - Identificación de amenazas, vulnerabilidades y su impacto sobre los activos
  - Tareas
    - Identificación y valoración de los activos
    - Identificación y descripción de las amenazas
    - Identificación y evaluación de las vulnerabilidades
    - Identificación y valoración de los impactos
    - Identificación de las salvaguardas establecidas, las planeadas y la necesidad de implantar otras nuevas
    - Evaluación del riesgo
    - Nivel de cumplimiento de la ISO 27002

2. El pliego. Descripción detallada

- Análisis de vulnerabilidades
  - Objetivo
    - Obtener una visión global del estado de la seguridad a niveles físico y lógico de los elementos definidos como críticos en el *Análisis de la situación actual*, tanto en la red interna como en la externa
  - Condición
    - Pruebas que no originen denegación o degradación de servicio
  - Tareas
    - Escaneo de puertos y vulnerabilidades
    - Descubrimiento de protocolos, servicios y servidores
    - Pruebas de filtrado de acceso, tanto desde el exterior como en el red interna
    - Estado de las credenciales, permisos y escalado de privilegios
    - Acceso a ficheros y bases de datos
    - Estado de algunas redes como WI-FI y VoIP

2. El pliego. Descripción detallada

- Estudio del estado de la seguridad en los centros del CSIC
  - Entrevistas a 6 centros de distinta tipología
    - Centros propios
    - Centros mixtos
    - Centros con instalaciones especiales
    - Centros con ubicaciones problemáticas
  - Los datos serán incluidos en un informe para
    - Mostrar su situación
    - Incluir sus necesidades dentro del Plan de Acción
    - Incluir sus características en las Políticas de Seguridad

2. El pliego. Descripción detallada

- Definición del Plan de Acción
  - Identificar las medidas y acciones correctoras necesarias a adoptar para reducir el nivel de riesgo y aumentar los niveles de seguridad en un plazo de 2 años
  - Distinguir entre actuaciones a corto, medio y largo plazo
  - Elaborar un calendario de implantación
  - Describir información detallada de cada tarea
    - Objetivos a alcanzar
    - Contenido y alcance de la acción
    - Estimación del esfuerzo necesario en cuanto a recursos personales y económicos
    - Dependencias e interrelación con otras tareas
    - Planificación

CSIC
Consejo Superior de Investigaciones Científicas

2. El pliego. Equipo de trabajo

- Equipo mínimo de 3 personas
  - Jefe de proyecto
  - Consultor estratégico
  - Consultor senior
- Experiencia mínima exigida de 3 años en proyectos similares
- Valorables las certificaciones
  - ISO 20001, ISO 27001
- Al menos una de las personas del equipo debía contar alguna de las certificaciones oficiales de seguridad
  - CISSP, CISM y CISA

CSIC
Consejo Superior de Investigaciones Científicas

2. El pliego. Equipo de trabajo

- Formularios de personal y de empresa para facilitar la lectura de los datos aportados
  - Personal
    - Actividades en empresas
    - Formación tecnológica y académica
    - Participación en proyectos similares
  - Empresa (indicación de las páginas donde se encuentra la información solicitada)
    - Datos relevantes referentes a la oferta
    - Certificaciones
    - Otras prestaciones
    - Proyectos similares
    - Relación de los miembros del equipo de trabajo y porcentaje de tiempo dedicado al proyecto

CSIC
Consejo Superior de Investigaciones Científicas

3. El concurso

- Se presentaron más de 20 empresas
  - Expertas en consultoría y auditoría
  - Los más conocidos integradores nacionales
  - Con diversa experiencia en materia de seguridad, en general, y de auditoría de seguridad en particular
- Hubo un buen equilibrio entre la oferta económica y la valoración técnica

CSIC
Consejo Superior de Investigaciones Científicas

4. Los inicios

- Reuniones, reuniones y más reuniones y muchas complicaciones para concertarlas
- Algunas dificultades para recopilar la información adecuada
  - ¿… y dónde está esa información?
  - ¿… y quién se encarga de …?
  - ¿Cuándo vas a enviarnos la información que te hemos pedido?
- Algunas dificultades con la terminología
  - Exactamente, ¿qué me estás preguntando?

CSIC
Consejo Superior de Investigaciones Científicas

5. El desarrollo

- Disminuye el número de reuniones externas pero no las relacionadas con el seguimiento del proyecto
- Aparecen las versiones iniciales de los informes y hay que revisarlas
- Continúan las dificultades de recopilación de información para completar los informes que se van generando
- Se van superando las dificultades con la terminología

6. Los resultados

- Informes, informes y más informes
  - Situación actual
  - Entrevistas con los centros
  - Adecuación a la LOPD
  - Adecuación a la ISO 27002
  - Vulnerabilidades técnicas encontradas
  - Análisis de riesgos para las unidades evaluadas
  - Ficheros de trabajo e informes extraídos de la herramienta PILAR
  - Política de seguridad
  - Organización de la seguridad y Plan Director para los próximos 3 años → demasiados proyectos para 2 años

CSIC
Consejo Superior de Investigaciones Científicas

6. Los resultados. Un ejemplo

- Análisis de la desviación en el cumplimiento de ISO 27002. Índice del documento
  - Alcance del trabajo y limitaciones del mismo
  - Descripción del trabajo realizado
  - Resumen ejecutivo
  - Situación actual
  - Resultados obtenidos
  - Recomendaciones
  - Anexo I. Tabla de madurez de los controles ISO 27002
  - Anexo II. Estado actual de los controles ISO 27002

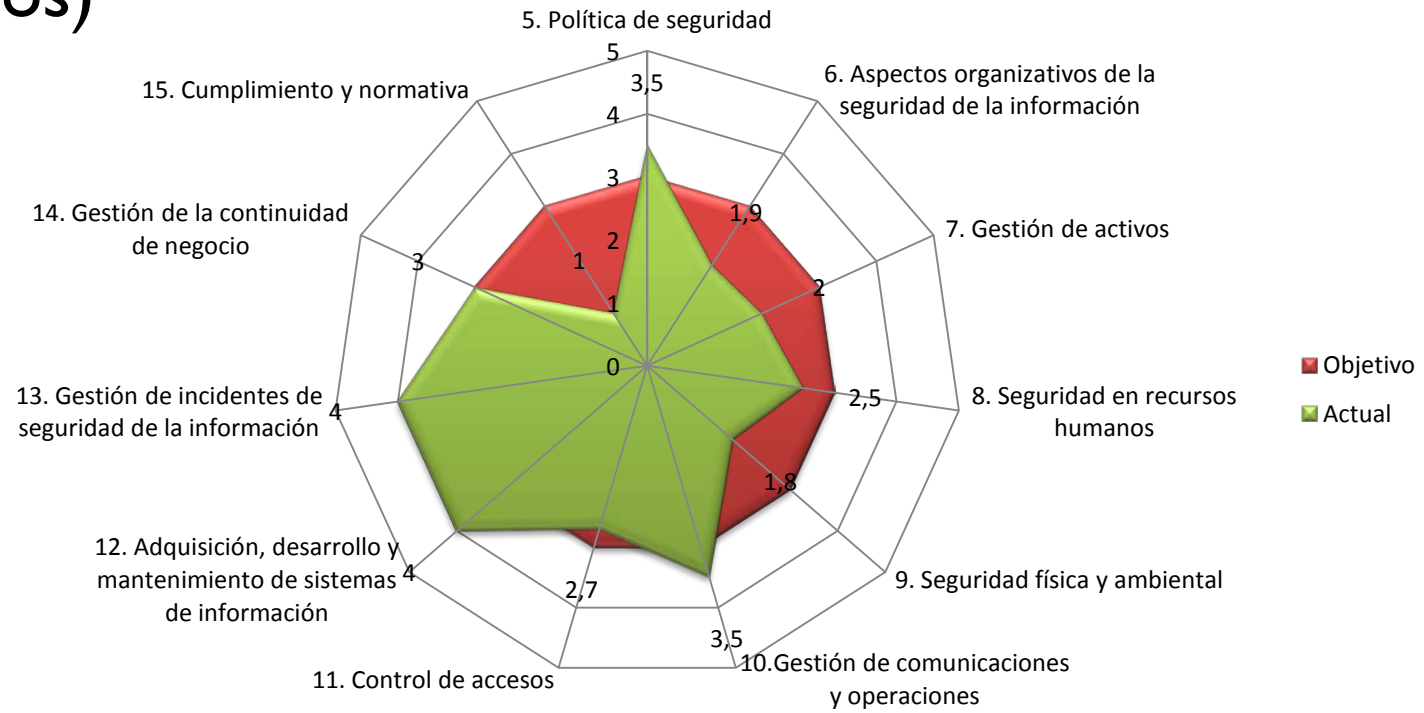
6. Los resultados. Un ejemplo

- Análisis de la desviación en el cumplimiento de ISO 27002. Resultados obtenidos
  - Descripción de la situación actual en cuanto al cumplimiento de la norma para cada uno de los 11 dominios de seguridad definidos en dicha norma
  - Niveles de madurez definidos
    - 0 – Inexistente
    - 1 – Inicial
    - 2 – Gestionado
    - **3 – Definido**
      - **La organización en su conjunto participa del proceso**
      - **Los procedimientos están implantados, documentados y comunicados mediante formación**
    - 4 – Cuantitativamente gestionado
    - 5 – Optimizado

Nuestro objetivo

6. Los resultados. Un ejemplo

- Análisis de la desviación en el cumplimiento de ISO 27002. Gráfica de los resultados obtenidos (datos ficticios)



CSIC
Consejo Superior de Investigaciones Científicas

6. Los resultados

- Resumen general
  - Nivel técnico aceptable
  - Nivel organizativo deficiente
- No hubo grandes sorpresas
  - Los resultados de los estudios confirmaron lo que más o menos ya se sabía
  - Quedaron registradas por escrito las deficiencias que ya conocíamos y algunas otras que ignorábamos

CSIC
Consejo Superior de Investigaciones Científicas

6. Los resultados

- Percepción general del desarrollo y los resultados del proyecto
  - Prometedor inicio
  - Buen desarrollo
  - Cierta desilusión con los resultados
    - No aportan muchos datos en materia de seguridad para los responsables de esta tarea en la institución
    - En la primera impresión, las recomendaciones parecen sacadas de un manual de buenas prácticas

CSIC
Consejo Superior de Investigaciones Científicas

6. Los resultados

- Lo mejor
  - Red WI-FI
  - VoIP
  - Aplicaciones más recientes
  - Concienciación en parte del personal
- Lo peor
  - Aspectos organizativos
  - Falta de un inventario único
  - Falta de seguridad en algunas aplicaciones antiguas (en proceso de cambio)
  - Falta de concienciación en parte del personal

CSIC
Consejo Superior de Investigaciones Científicas

7. El después

- Tareas inmediatas
  - ➢ Aprobación de la Política de Seguridad
  - ➢ Aprobación de la Organización de Seguridad
  - ➢ Adecuación a la LOPD
  - ❖ Redacción de los procedimientos de seguridad
  - ❖ Actualización y homogenización del inventario y clasificación de los activos
  - ❖ Definición del plan de recuperación de desastres
  - ❖ Definición del plan de continuidad de negocio

➢ Proyecto en marcha
❖ Se iniciará en breve
❑ Pilotos

CSIC
Consejo Superior de Investigaciones Científicas

7. El después

- Otras tareas
  - ❖ Revisión de la política y de la organización de seguridad para adecuarlas al Esquema Nacional de Seguridad
  - ➢ Auditorías periódicas
  - – Proyectos tecnológicos
    - ➢ Gestión de identidades, usuarios y permisos
    - ❑ NAC
    - ❑ Cortafuegos de aplicaciones

7. El después. Comparación con ENS

PDSI – CSIC

1) Política de seguridad de la información
2) Organización de seguridad de la información
3) Gestión de activos
4) Seguridad relacionada con los recursos humanos
5) Seguridad física y del entorno
6) Gestión de comunicaciones y operaciones
7) Control de acceso
8) Adquisición, desarrollo y mantenimiento de los sistemas de información
9) Gestión de incidentes de seguridad de información
10) Gestión de la continuidad del negocio
11) Cumplimiento

ENS

1) Organización e implantación del proceso de seguridad
2) Análisis y gestión de riesgos
3) Gestión de personal
4) Profesionalidad
5) Autorización y control de los accesos
6) Protección de las instalaciones
7) Adquisición de productos
8) Seguridad por defecto
9) Integridad y actualización del sistema
10) Protección de la información almacenada y en tránsito
11) Prevención ante otros sistemas de información interconectados
12) Registro de actividad
13) Incidentes de seguridad
14) Continuidad de la actividad
15) Mejora continua del proceso de seguridad

8.Y al final …¿qué?

- Pregunta:

  ¿Es recomendable elaborar un plan director de seguridad de la información?

- Respuesta:

Sin ninguna duda

8.Y al final …¿qué?

- Pregunta:

¿Por qué es recomendable?

- Respuesta:

Clarifica mucha información sobre la institución, no sólo de seguridad

Estupendo punto de partida para intentar poner un poco de orden

8.Y al final …¿qué?

- Pregunta:

¿Y si en mi institución al final no aprueban nada?

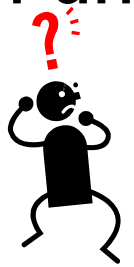
- Respuesta:

Puede que no lo hagan inmediatamente pero los estudios realizados, los datos obtenidos y algunas de las indicaciones apuntadas seguro que son útiles y se acaban implantando

8.Y al final …¿qué?

- Pregunta:

¿Es buen momento para empezar a pensar en un plan director de seguridad?

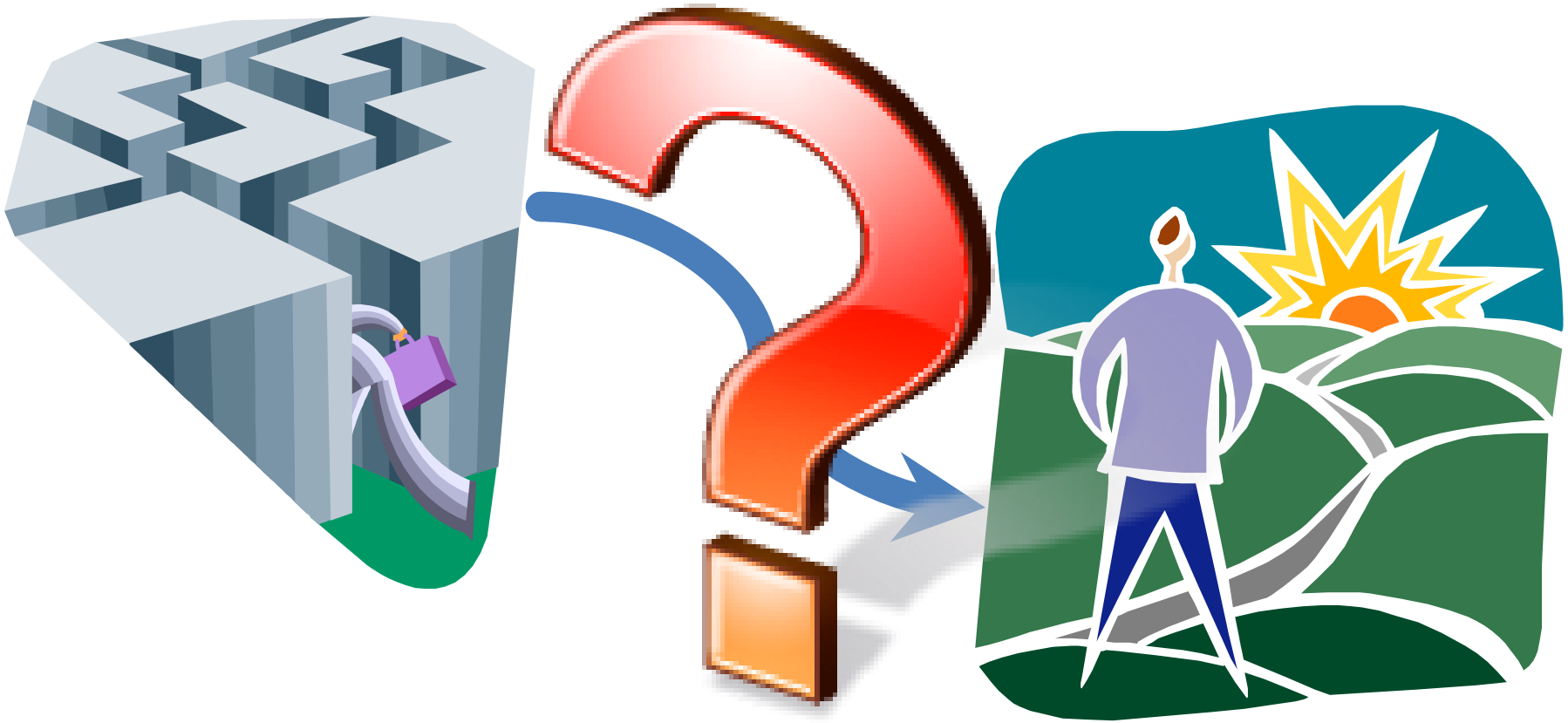


- Respuesta:

El mejor porque en estos momentos hay un importante aumento de la sensibilidad en materia de seguridad

CSIC
Consejo Superior de Investigaciones Científicas

8.Y al final …¿qué?



MINISTERIO
DE CIENCIA
E INNOVACIÓN

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS

GRACIAS POR SU ATENCIÓN