

# sira

## Seguridad Informática en la Red Académica

Iñaki Ortega [inaki.ortega@ehu.es](mailto:inaki.ortega@ehu.es)

Universidad del País Vasco / Euskal Herriko Unibertsitatea



# Lema

Fomentar las buenas  
prácticas en materia de  
seguridad informática  
dentro de las  
instituciones afiliadas a  
RedIRIS



# Agenda

- Breve historia de SIRA
- Estado de SIRA en los GT de Santiago
- Avances desde los GT de Santiago
- Descripción del informe de resultados
- Demo: formsira
- Proximas acciones
- Futuro de SIRA



# Breve historia de SIRA

Mayo 2008: GT Valencia	¿Porqué no hacemos un RACE para seguridad? Javier García, UM
Junio 2008	Se forma el grupo inicial con nombre REQSEG (REquisitos de SEGuridad)
Noviembre 2008: JT Alcalá de Henares	Se presenta la iniciativa con el nombre de SIRA
Abril 2009: GT Málaga	Tras los GT de Málaga en los que se presentan las líneas de trabajo del grupo y se realiza la 2ª reunión presencial
Noviembre 2009: GT Santiago	Se informa sobre los avances de los últimos meses y se presenta el cuestionario que servirá de base a la evaluación del estado de la seguridad de las Instituciones

# Qué es SIRA

- Sira NO es un RACE
- Herramienta de autoevaluación a partir de ISO 27002 adaptada a la comunidad de RedIRIS
- Informe de diagnóstico y recomendaciones





# Estado de SIRA en los GT de Santiago

- La ISO 27002 se separó por dominios y los llamamos secciones
- Se extrajeron los controles más interesantes de cada dominio para crear las preguntas del cuestionario
- Se creó el cuestionario y se adecuó al perfil de las Instituciones afiliadas a RedIRIS
- Se creó una aplicación a modo de herramienta para poder acceder y rellenar el cuestionario y presentar los resultados



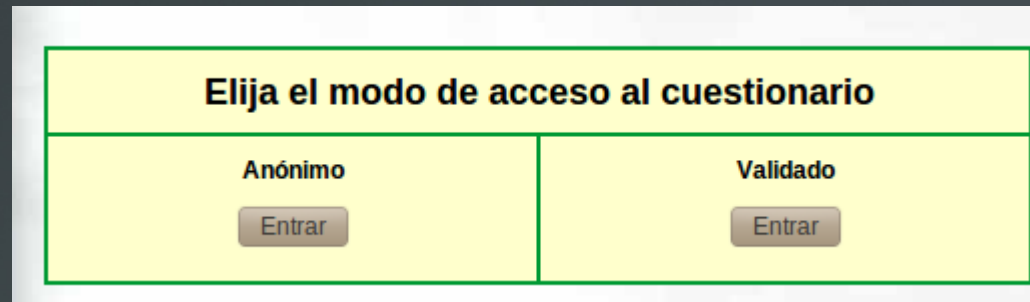
# Avances desde los GT de Santiago

- Mejoras en el acceso a la aplicación
- Mejoras en el cuestionario
- Mejoras en la aplicación
- Mejoras en la presentación de los resultados



# Mejoras en el acceso a la aplicación

- Tipos de acceso:



The image shows a screenshot of a web interface for selecting questionnaire access mode. The title is "Elija el modo de acceso al cuestionario". Below the title, there are two columns. The left column is labeled "Anónimo" and contains a button labeled "Entrar". The right column is labeled "Validado" and contains a button labeled "Entrar".









Elija el modo de acceso al cuestionario	
Anónimo	Validado
<input type="button" value="Entrar"/>	<input type="button" value="Entrar"/>

- ¿Quién tiene acceso a la aplicación?
  - Anónimo: Cualquiera
  - Validado: Responsables de seguridad TIC de las Instituciones



# Mejoras en el acceso (2)

- Diferencias hay entre el modo anónimo y el modo validado

Facilidad Modo	Acceso al cuestionario	Rellenar el cuestionario en varias sesiones	Asociar un proceso a la evaluación	Obtener el informe con los resultados
Anónimo				
Validado				

# Mejoras en el cuestionario

- ✓ Se ha añadido una introducción al cuestionario
- ✓ Se ha añadido una introducción a cada sección
- ✓ Se ha añadido una introducción a la mayoría de las preguntas del cuestionario



# Mejoras en la aplicación

- ✓ Se ha mejorado la integración con SIR
- ✓ Se han puesto las preguntas en contexto en base a las introducciones del cuestionario
- ✓ Se han corregido muchos bugs que han ido apareciendo



# Mejoras en la presentación de los resultados

- x Se eliminado la nota final
- ✓ Se ha añadido una visión global de los resultados
  
- x Se ha eliminado el diploma o certificado
- ✓ Se ha creado el informe con los resultados del cuestionario



# Visión global de los resultados

## FIN DE LA ENCUESTA

**GRADO DE CUMPLIMIENTO: 49 %**

<b>Sección 1: Política de seguridad</b>	<b>80%</b>
<b>Sección 2: Aspectos organizativos de la seguridad de la información</b>	<b>52%</b>
<b>Sección 3: Gestión de activos</b>	<b>50%</b>
<b>Sección 4: Seguridad ligada a los recursos humanos</b>	<b>48%</b>
<b>Sección 5: Seguridad física y ambiental</b>	<b>45%</b>
<b>Sección 6: Gestión de comunicaciones y operaciones</b>	<b>46%</b>
<b>Sección 7: Control de acceso</b>	<b>42%</b>
<b>Sección 8: Adquisición, desarrollo y mantenimiento de los sistemas de información</b>	<b>55%</b>
<b>Sección 9: Gestión de incidentes en la seguridad de la información</b>	<b>40%</b>
<b>Sección 10: Gestión de la continuidad del negocio</b>	<b>60%</b>
<b>Sección 11: Cumplimiento de los requisitos legales</b>	<b>53%</b>

[Ver informe completo](#)



# Estructura del Informe de resultados

- Cabecera
- Gráfica de radar
- Tres secciones peor valoradas
- Resultados completos
  - Resultados de sección
  - Resultados de pregunta



# Informe de resultados: Cabecera

Proceso  
(modo validado)

Imprimir

INFORME SIRA

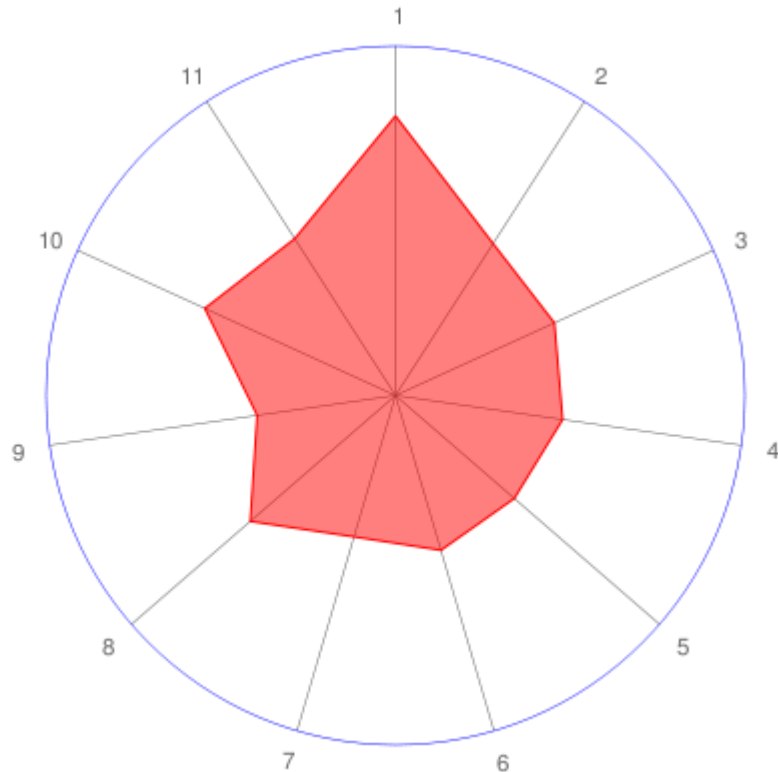


Proceso	Gestión Académica	Fecha	13/06/2010
Email	inaki.ortega@ehu.es	Institución	ehu.es

Quien rellena  
el cuestionario  
(modo validado)

Institución  
(modo validado)

# Informe de resultados: Gráfica de radar



- 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 sistemas de información
- 9 Gestión de incidentes en la seguridad de la información
- 10 Gestión de la continuidad del negocio
- 11 Cumplimiento de los requisitos legales

# Informe de resultados: Tres secciones peor valoradas

## Secciones peor valoradas

<u>9 Gestión de incidentes en la seguridad de la información</u>	40%
<u>7 Control de acceso</u>	42%
<u>5 Seguridad física y ambiental</u>	45%

# Informe de resultados: Resultados de sección

Grado de  
Cumplimiento  
de la sección

## Sección 2: Aspectos organizativos de la seguridad de la información

52%

Se debe establecer un marco de gestión para controlar el grado de aplicación de la seguridad de la información dentro de la Institución. Esta gestión debe aprobar la política de seguridad, asignar roles y coordinar y revisar la implementación de la seguridad en la Institución.

Si es necesario, debe ponerse a disposición de la Institución fuentes de información especializadas en seguridad. Se deben establecer contactos con especialistas o grupos externos de seguridad, incluidas las autoridades pertinentes, de cara a mantenerse al día con las tendencias industriales, supervisión de las normas y métodos de evaluación y proporcionar puntos de enlace adecuados para solventar los incidentes de seguridad. Se debe dar un enfoque multidisciplinario a la seguridad de la información.



# Informe de resultados: Resultados de pregunta

- Pregunta de respuesta única

## Pregunta 1.1

¿Existe en la Institución un documento que recoja la política de la seguridad de la información?

- No existe	0.00
- Sí existe, pero no está aprobado, no está publicado y por tanto no es conocido por los usuarios	0.20
- Si existe, está aprobado por la Dirección de la Institución, es de obligado cumplimiento pero no está publicado y por tanto no es conocido por los usuarios	0.40
- Sí existe, está aprobado por la Dirección de la Institución, es de obligado cumplimiento, está publicado y es conocida por los usuarios	0.80
- Además de la respuesta anterior se realizan revisiones periódicas del documento y se modifica si es necesario	1.00

Respuesta  
marcada

# Informe de resultados: Resultados de pregunta

- Pregunta de respuesta múltiple

## Pregunta 2.3

Se deben establecer contactos con especialistas o grupos externos de seguridad, incluidas las autoridades pertinentes, de cara a mantenerse al día con las tendencias industriales, supervisión de las normas y métodos de evaluación y proporcionar puntos de enlace adecuados para solventar los incidentes de seguridad.

### Mantiene su Institución contactos con:

- RedIRIS	0.25
- ISPs	0.25
- Fuerzas de seguridad del Estado	0.25
- Otros grupos de interés y foros de seguridad	0.25
- Ninguna de las anteriores	0.00

# Demo: formsira





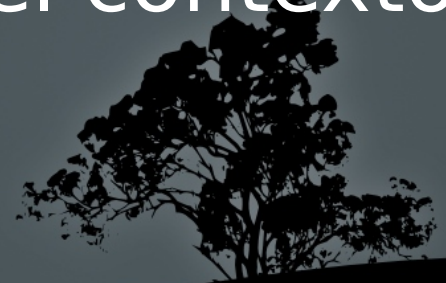
# Próximas acciones

- Liberar formsira **Beta**
  - Cambiar el dominio de la URL
  - Disponer de dirección de email de contacto
  - Limpiar la Base de Datos
  - Anunciar la disponibilidad de la herramienta en las listas de RedIRIS



# Futuro de SIRA

- Vuestro Feedback
  - Preguntas
  - Sugerencias
- Participación en el Grupo
- Uso de la herramienta
- Esquema Nacional de Seguridad (ENS)
  - ¿Tiene sentido SIRA en el contexto del ENS?





# Recursos

- Evaluación (en breve)

<https://formsira.rediris.es>

**Beta**

- SITE: Google Site

<https://sites.google.com/site/redirissira/>

- Lista de distribución

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

- Web RedIRIS

<http://www.rediris.es/actividades/gt-sira/>

# Agradecimientos

- A todos los miembros del grupo
- Y en especial a las Instituciones más activas
  - CSIC
  - RedIRIS
  - Universidad de Castilla la Mancha
  - Universidad de Murcia
  - Universidad de Santiago de Compostela
  - Universidad del País Vasco / Euskal Herriko Unibertsitatea



# ¿Preguntas?

