

sira

Seguridad Informática en la Red Académica

Iñaki Ortega inaki.ortega@ehu.es

Universidad del País Vasco / Euskal Herriko Unibertsitatea



RedIRIS

Jornadas Técnicas RedIRIS 2009
Santiago de Compostela

Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Lema

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

Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Repaso de la iniciativa

- Mayo de 2008: GT Valencia

¿Porqué no hacemos un RACE para seguridad?

Javier García, UM

- Junio de 2008

- Se forma el grupo inicial con nombre REQSEG (REQuisitos de SEGuridad)

- Noviembre de 2008: GT de Alcalá

- Se presenta la iniciativa con el nombre de SIRA
 - Tras la 1^a reunión presencial a la que se incorporan nuevos miembros se cambia el enfoque de la iniciativa

- Abril de 2009: GT de Málaga

- Tras los GT de Málaga en los que se presentan las líneas de trabajo del grupo y se realiza la 2^a reunión presencial
 - Se planifica el trabajo para los próximos seis meses coincidiendo con los GT de Santiago
 - Se captan nuevos colaboradores para el grupo

Repaso de la iniciativa

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



Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Avances desde los GT de Málaga

- Dividir la ISO 27002 en dominios y repartirlos entre los integrantes del grupo
- Desmenuzar los controles de cada dominio para extraer las preguntas de la encuesta
- Crear la encuesta
- Revisar la encuesta en conjunto
- Adecuarla al perfil de las Instituciones afiliadas a RedIRIS
- Crear aplicación de apoyo

Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Presentación de la encuesta

- Encuesta basada en unas 40-45 preguntas agrupadas en 11 secciones
- Estado actual de la encuesta “Beta” a partir de la ISO y faltan preguntas y/o secciones de la comunidad de RedIRIS
- Dos tipos de preguntas: Respuesta simple o respuesta múltiple
- Hemos creado una aplicación de apoyo que permite gestionar la encuesta facilitando el acceso al cuestionario y la forma de rellenarla

Secciones

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

Pregunta de respuesta única

Pregunta: ¿Se establecen acuerdos de confidencialidad y no divulgación sobre el acceso e intercambio de información?

- No
- Sí, sólo para el personal interno
- Sí, sólo para terceros
- Sí, tanto para personal interno como para terceros
- Sí, para ambos y además se revisan periódicamente

Pregunta de respuesta múltiple

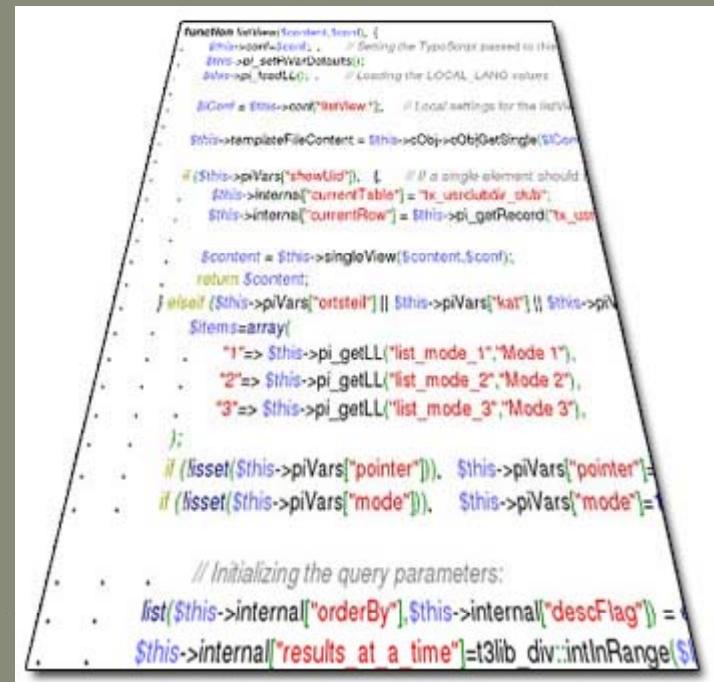
Pregunta: Mantiene su Institución contactos con:

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

Aplicación de apoyo

● Varias alternativas:

- Hoja tipo excel
- Aplicación existente
- Otro tipo de soluciones
- Desarrollo específico



```
function piViewRecord($recId) {
    $piVars->pi_setRecord($recId); // Setting the Type/Source passed to the
    $this->pi_setViewDetails(); // $this->pi_loadLoc(); // Loading the LOCAL_LANG values
    $sConf = $this->conf["view"]; // Local settings for the view
    $this->templateFileContent = $this->piObj->piObjGetSingle($sConf);

    if ($this->piVars["showId"], 1, // If a single-element should
       $this->internal["currentTable"] = "tx_urcadatav_ueb";
       $this->internal["currentRow"] = $this->pi_getRecord("tx_urcadatav_ueb"));

    $sContent = $this->singleView($content, $conf);
    return $sContent;
} elseif ($this->piVars["ortsteil"] || $this->piVars["kai"] || $this->piVars["pointer"]) {
    $items = array(
        "1" => $this->pi_getLL("list_mode_1", "Mode 1"),
        "2" => $this->pi_getLL("list_mode_2", "Mode 2"),
        "3" => $this->pi_getLL("list_mode_3", "Mode 3"),
    );
    if (!isset($this->piVars["pointer"])) { $this->piVars["pointer"] = 1; }
    if (!isset($this->piVars["mode"])) { $this->piVars["mode"] = 1; }

    // Initializing the query parameters:
    list($this->internal["orderBy"], $this->internal["descFlag"]) =
        $this->internal["results at a time"] = t3lib_div::intInRange($
    $this->internal["results at a time"], 1, 100);
}
```

Aplicación de apoyo

◎ Nos decidimos por un desarrollo propio por:

- Disponer de recursos humanos preparados
- Disponer de las herramientas necesarias
- Disponer de tiempo
- Con el desarrollo propio tenemos el control

Requisitos de la aplicación

- Agnóstica al Sistema Operativo y al Navegador
- Desarrollada con software libre (LAMP)
- Acceso público (frontend) y administrativo (backend)
- Tres modos de uso:
 - Test: No es necesaria la autenticación
 - Encuesta: Hay que autenticarse en la aplicación
 - Administración: Hay que autenticarse en la aplicación
- Autenticación mediante SIR

Demo



Sergio Escribano sergio.escribano@ehu.es

Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Tareas pendientes

- Añadir, quitar o modificar preguntas en la encuesta
- Asignación de pesos a las secciones
- Asignación de puntuaciones a las preguntas dentro de su sección
- Proponer medidas correctoras según el resultado de las secciones
- Refinar el método de autenticación (pendientes del desarrollo de la figura del PEC)

Agenda

- Repaso de la iniciativa
- Avances desde los GT de Málaga
- Presentación de la encuesta
- Tareas pendientes
- El futuro de sira

Futuro de sira

● Esquema Nacional de Seguridad

- Desarrolla el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos donde se habla de la seguridad en la utilización de medios electrónicos en la Administración Electrónica.
- Será una reglamentación de obligado cumplimiento dentro de las Administraciones Públicas para garantizar la seguridad informática de los trámites online, y por ende, la seguridad jurídica. Dado que la validez jurídica y robustez de los procesos administrativos recae en la informática, ahora es necesario garantizar que no habrá problemas jurídicos cuando todo se base en la tecnología.

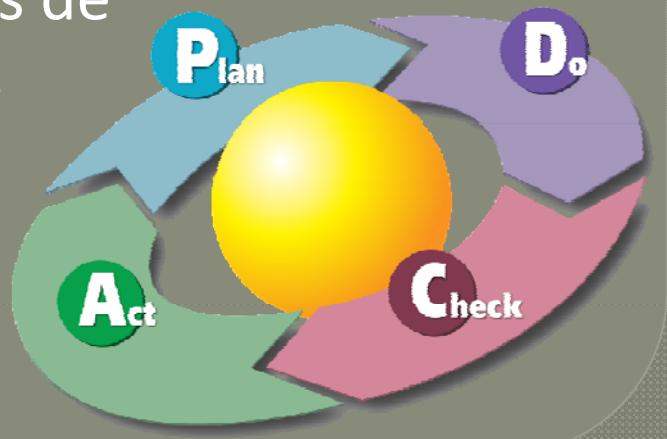
http://www.csae.map.es/csi/pdf/20090715_Proyecto_RD_ENS_cn.pdf

Futuro de sira

○ ISO27004

- La ISO27001 establece un marco de gestión dentro de las organizaciones pero no significa que exista una buena seguridad.
- La ISO27004 establece criterios para la medición del estado de la seguridad lo que permite conocer si las medidas de seguridad están funcionando o no.

http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106



Recursos de SIRA

- 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/>

- Encuesta (Beta)

- <http://158.227.1.23/>



Realimentación

- Como siempre necesitamos vuestras opiniones

- Apúntate al GT-SIRA
- Critica lo hecho o aporta ideas nuevas
- Usa la encuesta y ayúdanos a mejorarla
- Danos tu opinión
- Seguro que tienes algo que aportar

Contacta con nosotros cuando lo necesites

Agradecimientos

RedIRIS - UCLM - UM -
UPV/EHU - UPO – USC -
CSIC - URV - Unirioja -
UPC - UAL – Unavarra -
Etc...