Universidad Politécnica de Cartagena

Proceso de adaptación al ENS en la UPCT

Francisco J. Sampalo Lainz
Universidad Politécnica de Cartagena
Paco.sampalo@si.upct.es

CAMPUS MARE NOSTRUM

Programa

Universidad Politécnica de Cartagena

1. Consideraciones previas.
2. ¿Cómo lo hemos abordado en la UPCT?
3. Descripción del proceso.
4. Siguientes pasos.
5. Conclusiones y opiniones

Consideraciones previas

- El proceso debía ser de utilidad REAL; sería la forma de empezar a realizar una gestión GLOBAL de la seguridad.
- Debía ser sencillo y asumible (dentro de nuestras limitaciones).
- La Universidad no disponía de una política de seguridad debidamente aprobada.
- Se debía implicar a todas las secciones del Servicio de Informática.
- ***"La UPCT desea manifestar la necesidad de una infraestructura TIC que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales."*** (extraído de la Política de seguridad de la UPCT)

¿Cómo lo hemos abordado?

Personas implicadas

Universidad Politécnica de Cartagena

- Vicerrectora de Nuevas Tecnologías.
- Jefe del Servicio de Informática.
- Jefes de las secciones del SI (4 en total).
- Un técnico de Sistemas.
- Un consultor externo.

Plan de trabajo

Universidad Politécnica de Cartagena

1. Curso de formación sobre ENS y Gestión de riesgos (Nov-2010). Para todo el Servicio de Informática.
2. Elaboración y publicación de la Política de seguridad (https://sede.upct.es/docs/ENS_PoliticaSeguridadUPCT.pdf)
3. Catalogación y valoración de los Sistemas de Información según lo establecido en el ENS.
4. Análisis de Riesgos.
5. Plan de mejora.
6. Informe final.

- 10 reuniones en total, comenzando el 1 de feb y finalizando el 12 de mayo.

Herramientas utilizadas

Universidad Politécnica de Cartagena

- **Esquema Nacional de Seguridad.**
- **Guías CCN-STIC:** https://www.ccn-cert.cni.es
- **MAGERIT.**
- **PILAR v 5.1.**

Descripción del proceso.

Paso 1: Identificación y valoración de los sistemas de información

Valoración de los servicios (criterios)

Universidad Politécnica de Cartagena

• Los criterios seguidos para la inclusión de los servicios e informaciones en la adecuación al ENS son los referidos por la Ley 11/2007: aquellos sistemas de información relacionados con el ejercicio de derechos y de deberes de acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

•Además, se decidió incluir aquellos que tienen especial significación para la universidad, bien sea por los daños reputacionales que se desprenderían de un incidente de seguridad en los mismos, bien por la creciente importancia que van adquiriendo.

•Las dimensiones de los servicios han sido valoradas por criterios desligados de la información. La confidencialidad del servicio ha sido valorada por su difusión y restricciones de acceso. La autenticidad del servicio ha sido valorada según el impacto que causaría el hecho de que un tercero suplantara el servicio legítimo. La integridad del servicio ha sido valorada como la posibilidad de que el funcionamiento o finalidad del servicio sea alterada. La disponibilidad del servicio ha sido valorada independientemente de la existencia de información en aquellos casos que ha sido posible.

Valoración de los servicios (resultados)

Universidad Politécnica de Cartagena

Servicio	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global	Aplicabilidad ENS
ERP - Académico	Bajo	Medio	Medio	Bajo	Bajo	Medio	Aplica
ERP - Económico	Bajo	Medio	Medio	Bajo	Bajo	Medio	Aplica
ERP - RRHH	Medio	Bajo	Medio	Bajo	Bajo	Medio	Aplica
ERP - SiCARTA	Bajo	Bajo	Medio		Bajo	Medio	Aplica
ERP - Registro Presencial	Medio			Bajo	Bajo	Medio	Aplica
ERP - Cursos Propios	Bajo	Bajo	Medio	Bajo	Bajo	Medio	Aplica
ERP - Gestión Ayudas Sociales	Medio*	Bajo	Bajo	Bajo		Medio*	Aplica
ERP - Portal	Bajo	Bajo	Medio	Bajo	Bajo	Medio	Aplica
Web Institucional		Bajo	Bajo		Medio	Medio	Ampliación ENS
Docencia Virtual	Bajo		Medio	Bajo	Medio	Medio	Ampliación ENS
AE - Sede		Medio	Medio	Bajo	Medio	Medio	Aplica
AE - Tablón Oficial		Medio	Medio	Bajo	Medio	Medio	Aplica
AE - Portafirmas	Bajo	Medio	Medio	Bajo	Bajo	Medio	Aplica
AE - Registro Telemático + Tramitación	Medio	Medio	Medio	Medio	Bajo	Medio	Aplica
AE - Factura Electrónica	Bajo	Medio	Medio	Bajo	Bajo	Medio	Aplica
Dumbo	Bajo		Medio		Bajo	Medio	No aplica
ALAs		Bajo	Bajo	Bajo		Bajo	No aplica
ERP - Évalos	Bajo	Bajo	Bajo	Bajo		Bajo	No aplica

Sistemas identificados

Universidad Politécnica de Cartagena

Sistema	Servicio	Aplicabilidad ENS
Sistema ERP Institucional	ERP – Académico	Aplica
Sistema ERP Institucional	ERP – Económico	Aplica
Sistema ERP Institucional	ERP – RRHH	Aplica
Sistema ERP Institucional	ERP – SiCARTA	Aplica
Sistema ERP Institucional	ERP - Registro Presencial	Aplica
Sistema ERP Institucional	ERP - Cursos Propios	Aplica
Sistema ERP Institucional	ERP - Gestión Ayudas Sociales	Aplica
Sistema ERP Institucional	ERP – Portal	Aplica
Sistema AE - Subsistema Publicación	AE – Sede	Aplica
Sistema AE - Subsistema Publicación	AE - Tablón Oficial	Aplica
Sistema AE - Subsistema Publicación	AE - Factura Electrónica	Aplica
Sistema AE - Subsistema Tramitación	AE – Portafirmas	Aplica
Sistema AE - Subsistema Tramitación	AE - Registro Telemático + Tramitación	Aplica
Sistema Ampliación ENS	Web Institucional	Ampliación ENS
Sistema Ampliación ENS	Docencia Virtual	Ampliación ENS

Catalogación de sistemas

Universidad Politécnica de Cartagena

Sistema	Confidencialidad	Integridad	Autenticidad	Trazabilidad	Disponibilidad	Nivel Global
Sistema ERP Institucional	Medio	Medio	Medio	Bajo	Bajo	Medio
Sistema AE - Subsistema Publicación	Bajo	Medio	Medio	Bajo	Medio	Medio
Sistema AE - Subsistema Tramitación	Medio	Medio	Medio	Medio	Bajo	Medio
Sistema Ampliación ENS	Bajo	Bajo	Medio	Bajo	Medio	Medio

Descripción del proceso.

Paso 2: Análisis de riesgos

Análisis de riesgos: en qué consiste?

Universidad Politécnica de Cartagena

- Activos y su valoración: Relación de activos necesarios para la prestación de los servicios, con sus interrelaciones y su valoración de las dimensiones de seguridad para las capas de información y servicios. Capas: información, servicios, aplicaciones, servicios IT, hosts, hardware, red, ubicaciones y personas.

- Resumen de amenazas y valoración de amenazas: Valoración de las amenazas, incluyendo frecuencia y degradación de los activos afectados.

- Resumen del tratamiento de los riesgos y salvaguardas: Estrategia (plan) para el tratamiento de los riesgos y salvaguardas aplicadas.

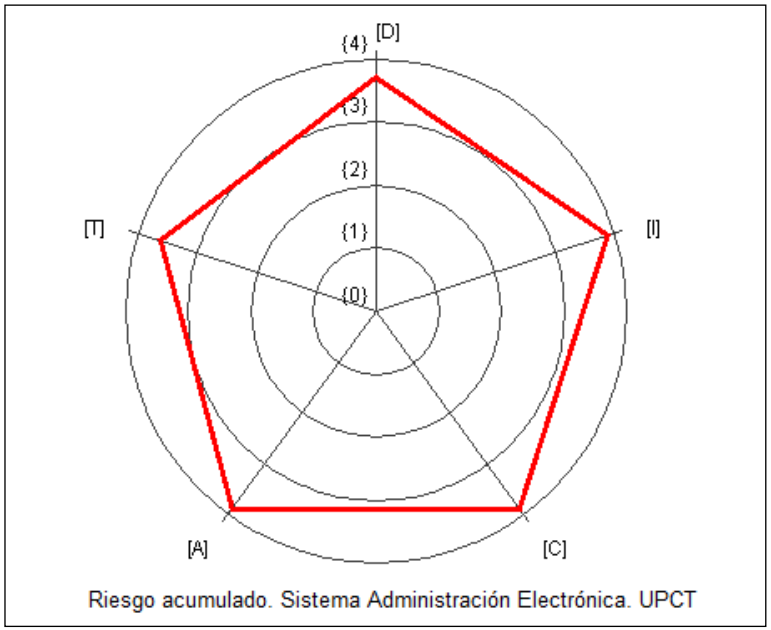
- Resumen de valores residuales de impacto y riesgo: Valores cuantitativos de impacto y riesgo para los activos más significativos.

Análisis de riesgos: qué se obtiene?

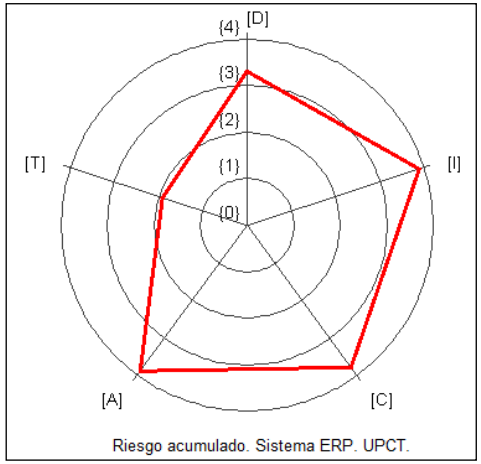
Universidad Politécnica de Cartagena

- Situación actual: Valores del riesgo actual para cada una de las dimensiones de seguridad en cada uno de los sistemas.
- En nuestro caso, se detectó baja madurez y baja homogeneidad en las salvaguardas existentes. Esto lleva a unos niveles de riesgo altos en las dimensiones dominantes de los sistemas.
- Estado actual de cumplimiento del ENS (según checklist en PILAR).
- Se hace una prospectiva de las consecuencias de la aplicación del ENS (según el plan establecido de aplicación de medidas) y se ve claramente la reducción de riesgos que supone.
- Recomendaciones sobre medidas de protección específica de las áreas más significativas de riesgo: políticas de autenticación y contraseñas, concienciación, formación, desarrollo, etc.

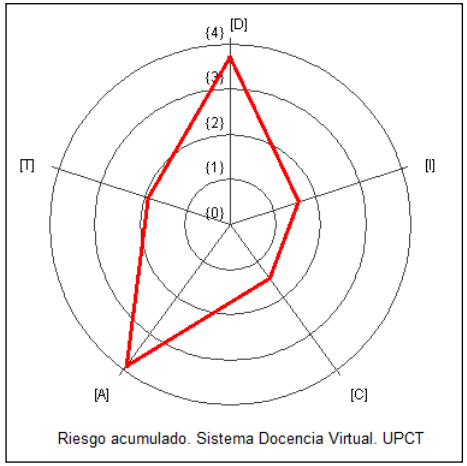
Análisis de riesgos: Situación actual



Riesgo acumulado. Sistema Administración Electrónica. UPCT

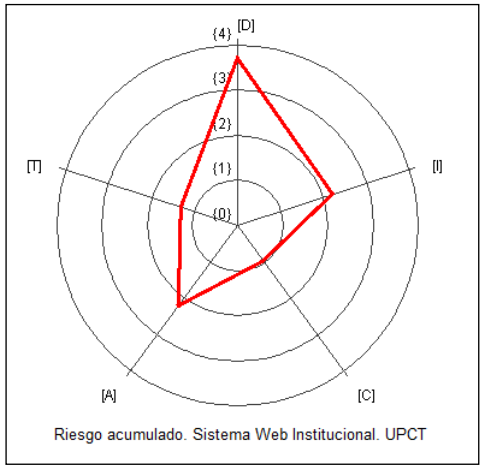


Riesgo acumulado. Sistema ERP. UPCT.



Riesgo acumulado. Sistema Docencia Virtual. UPCT

[org] Marco organizativo	**28 %**
[op] Marco operacional	**44 %**
[mp] Medidas de protección	**42 %**



Riesgo acumulado. Sistema Web Institucional. UPCT

Descripción del proceso.

Paso 3: Plan de mejora

Plan de mejora

- FASE 1– Diciembre 2011
  - Corrección de insuficiencias severas (por debajo del 15% de cumplimiento)
  - Mejora general del marco organizativo
  - Planificación de medidas derivadas del análisis de riesgos

- FASE 2 - Diciembre 2013
  - Corrección de insuficiencias moderadas (por debajo del 30% de cumplimiento)
  - Madurez en las áreas críticas de riesgo

- FASE 3: Desde enero de 2014
  - Madurez en las medidas exigibles por el ENS, alcanzando al menos un 50% en todas las medidas.

Siguientes pasos

Siguientes pasos

Universidad Politécnica de Cartagena

1. Se ha informado al Consejo de Dirección sobre el proceso realizado.
2. Se ha informado a los responsables de la información y de las áreas funcionales sobre el proceso de valoración de los sistemas.
3. Aprobación por parte del CDU del informe y del Plan de Adecuación y de la Normativa de Seguridad (Oct-2011) (https://sede.upct.es/docs/Plan_de_mejora_de_Seguridad_en_la_UPCT.pdf).
4. Se ha informado a todo el personal del SI.
5. Plan de mejora: establecimiento de medidas concretas (ver guía CCN-STIC 808).
6. Tareas de seguimiento.

Ejemplo 1 de medidas en el plan de mejora

Universidad Politécnica de Cartagena

Op.acc.6: Acceso local (local logon):

Se considera acceso local al realizado desde los puestos de trabajo dentro de las propias instalaciones de la Universidad.

Habrá que considerar las siguientes acciones:

1. Prevenir la revelación de información del sistema: Los diálogos de acceso (al puesto local dentro de la propia instalación de la organización, al servidor, al dominio de red, etc.) no deben revelar información sobre el sistema al que se está accediendo. Por ejemplo, en el SSO de acceso a los servicios de la UPCT se puede poner el siguiente mensaje: *"El acceso a este sistema está restringido a personal autorizado, se le informa que su uso deberá ceñirse al autorizado en la política de seguridad y su acceso quedará registrado"*. En los errores de autenticación el mensaje correcto será *"Datos incorrectos"*.
2. Limitar el número de intentos de acceso fallidos, después de los cuales se bloqueará la cuenta del usuario. Hacerlo de la forma más "amigable" posible para el usuario.
3. Registrar los accesos, tanto los correctos como los fallidos.
4. Avisar al usuario de sus obligaciones inmediatamente después de obtener el acceso.
5. El sistema debe informar al usuario del último acceso con su identidad con éxito.
6. No pondremos limitación de horarios para acceso.
7. Definir e implementar (¿?) políticas para salvapantallas.

Ejemplo 2 de medidas en el plan de mejora

Universidad Politécnica de Cartagena

Mp.sw.1: Desarrollo de aplicaciones:

Se nos pide disponer de una política o normativa para el desarrollo de aplicaciones, que cubra los siguientes aspectos:

1. Desarrollar aplicaciones sobre un sistema diferente y separado del de producción.
2. Aplicar una metodología de desarrollo reconocida.
3. Los mecanismos siguientes deben ser parte integral del diseño del sistema:
   - de identificación y autenticación
   - de protección de la información
   - de pistas de auditoría (trazabilidad).
4. Pruebas anteriores a la implantación o modificación de los sistemas de información.

Esta normativa debemos acompañarla de herramientas de desarrollo concretas que permita a los desarrolladores el cumplimiento de las medidas expuestas.

En nuestro caso, hemos adoptado el **estándar ASVS (Estándar de verificación de seguridad en aplicaciones) definido por OWASP**, considerando sus niveles 1 (verificación automática) y 2 (verificación manual) como suficientes para nuestras aplicaciones. Estos dos niveles, suponen la adopción de un conjunto de buenas prácticas (definidas en una checklist) orientadas a:

- Escaneo dinámico de vulnerabilidades.
- Análisis estático del código fuente.
- Test de penetración en aplicación.
- Revisión de código para cumplimiento de requisitos de seguridad.

Conclusiones

- Ha sido un proceso muy útil y positivo. La implicación de todo el personal es muy importante; p.ej. los desarrolladores han incluido la seguridad como un aspecto a considerar desde la fase de diseño y en todo el ciclo de vida.
- A veces un poco tedioso pero creo que su duración y esfuerzo es asumible.
- Valoración muy positiva de la empresa consultora: conocimientos, dedicación y atención muy particularizada. Además, coste razonable.
- Saca a relucir carencias normativas y organizativas.
- Gestión de la seguridad: aplicación homogénea y razonada de las medidas y salvaguardas.
- Continuidad.