


Proceso de adaptación al ENS en la UPCT

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

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

- 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?

- 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. 

1. Curso de formación sobre ENS y Gestión de riesgos (Nov-2010). Para todo el Servicio de Informática.
 2. 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.

- **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

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

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

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

- **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.

- 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.

Descripción del proceso.

Paso 3: 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

1. Se informará al Consejo de Dirección sobre el informe realizado.
2. Se informará 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.
4. Se informará a todo el personal del Servicio de Informática.
5. Plan de mejora: establecimiento de medidas concretas (ver guía CCN-STIC 808).
6. Tareas de seguimiento.

- Ha sido un proceso muy útil y positivo.
- 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.
- Saca a relucir carencias normativas y organizativas.
- Gestión de la seguridad: aplicación homogénea y razonada de las medidas y salvaguardas.
- Continuidad.