Plan de mejora de la Seguridad TI en la UPCT (2015-16)

En el año 2011 la Universidad Politécnica de Cartagena emprendió las acciones necesarias para evaluar nuestros sistemas y planificar el proceso de adecuación al ENS de los mismos. Transcurridos 4 años, se ha realizado una auditoría sobre el estado actual de la seguridad habiéndose detectado determinadas carencias y puntos de mejora.

Tomando como punto de partida el informe del equipo auditor (las evidencias, opiniones y recomendaciones reflejadas en el informe), elaboramos el siguiente plan de actuación para la mejora de la gestión de la seguridad de las TI en nuestra Universidad.

INTERVALO DE EJECUCIÓN TEMPORAL:
Las acciones definidas en este plan se ejecutarán a partir del 1 de abril de 2015 y finalizarán el 31 de marzo de 2017, momento en el cual se realizará una auditoría para medir y analizar los resultados obtenidos.

OBJETIVOS:
Analizadas las conclusiones del informe de auditoría, las actuaciones definidas en este plan deben ir orientadas a mejorar en dos áreas fundamentales:

- La gestión interna del Sistema, que se refiere a aspectos sobre la organización interna del trabajo y la gestión de la Seguridad en la Unidad de Informática.
- El Gobierno corporativo de la Seguridad TI, desarrollando nuevas políticas para el tratamiento de la información y fomentando acciones corporativas de concienciación y formación en Seguridad TI.

Además, en este plan también se incluye un conjunto de actuaciones, que no están recogidas dentro de ninguno de los puntos anteriores, pero que nos permitirán mejorar el nivel de madurez de algunas medidas del ENS en las que así se requiera.

Por lo tanto, las actuaciones incluidas en este plan están orientadas al cumplimiento de los siguientes objetivos generales:

1. Gestión interna: **Configurar sistemas seguros, manteniéndolos en el tiempo, reportando y registrando los incidentes de seguridad** que se vayan produciendo sobre estos sistemas.
2. Gobierno corporativo de la Seguridad: **Definir y poner en marcha medidas organizativas y corporativas de concienciación y formación** (tanto de usuarios como de técnicos) y también de **calificación de la información.**
3. Otras acciones concretas para mejorar el nivel de madurez en medidas del marco de protección y de operación.

PLAN DE ACTUACIÓN:
Las acciones se van a estructurar en tres bloques, correspondiendo cada uno de ellos con los objetivos generales definidos en el punto anterior. Dentro de cada bloque, el orden en el que se presentan las medidas es significativo sobre su prioridad.

1. **Gestión interna de la Seguridad:**
    1. La Unidad de Informática deberá revisar y mejorar su **procedimiento de Gestión del cambio** (basado en ITIL) de tal forma que permita gestionar conjuntamente los aspectos que cubre hasta ahora, y que incluya al menos los siguientes aspectos:
        - Información de capacidad para dimensionamiento sistemático de los cambios que se quieran implementar.
        - Garantizar la actualización del actual Inventario de Activos (CMDB).
        - Definir un ciclo de cambio-entrega que garantice la ejecución de pruebas, previas a la puesta en explotación.
        - Gestionar actualizaciones de seguridad de los activos (al menos de los más críticos o de las actualizaciones más importantes) mediante este proceso.
        - Revisión del proceso y mejora según la experiencia hasta el momento.
    2. La Unidad de Informática deberá implantar un proceso y herramienta para la **gestión de incidentes de seguridad**, basado en la herramienta LUCIA, adaptada para el ENS por el CCN-CERT.
    3. Los responsables del Sistema deberán definir nuevos procedimientos de seguridad que complementen a los ya existentes y complementando la gestión de cambios: actualización y tratamiento de vulnerabilidades, fortificación de sistemas y servicios, monitorización de la seguridad, requisitos de seguridad en la adquisición de los elementos del sistema
    4. Los responsables del Sistema deberán mejorar la **protección de aplicativos web**, implementando de forma sistematizada varias capas de seguridad: filtrado en cabecera de red (cortafuegos) y técnicas de filtrado a nivel de aplicación y/o servidor.
    5. El responsable de seguridad deberá redactar un Documento de **Arquitectura de seguridad**, según lo especificado en el ENS.
    6. Los responsables del Sistema deberán definir un procedimiento para la **gestión de claves privadas** de servidores y sello de órgano (solicitudes CSR y gestión de certificados: generación, custodia en explotación, etc).
    7. El responsable de seguridad deberá Documentar la arquitectura de la gestión de identidades.

2. **Gobierno corporativo de la Seguridad:**
    1. El Equipo de Gobierno, los Responsables del Sistema y el Responsable de Seguridad deberán revisar y actualizar la Política y

Normativa de Seguridad de la UPCT y darle máxima difusión dentro de la Universidad.

2. El Equipo de Gobierno deberá aprobar una **Política de calificación de la información** y lo que se puede o no se puede hacer con ella, partiendo de la base de lo que ya hay establecido para el ENS y el cumplimiento de la LOPD. La política debe cubrir aspectos tales como:
    - Calificación de la información, según su grado de confidencialidad.
    - Condiciones en el tratamiento de cada tipo de información, según su calificación.
    - Requisitos para la transmisión de la información.
    - Restricciones sobre la difusión y almacenamiento.
3. El Equipo de Gobierno deberá aprobar una **Política de Firma y sellado de tiempo** que explicite los motivos por los que la información debe, o no, ser firmada digitalmente y los mecanismos usados para ello en cada caso.
4. El responsable del Sistema correspondiente, a instancias del Equipo de Gobierno, deberá implementar mecanismos de **control de calidad de las contraseñas** que garanticen, al menos, una longitud y complejidad mínimas y un tiempo de vida limitado.
5. El equipo de Gobierno, con el apoyo de los Responsables del Sistema y del Responsable de Seguridad, deberá aprobar y ejecutar un **plan de concienciación en Seguridad TI** para todo el personal de la organización; este plan incluirá la organización de pequeños talleres y jornadas a lo largo del año, centradas en actividades eminentemente prácticas, así como el envío periódico de píldoras informativas.
6. Tal y como establece el RD 3/2010 de 8 de enero de 2010, el Equipo de Gobierno deberá aprobar un **Plan de formación** que explícitamente cubra los requisitos en materia de seguridad de la información deseables para el personal de la Unidad de Informática; además deberá dotarlo con los recursos necesarios, ya sea incorporándolo al plan de formación del PAS de la UPCT o reservando una partida económica en el presupuesto anual.
7. Los responsables del Sistema y el Responsable de Seguridad, con la aprobación del Equipo de Gobierno, deberán definir e implementar la homogenización de medidas de **protección en los equipos de usuario** y en los equipos portátiles, definiendo, según el tipo de equipo, puesto de trabajo e información tratada aspectos de la configuración de seguridad tales como: antivirus, política de actualización de escritorio, cortafuegos personal, bloqueo, encriptación, etc.

3. **Acciones para madurez de medidas concretas:**
   Todas estas acciones serán llevadas a cabo por los Responsables del Sistema dentro de su ámbito de actuación.

   1. Acceso remoto.
   2. Mejorar el **acondicionamiento del CPD**.
   3. Correo electrónico.
   4. Pruebas del sistema de Copias de seguridad.
   5. Protección frente a **ataques de denegación de servicios** (DDoS).
   6. **Destrucción de soportes**.
   7. Gestión de **continuidad TI**.

Finalmente, para determinar el grado de ejecución de este plan y el impacto producido sobre el grado de cumplimiento del ENS, a la finalización del mismo (abril de 2017) se realizará una nueva auditoría de Seguridad TI en la UPCT.

APROBACIÓN:
Este plan ha sido aprobado por el Comité de Seguridad TIC, dentro de la Comisión de Nuevas Tecnologías.