Plan de Adecuación al Esquema Nacional de Seguridad

Aprobado por Comisión de Seguridad de la UAL el 15/03/2013

La Universidad de Almería ha emprendido las acciones necesarias para evaluar sus sistemas de información y definir el proceso de adecuación al Esquema Nacional de Seguridad (RD 3/2010) de los mismos. En concreto, se han realizado las siguientes tareas:

- Identificación y catalogación de información, sistemas y servicios prestados, así como su relación con el RD 15/99, de la Ley Orgánica de Protección de Datos. Identificación de subsistemas y de medidas de seguridad aplicables
- Análisis de Riesgos acorde a la metodología Magerit V2.
- Identificación de insuficiencias existentes respecto a los requerimientos de seguridad marcados por el ENS y los existentes en la organización.

El punto 2 de la Disposición transitoria del ENS (RD 3/2010) establece la necesidad de definir un plan de actuación para que las AAPP se adecúen al ENS.

Basándonos en los resultados obtenidos en el proceso antes citado, hemos definido nuestro plan de actuación. La Universidad de Almería, debido a las limitaciones presupuestarias existentes en la actualidad, así como a las limitaciones en recursos humanos, debe afrontar este proceso de adecuación de forma gradual y estableciendo una planificación inicial generalista, que en sucesivas fases deberá ser gradualmente definida y concretada, según la capacidad económica y humana existente. Para la elaboración del Plan de Adecuación hemos localizado lo que hemos llamado insuficiencias severas y moderadas:

- **Insuficiencias severas**: aquellas medidas de seguridad establecidas en el ENS en las que hemos detectado que el cumplimiento de las condiciones para cubrir las mismas es actualmente inferior al 15%.
- **Insuficiencias moderadas**: aquellas medidas de seguridad establecidas en el ENS en las que hemos detectado que el cumplimiento de las condiciones para cubrir las mismas es actualmente inferior al 30%.

Toda la información detallada obtenida en este proceso, así como las insuficiencias detectadas y las medidas concretas para resolverlas, están en la documentación interna de la UAL y estará a disposición de los auditores que la requieran.

Teniendo en cuenta estas consideraciones previas, el plan de mejora propuesto es el siguiente:

FASE 1: OBJETIVOS A CORTO PLAZO – OCTUBRE 2013

Se establecen como objetivos a corto plazo, con ejecución anterior a JUNIO de 2013, los siguientes:

- **Corrección de las insuficiencias severas**: El objetivo más inmediato a corto plazo es la eliminación de insuficiencias severas del sistema de información, permitiendo que todas las medidas a adoptar alcancen al menos un nivel de madurez por encima del 15% (L1).

- **Mejora general del marco organizativo:** Debido a la descompensación existente entre el margo organizativo y los marcos operacional y técnico, la mejora del marco organizativo y la creación de un proceso de gestión de seguridad de la información serán tarea fundamental inicial.

- **Garantía de cumplimiento de medidas actuales:** Antes de iniciar la creación de nuevas medidas técnicas u operativas, se debería garantizar el cumplimiento de las actuales para todo el conjunto de tareas y procedimientos del STIC.

- **Planificación de medidas derivadas del análisis de riesgos:** El último de los objetivos a satisfacer en el corto plazo es la planificación de las medidas que se adoptarán a medio plazo en aquellas áreas de actuación en las que el Análisis de Riesgos ha determinado un mayor aprovechamiento de los recursos invertidos en su relación a las necesidades de la organización y a la reducción del riesgo.

FASE 2: OBJETIVOS A MEDIO PLAZO Y LARGO PLAZO

Se establecen como objetivos a medio y largo plazo, con ejecución esperada anterior a Octubre de 2015 los siguientes:

- **Corrección de las insuficiencias moderadas**: El objetivo inicial a medio plazo es la eliminación de insuficiencias moderadas del sistema de información, permitiendo que todas las medidas a adoptar alcancen al menos un nivel de madurez por encima del 30%.

- **Desarrollo de medidas**: Desarrollar medidas operativas y técnicas acorde a lo planificado en el proceso de análisis de riesgos.

- **Atención a medidas de seguridad de difícil implantación y maduración:** Según las recomendaciones del análisis de riesgos se recomienda centrar el esfuerzo a largo plazo en potenciar aquellas medidas de difícil implantación.

Actuaciones en el primer año

Durante el primer año, y según los objetivos marcados, las medidas sobre las que se ejecutarán actuaciones operativas, encaminadas a la reducción del riesgo y a la implementación de controles son las siguientes:

	Actuación operativa
org.3	Procedimientos de seguridad
op.pl.2	Arquitectura de seguridad
op.pl.3	Adquisición de nuevos componentes
op.pl.4	Dimensionamiento / Gestión de capacidades
op.acc.6	Acceso local (local logon)
mp.per.4	Formación
mp.eq.2	Bloqueo del puesto de trabajo
mp.info.2	Calificación de la información

mp.s.2	Protección de servicios y aplicaciones web
mp.s.8	Protección frente a la denegación de servicio

Estas actuaciones permiten el cumplimiento de los dos objetivos inicialmente marcados, por un lado la corrección de las insuficiencias severas y por otro la mejora del marco organizativo y del proceso de gestión de la seguridad.

Como complemento a estas actuaciones operativas, se iniciarán actuaciones de planificación sobre cómo dotar de madurez a aquellas medidas que el análisis de riesgos ha calificado como de difícil implantación a largo plazo.

Planificación

op.ext.2	Gestión diaria
op.acc	Controles de acceso
op.ext	Servicios externos
mp.si	Medidas de protección de los soportes de información
mp.info	Medidas de limpieza de información y calificación de la información

Actuaciones en años sucesivos

Las actuaciones en años sucesivos, una vez eliminadas las insuficiencias y garantizado el cumplimiento actual, irán destinadas a dos aspectos fundamentales:

- Madurar las medidas según el desarrollo realizado en el análisis de riesgos.
- Atender a las medidas de difícil implantación.

Las actuaciones concretas serán planificadas antes de ser acometidas.