



UNIVERSIDADES: ALINEANDO LOS ENFOQUES DE SEGURIDAD CON LOS NUEVOS ESCENARIOS

En las universidades se han producido cambios relevantes de entorno. Así pues, tras ver éstos, analizaremos la especial conveniencia de una revisión de la estrategia de seguridad. Las universidades tienen la docencia y la investigación como actividades nucleares, y como cualquier otra organización, la propia actividad de gestión.

El Espacio Europeo de Educación Superior, asociado por todos a Bolonia, está siendo un gran factor de cambio para la actividad docente. Recordemos algunos de los conceptos de mayor relevancia: validez de los títulos en el espacio europeo, movilidad de estudiantes entre

De todo lo visto se desprende que ámbitos clásicos de la seguridad tienen que estudiarse a fondo, contraponiendo a las oportunidades de los nuevos proyectos y tecnologías los riesgos potenciales que implican, desde una perspectiva holística. Un buen punto de vista lo puede aportar un análisis de riesgos con especial énfasis en la visión de "negocio" y con la participación de todas las partes implicadas. Analizaremos los ámbitos de mayor afectación.

En el control de acceso a la red debe contemplarse el amplio espectro de ordenadores que solicitarán conexión. Los ordenadores de sobremesa de las aulas informáticas se han

Es cierto que las universidades están abordando con cautela las soluciones de *cloud computing* para procesos de gestión, pero por el contrario sí están incorporándolas con más ímpetu en el ámbito docente. Cabe analizar dos temas importantes al respecto. Gran parte de los contenidos de conocimiento que anteriormente estaban en servidores internos y en formatos más clásicos, cada vez más se ubican en servicios en "la nube" y en formatos más interactivos y voluminosos. Esto implica un mayor requerimiento de amplitud y disponibilidad de la red, y un menor control sobre el acceso a los contenidos.

La concienciación es el eterno punto de mejora, y además urgente. El personal con una relación más estable está cada vez más concienciado, pero también es verdad que los requerimientos legales son más fuertes. Los estudiantes ya se incorporan con unas habilidades tecnológicas previas importantes, pero en muchos casos sin una suficiente concienciación en materia de seguridad. Aquí sí que la universidad tiene la obligación de formar a estos estudiantes en un uso responsable de las TIC.

La concienciación es el eterno punto de mejora, y además urgente. El personal con una relación más estable está cada vez más concienciado, pero también es verdad que los requerimientos legales son más fuertes. Los estudiantes ya se incorporan con unas habilidades tecnológicas previas importantes, pero en muchos casos sin una suficiente concienciación en materia de seguridad. Aquí sí que la universidad tiene la obligación de formar a estos estudiantes en un uso responsable de las TIC.

universidades, incremento de las prácticas en empresas, y potenciación de las competencias en idiomas, TIC y trabajo en grupo y en red (herramientas colaborativas, *blogs*, *wikis* y 2.0 en general). Es interesante hacer tres reflexiones sobre el perfil de los estudiantes. Por un lado, los jóvenes que se incorporan a la universidad, mayoritariamente son ya "nativos digitales". La formación continuada está cobrando más peso dentro de la formación ofertada, con un perfil de alumno más variado. Y, finalmente, la formación virtual está cada vez más presente en todas las universidades, ya sea complementando la presencial, o en algún caso sólo ofertando *e-learning*.

En el apartado de la investigación, y atendiendo a la situación económica actual, la investigación y la innovación se apuntan como elementos clave para la mejora de la productividad. Y esto pasa por una más estrecha colaboración con la empresa, la potenciación de institutos mixtos, la captación de talento investigador, la transferencia de tecnología, etc. Claramente el conocimiento generado será un activo muy importante.

Dentro del ámbito de la gestión hay que contemplar la coyuntura económica general, y el continuo crecimiento de la externalización de servicios y desarrollo de proyectos. El Esquema Nacional de Seguridad se ha añadido a los requerimientos de cumplimiento anteriores. Y, finalmente, se debe tener muy presente que la organización de las universidades está formada por una interrelación de facultades, departamentos, institutos y grupos de investigación, y áreas funcionales; resultando un sistema de gobierno propio.

visto desplazados por los portátiles con conexión inalámbrica, como puesto de trabajo mayoritario de los alumnos. Con la movilidad interuniversitaria, no sólo de estudiantes, sino también de profesorado e investigadores, y la presencia de otras personas de empresas externas se ha disparado el número de ordenadores "foráneos" conectados. Éstos, en su origen, no están sujetos a las políticas de acceso de la universidad. Si bien facilitar el trabajo en red de estas personas es primordial, también lo es minimizar el riesgo que implica. Va en aumento la necesidad de garantizar el acceso remoto seguro a las personas de la organización que deben acceder desde fuera del *campus* universitario.

La gestión de identidades cobra protagonismo especial. Aparte de los colectivos mencionados en parte en el anterior párrafo, el número de servicios con base tecnológica se ha multiplicado. Y en este sentido cada persona debe poder acceder a los servicios de acuerdo con sus roles, pero no a los que no debe. La autorización es clave, y como es de suponer en tan amplio y heterogéneo colectivo, también lo es la trazabilidad de las acciones individuales. Si bien las contraseñas son aún el método de autenticación más frecuente, la firma digital va implantándose en áreas concretas, y ha habido algunas experiencias biométricas.

La continuidad de negocio debe ser revisada en muchos casos, debido a que gran parte de los servicios 24x7 no contemplaron suficientemente estos requerimientos en su nacimiento: docencia virtual, biblioteca electrónica, correo-e, repositorios de documentos, equipos específicos de investigación, etc.

Los Esquemas Nacionales de Seguridad e Interoperabilidad suponen un reto importante, dada la complejidad de las organizaciones, los plazos ajustados para su despliegue y el panorama presupuestario venidero. Desde una perspectiva positiva de los responsables de la seguridad de la información, pueden ser un catalizador para priorizar proyectos de seguridad que se habían aplazado. Éste es un ejemplo en el que compartir experiencias y planteamientos entre universidades resultará beneficioso.

Por suerte, frente a todos estos múltiples retos, estamos asistidos de marcos de trabajo, estándares, y buenas prácticas suficientemente maduras y aplicables a cualquier organización. Ya son muchos los proyectos acometidos en los ámbitos de gestión de la seguridad de la información, gestión de riesgos y gestión de servicios. En paralelo, los sistemas de indicadores han ido avanzando tras varios ciclos de mejora continua. En todo esto la transversalidad de la función de seguridad de la información nos ha implicado más que a otras áreas más verticales de TI.

Y ya para finalizar, cabe destacar la creciente preocupación por formalizar y consolidar el gobierno de TI, con una clara implicación de la alta dirección, los responsables de los procesos y la propia TI, facilitándose así el alineamiento de la función de seguridad de la información. ■



Xavier Rubiralta Costa
Responsable de Proyectos de Seguridad de la Información

UNIVERSIDAD AUTÓNOMA DE BARCELONA