Seguridad de la información: una tarea de toda la comunidad UACh

*** Durante este año la Dirección de Tecnologías de Información realizará diversas acciones que permitan a funcionarios y académicos apropiarse de este concepto de gran importancia estratégica y corporativa.**

Escrito por: Jose Luis Gómez Guenchor - Periodista Relaciones Públicas UACh Email: josegomez@uach.cl
Fotografía: Imagen gentileza de http://www.valiantsolutions.com/
15-07-2014

* En ese marco desde hace un par de meses se encuentra funcionando un Comité de Seguridad de la Información al mismo tiempo que se contrató a un profesional a cargo de este tema.

"Seguridad de la información: tarea de todos". Ese es el llamado que está haciendo la Dirección de Tecnologías de Información de la Universidad Austral de Chile, la que actualmente se encuentra liderando un ambicioso proyecto que busca que académicos y funcionarios UACh se apropien de este tema sensible y de gran relevancia estratégica y corporativa.

Según informó la Directora de Tecnologías de Información UACh Nadja Starocelsky, "en el actual Plan Estratégico viene establecido un proyecto de seguridad de la información corporativa. En base a esto se generó el cargo de Responsable de la Seguridad de la Información DTI, cuyo responsable es el ingeniero informático Daniel San Martín".

Comentó además que desde hace meses que se encuentra funcionando un Comité de Seguridad de la Información donde participan representantes de la Vicerrectoría de Gestión Económica y Administrativa, Vicerrectoría Académica, de las Facultades (Decano), de la Sede Puerto Montt y Campus Patagonia en Coyhaique, además del Director de Personal, la Directora de la DTI y desde ahora el Responsable de la Seguridad de la Información.

"Ese comité tiene la labor de entregarle propuestas a Rectoría sobre seguridad. Hemos estado trabajando en los últimos meses más que nada en detectar en qué aspectos vamos a ir avanzando este año. Durante los próximos meses les llegará a la comunidad información sobre los pasos que vamos a ir dando", aseguró.

Por su parte, Daniel San Martín puso el énfasis en que lo que se quiere hacer es sensibilizar a la comunidad en temas de seguridad de la información. "Estamos hablando concretamente sobre los datos que maneja la organización como por ejemplo correos electrónicos, datos sensibles que tienen que ver con la parte financiera, área personal y en general toda información de valor para la organización. Todos estos son activos de información en donde la DTI tiene un rol administrador, custodiando la información por medio de sus servidores y aplicaciones con el propósito de dar un servicio de calidad en términos de confidencialidad, integridad y disponibilidad", explicó.

Generar buenas prácticas

La Directora de la DTI destacó que en el mundo actual las corporaciones e instituciones tienen que salvaguardar la información ya que es el activo más fuerte que poseen. "Desde hace unos diez o quince años que las organizaciones han empezado a poner mucha fuerza en 'segurizar' su información. No solamente 'segurizarla' desde el punto de vista informático si no que generar las buenas prácticas en las personas que trabajan con esta información para que siga siendo confidencial".

Por lo tanto la idea es instaurar este tema a nivel transversal y sobre todo esperan que los académicos y administrativos se sensibilicen en aspectos como la información que se entrega desde el correo electrónico corporativo. Otro caso es el de los comunicados que dicen ser institucionales pero que no tienen un correo emisor que sea institucional y que buscan capturar contraseñas. "Además si ve un enlace en un correo en el cual no confía, no lo abra, y si tiene alguna duda llame a la Mesa de Ayuda de la Dirección de Tecnologías para que lo apoyen", indica.

En esa línea la Directora propone a la comunidad que se haga algunas preguntas: ¿cuándo sale de su oficina cierra las sesiones que están activas en su computador? o ¿sus computadores tienen claves de acceso para evitar que personas no autorizadas accedan a su información? Y en el caso de las personas que gestionan sus correos electrónicos institucionales o personales en sus dispositivos móviles como teléfonos o tablet: ¿estos dispositivos cuentan con una contraseña de acceso para evitar que ingrese un extraño en caso de robo?

Finalmente todos estos resguardos se toman porque si la información corporativa llega a personas no deseadas esto podría generar problemas graves a la institución, advierten desde la Dirección de Tecnologías de la Información UACh.