

# SEGURIDAD INFORMÁTICA

**EDUTIC** Chile

REVIEW N°2 Octubre 2011



**TECNOLOGÍA E INNOVACIÓN**  
DESAFÍOS PARA EL DESARROLLO  
DE LA EDUCACIÓN SUPERIOR

**Comité Editorial Edutic**

Cristian Ocaña  
Hernán Silva  
Francisco Valdivia

**Colaboradores**

Jorge Romero A.  
Alejandro Arias

**Producción**

Uno a Uno Marketing



 [contacto@eduticchile.cl](mailto:contacto@eduticchile.cl)  
[www.eduticchile.cl](http://www.eduticchile.cl)

# ¿Está Segura su Seguridad? ¿Seguro?

En el estudio 2010 EDUTIC, sobre "Situación de las TICs en las Instituciones de Educación Superior en Chile", la Seguridad apareció como uno de los temas que le importaba a las Instituciones de Educación Superior (IES) chilenas. El informe reveló que el 44% de las IES aún no había realizado una evaluación formal del riesgo de la seguridad TIC.

La Seguridad Informática muchas veces es vista por quien no la entiende, como un tema de los técnicos, de los "computines", de fanáticos que pasan pegados en un computador. Sin embargo, sabemos que es el pilar fundamental en la provisión de servicios digitales en el siglo 21. La banca no podría ofrecer transferencias electrónicas online desde un Smartphone si no hubiese asegurado a sus clientes la confianza y credibilidad respectivas. Lo mismo con servicios como Webpay, Previred o el mismo SII con su sistema de declaración de impuestos y facturas electrónicas ¿Cuánto confiamos en ellos!

Incluso los mismísimos Gmail, Facebook o Twitter ¿Qué habría sido de ellos si la seguridad no hubiese regido el espíritu de esos emprendimientos? Con cuánta facilidad navegamos por la red entregando nuestros datos personales en sitios que están "no sé dónde en la nube", como Amazon, Paypal, eBay, LAN.com ¿qué activos tienen ellos, en particular? Confianza, credibilidad, seriedad, respeto y responsabilidad con sus clientes.

¿Qué quiere decir todo esto? Muy simple: la seguridad representa una base relevante en los servicios del mundo digital y, por tanto, requiere ser entendida y aceptada como parte de la misma organización. Ello significa que entra de lleno al compromiso institucional con el buen servicio, con la atención a los clientes, al velar y resguardar el propio negocio ¿Están las TI sentadas en el directorio de su organización?

Por otro lado, la Seguridad también debiese abarcar si-

tuaciones excepcionales como algún desastre o fuerza mayor como un terremoto, una inundación o un ataque malintencionado. Contar con los planes de contingencia ante estas potenciales amenazas (DRP o Planificación de Recuperación ante Desastres) pone a la institución en una ventaja competi-

tiva interesante para garantizar los servicios que se entregan. Pregunta como si ¿Ud. tiene planes DRP? o si ¿Sabe de qué se tratan? o ¿Qué haría frente a un desastre? o ¿Qué hizo para el último terremoto? ¿Qué perdió? ¿Cuántos ataques tiene al día? ¿Sabe si éstos son internos o externos?

Bueno, a lo mejor ud. sabe, pero ¿lo saben sus jefaturas superiores? ¿Están al tanto de la situación de riesgo que tienen en su propia organización? Porque si lo supiesen, debiese tener la conciencia

suficiente para asignar los recursos apropiados para cubrirse y proteger los servicios institucionales. Basta con recordar los ataques conocidos del grupo ciberactivista Anonymous a los sitios de Sony Playstation, BBVA, Bankia, webs gubernamentales de Argelia, Chile, Colombia, Irán, Libia, Nueva Zelanda ¿Recuerdan el ataque al web del MINEDUC en Julio pasado?

En síntesis, La Seguridad es un proceso evolutivo y también es parte del compromiso institucional. El mundo avanza de manera vertiginosa y quedarse atrás es muy simple. El tema es si se está lo suficientemente atento para que ello no ocurra ¿Las autoridades institucionales están conscientes que las diferentes temáticas tecnológicas nunca acaban, que si llegaron fueron para quedarse? La TI en la Mesa del Directorio es la mejor muestra de haber adquirido este nivel de conciencia.

**La seguridad  
representa una  
base relevante en  
los servicios del  
mundo digital y, por  
tanto, requiere ser  
entendida y aceptada  
como parte de la  
misma organización**



Cristian Ocaña  
cristian.ocana@eduticchile.cl  
Director Ejecutivo de EDUTIC

# Desafíos para el segmento educación

Desde hace veinte años se han desarrollado estudios que tomando la experiencia del uso tecnológico en el quehacer organizacional, han permitido enfrentar de forma sistematizada los riesgos relacionados con el concepto de la SEGURIDAD. La publicación de la British Standard BS 7799-1, publicada en 1995, ya en su primera versión, plantea el claro objetivo de establecer ciertos protocolos que permitan certificar la protección de transacciones, especialmente en el mundo de las mesas de dinero y transacciones electrónicas. Estas normativas iniciales, antecesoras de la actual ISO 27000, surgieron con el claro propósito de establecer una línea base en referencia al estado del arte vigente en la industria dedicada a la seguridad.

Cuando se habla de seguridad, existe la tendencia general a encasillar los riesgos de falta de seguridad dentro de un contexto de ataques informáticos, robo de bases de datos, hackeos de sitios, violación de equipos como firewall o denegación de servicios. Sin embargo, el estándar ISO 27000, centra su foco en una cobertura integral del cuidado de los bienes de una compañía adoptando una mirada estructurada que brinda cobertura global, sobre bienes, activos fijos, transacciones, documentación, información estratégica del negocio, la continuidad operacional entre otros. Es decir, analiza la seguridad de la información en todas las áreas claves del negocio.

La normativa ISO modela el control de la seguridad en

## La Seguridad de la Información es mucho más que preocuparse de firewalls, redes o ataques de hackers

11 dimensiones, para segregar los elementos que componen el análisis de la seguridad de una manera estructurada, estableciendo indicadores que sirven para medir la gestión interna de los servicios que funcionan sobre una estructura de TI. Elevar los niveles de seguridad es la acción de mejora continua (Teoría de Deming - ciclo PDCA), que logra optimizar todos los procesos críticos de negocio.

Por otro lado, se observa que las dimensiones de la ISO atraviesan transversalmente a todas las áreas de una compañía, por lo tanto, el concepto de la Seguridad de la Información es un proceso que depende fuertemente de

la alta dirección y la cultura organizacional.

A medida que aumenta la complejidad y cantidad de procesos críticos de una organización, es evidente que se complejiza el control y la administración interna. La norma ISO define una herramienta conceptual para el control y organización de la seguridad de la información: el Sistema General de la Seguridad de la información (SGSI), que corresponde a aquella parte del Sistema de Gestión Global orientada a implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. Para la implementación de un SGSI es necesario establecer: el alcance; criterios de riesgo; identificar y valorizar los activos de información; nivel de riesgo real; política general de seguridad; aplicabilidad; normas y procedimientos; implantación y puesta en marcha y por último documentar, auditar y revisión del SGSI.

En la administración del SGSI se requiere un Oficial de Seguridad quien, por regla general, reporta directamente a alguna gerencia de primera línea, idealmente relacionada con el más alto nivel de toma de decisiones operativas. El Oficial de Seguridad, tiene entre sus responsabilidades impulsar y coordinar el Comité de Seguridad de la información (CSI), compuesto generalmente por representantes de cada una de las gerencias o direcciones operativas de una organización.

Reafirmamos que la Seguridad de la Información es mucho más que preocuparse de firewalls, redes o ataques de hackers, sino que es un tema que debe ser relevado al control directo de la Alta Gerencia. Cuando las organizaciones le dan este nivel de importancia, pueden aprovechar toda la normativa existente para diseñar y crear una estructura interna capaz de proteger adecuadamente sus intereses. Dado que la mejora de la seguridad es un proceso continuo que involucra a toda la organización, es fundamental que la Alta Gerencia lo considere como una de sus responsabilidades fundamentales.



Jorge Romero A.  
Jefe de Redes y Seguridad  
Universidad San Sebastián

# Infraestructura de la seguridad

¿Se puede comprar la seguridad informática? La respuesta es, lamentablemente, no del todo. El concepto que llamamos seguridad informática, debe ser entendido, administrado, incorporado en todos nuestros procesos y deber ir más allá de los equipos, mas allá de las políticas y procedimientos. Debe estar inserto en nuestras mentes, en nuestra vida diaria, como parte de nuestra forma de actuar. Todo esto sin caer en la paranoia, porque las soluciones existen, los expertos existen; y una buena combinación de estos nos permiten mitigar el impacto de la realidad imperfecta del escenario tecnológico del mundo actual.

Atrás quedaron los días en que solo un firewall nos bastaba para estar protegidos. En la actualidad es necesario contar con un arsenal mucho más extenso. Encontramos así numerosas marcas y productos como sistemas heurísticos de detección de ataques, de virus y spam. Además, un sin fin de herramientas y técnicas de diagnóstico que combinados adecuadamente definirán nuestro nivel de seguridad o riesgo.

Pero la tarea no termina aquí. Cuando hablamos de seguridad hay que entender que nuestra información y sistemas siempre deben estar disponibles y tienen que contar con los niveles de integridad y confidencialidad suficiente a nuestra necesidad. Es en este punto donde necesitamos ayuda más especializada y conocimiento experto respecto de cómo hacer las cosas, de las buenas prácticas y de cómo incorporar la seguridad en nuestras organizaciones.

En el terreno formal, encontramos numerosas instituciones con experiencia en seguridad informática. Muchas de ellas han adoptado la serie de normas inter-

nacionales ISO 27000, entre otras, y desarrollado metodologías aplicables a nuestra realidad. Si buscamos ayuda en esta dirección lo primero que debemos hacer es conocer nuestra brecha respecto del estándar. Este parámetro nos permitirá apreciar qué tan vulnerable somos y cuánto será nuestro esfuerzo para llegar a los niveles deseados. A poco andar nos encontraremos con conceptos nuevos (o no tan nuevos) según nuestra experiencia: "Política General de Seguridad"; "Política de Respaldo"; "Política de control de cambios"; "Plan de continuidad de negocio",

entre muchos otros. Estos conceptos son fundamentales y requerimos entenderlos, desarrollarlos, e incorporarlos a nuestros procesos.

El mundo ya cambió. Si continuamos ignorando las señales no sabremos lo que debemos hacer. Inventaremos la rueda cada vez que ocurra un incidente, o reaccionaremos demasiado tarde a un costo muchas veces muy alto. Sin un plan de seguridad definido, será muy difícil crecer o asimilar nuevos conceptos, será muy difícil incorporar nuevos productos o externalizar servicios, serán muy costosos nuestros planes de alta disponibilidad. Y será mucho más difícil proyectarnos hacia el futuro.

## Atrás quedaron los días en que solo un firewall nos bastaba para estar protegidos



Alejandro Arias  
Director de Tecnologías  
de Información  
Universidad Diego Portales