Economía&Negocios

INACER	
Enero-marzo 2018	+6,4%
IPC	
Abril	0,3%
Anual	1,9%
TPM	
Desde 18/05/2017	2,50%

UNIDAD DE FOMENTO
$27.099,26

UTM MAYO
$47.538,00

BOLSAS DE VALORES					
Ipsa	5.467,87	-0,54%	Igpa	27.667,69	-0,47%
MONEDAS EXTRANJERA					
Dólar Observado	$630,63		Euro		$744,99
COMMODITIES					
Celulosa (US$/T)	$1.170,00		Cobre (US$c/libra)		$328,65
H. de Pescado (US$/T)	$1.525,00		Petróleo (US$)		$ 65,95

DESPUÉS QUE LOS BANCOS DE CHILE, ITAU Y SANTANDER SE VIERAN AFECTADOS EN SUS RESPECTIVOS SISTEMAS

Informáticos entregan las **claves para mejorar la seguridad** en las empresas

Una eventual política de Estado debiera considerar segmentar los servicios privados de los públicos y sus respectivos protocolos. Las áreas a proteger deben ser Software, Hardware y datos.

Edgardo Mora Cerda
edgardo.mora@diarioconcepcion.cl

Tras los problemas informáticos sufridos por los bancos de Chile, Itau y Santander que incluso dieron paso a una comisión investigadora en la Cámara Alta requerida por el Senador Felipe Harboe, informáticos regionales entregan las claves para mejorar la seguridad en las empresas.

También, dieron a conocer cuáles debieran ser los ejes principales de una eventual política de Estado en relación a la seguridad informática nacional.

Cabe recordar que hasta el momento de los 54 reclamos de clientes del Banco de Chile, 32 estarían solucionados, 10 en proceso y 14 pendientes según la información entregada por la Superintendencia de Bancos e Instituciones Financieras, Sbif.

54
Fueron en total hasta el momento los reclamos por parte de los clientes afectados por el virus en el banco de Chile.

40
Años y más tiene de trabajo en la región del Bío Bío la empresa Crecic especializada en el rubro informático.

Principales ejes de una política de Estado

José Arellano, gerente comercial de soluciones de Crecic, empresa con más de 40 años de trabajo en la Región del Bío Bío, estima necesario "segmentar todos los servicios prestados por el sector privado y los que afecten a la población, para ser fiscalizados por algún ente externo, más o menos como la propuesta del gobierno anterior con el Ministerio de Ciencias y Tecnología el cual aún se encuentra en discusión".

Orellana plantea también que "la fiscalización en temas de seguridad informática se debe presentar por la protección de la información de las personas, quienes son los principales afectados de los ciberataques" y puso como ejemplo que "en Salud podríamos consultar sobre los datos almacenados por Autentia (La base biométrica para la venta de bonos electrónicos y licencias médicas) y cómo validan que esa información no sea usada para otros fines".

Por su parte, César Arévalo, docente de Ingeniería en Conectividad y Redes de Duoc UC sede Concepción reconoce que "en general en Chile, a nivel técnico, no existen mayores problemas en cuanto al nivel de seguridad de las instituciones financieras, pero la seguridad es una competencia constante" y afirma que una eventual política de Estado debiera considerar aspectos tales como "establecer claramente los mecanismos de acción ante la ocurrencia de eventos. La idea es que cada integrante de la organización tenga claro su papel al momento de concretarse un evento. Educación informática: una gran cantidad de ataques se concretan debido al desconocimiento de los integrantes de la organización en cuanto a los métodos de ingeniería social usados por los atacantes. Cumplir con la triada de seguridad: Confidencialidad (Proteger la información), Integridad (Ser capaces de identificar cualquier alteración de la información) y Disponibilidad (Mejorar los mecanismos de acceso a la información)".

Claves para la seguridad

En cuanto a qué deben tener en cuentas las empresas para resguardar su seguridad informática, el gerente comercial de soluciones de Crecic, afirma que "el término Seguridad Informática abarca varias áreas, los 3 principales son software, hardware y datos, para lograr proteger esto, nos debemos ocupar de las amenazas, las cuales pueden ser categorizadas en 3 grupos: Personas: Personal interno y hackers; lógicas: Bugs de software, Virus, Gusanos, accesos externos (Redes), y otros; físicas: Robo, suministro eléctrico".

En tanto, el docente de Ingeniería en Conectividad y Redes de Duoc UC sede Concepción, detalla "los pasos a seguir (por las Pymes) deberían ser: Cuantificar el valor de su información; auditar constantemente sus sistemas internos, generando una política de verificación en sus sistemas informáticos; educar a los integrantes de la Pyme, a fin de evitar lo máximo posible los ataques debidos a mal uso de software, exceso de confianza en cuanto a aplicaciones y lo más importante, tomar la decisión de invertir en seguridad informática. Es mucho mejor tenerla y no necesitarla... que necesitarla y no tenerla...".

Costos Asociados

Respecto de los costos asociados a la seguridad informática, desde Crecic, su gerente comercial de soluciones indica que "en redes a modo de ejemplo nos ajustamos a un equipo Cortafuego, más conocido como Firewall, puede partir desde los US$2.000.- como equipamiento, y en Servicios puede iniciar en 8 a 12 UF mensuales, dependiendo enormemente del tamaño de la organización. Estos valores de Servicios son como promedio, teniendo valores más bajos para organizaciones pequeñas, y obviamente más altos para organizaciones de tamaño importante, ya que nuestra área de ingeniería realiza los dimensionamientos de la necesidad del cliente, tanto actual como futura, y de acuerdo a eso se ofrecen las soluciones".

OPINIONES
Twitter @DiarioConce
contacto@diarioconcepcion.cl