LITORALPRESS

Fecha: 16-06-2018
Fuente: The Clinic
Título: **Ciberseguridad: Demos vida a la letra muerta**

Visitas: 179.238
VPE: 600.447

Favorabilidad: No Definida

Link: http://www.theclinic.cl/2018/06/16/ciberseguridad-demos-vida-la-letra-muerta/

Ciberseguridad: Demos vida a la letra muerta Lucía Dammert y Paula Vial 16 Junio, 2018 Aunque seguramente muchos deben ignorarlo, Chile tiene una Política Nacional de Ciberseguridad ) ¿Pero para qué sirve, si descansa en un cajón de escritorio? Como en muchas áreas, los gobiernos aprueban documentos que posteriormente pierden prioridad, dejando en el olvido largos procesos de participación público-privada donde se exponen avances y desafíos claros en una determinada temática. En ciberseguridad las amenazas son crecientes y requieren de acción rápida, lo que aún no está pasando. Robos, estafas, fraudes y suplantación de identidad son algunos de los delitos que se masifican por las redes de forma cotidiana. En la última década los países desarrollados han visto una sistemática caída de los homicidios y de los delitos callejeros como robos y hurtos, pero el menú de la inseguridad se ha llenado de las amenazas que llegan por la web. Las víctimas pueden ser individuos, instituciones o Estados. Los victimarios son de difícil rastreo, ubicados en otros países, con altos niveles de sofisticación y en muchos casos imposibles de rastrear. Sin duda, la ciberseguridad pone en jaque las capacidades investigativas de las instituciones policiales y el Ministerio Público así como los marcos legales que tienden a estar permanentemente desactualizados. Además la cibercriminalidad evidencia la complejidades de las cooperación policial internacional. Todos los que han sido víctimas de una clonación o fraude bancario saben que las respuestas son pocas y que el factor de que los hechos fueran organizados en otros países consolida la impunidad. Situación similar se observa cuando se analizan las organizaciones criminales que trafican mujeres y niñas con propósito de explotación sexual y que usan las redes para intercambiar información (incluso fotos) de las víctimas. La web permite todo tipo de intercambios ilegales, prácticamente todo se comercia en espacios encriptados, flexibles y poco rastreables. Sin embargo, necesitamos de la informática, la tecnología y las redes. Pero esperar que la prevención descanse en los individuos es poco serio. Los ciudadanos, cada día más conectados y realizando todo tipo de actividades desde sus teléfonos y computadores, no son los llamados a enfrentar de forma efectiva a grupos criminales de alta sofisticación y organización. El sistema bancario requiere aumentar las barreras de seguridad, compartir información sobre ataques, resultados y logros entre algunas medidas urgentes. El marco legal es antiguo y no entrega músculo real a la Superintendencia para jugar un rol en aumentar el conocimiento en esta materia. No parece adecuado ni conveniente que en la actualidad los bancos ofrezcan seguros anticlonación, cuando su principal labor es asegurar que sus sistemas sean seguros. Los clientes quedan desprovistos de la protección que sus instituciones deberían entregarles. Esta semana supimos que el Banco de Chile sufrió un ataque, se desconoce la magnitud del daño pero es evidente que no es ni la primera ni la última vez que el sistema financiero será atacado. Se requiere transparencia y efectividad en controles y soluciones, tanto públicas como privadas. No se trata sólo del patrimonio del banco, o de la institución que haya sido atacada en cada ocasión, ni siquiera del patrimonio de los usuarios, sino de la confianza en el sistema completo. Pero el dinero no es lo único que se intercambia en la web. La información personal tiene un alto valor y queda al menos la duda si las bases de datos de instituciones privadas y públicas son amenazadas. Estamos ciegos transitando un campo minado de múltiples ventanas del ciberespacio que están siendo mal reguladas y mínimamente protegidas. Más que inventar la rueda o constituir otra mesa de trabajo, vale la pena revisar la Política Nacional de Ciberseguridad promulgada pero sin implementación efectiva. Las ciberamenazas son evidentes y requieren de cambios legales, estrategias gubernamentales y acción privada rápida urgente. *Académica Universidad de Santiago de Chile **Académica Derecho UC Lorena Fríes y el incierto paradero de los fragmentos óseos encontrados en la AFDD: "No puede pasar por segunda vez que restos de seres humanos queden en el limbo" Por: Alejandra Matus y Benjamín Miranda 15 Junio, 2018