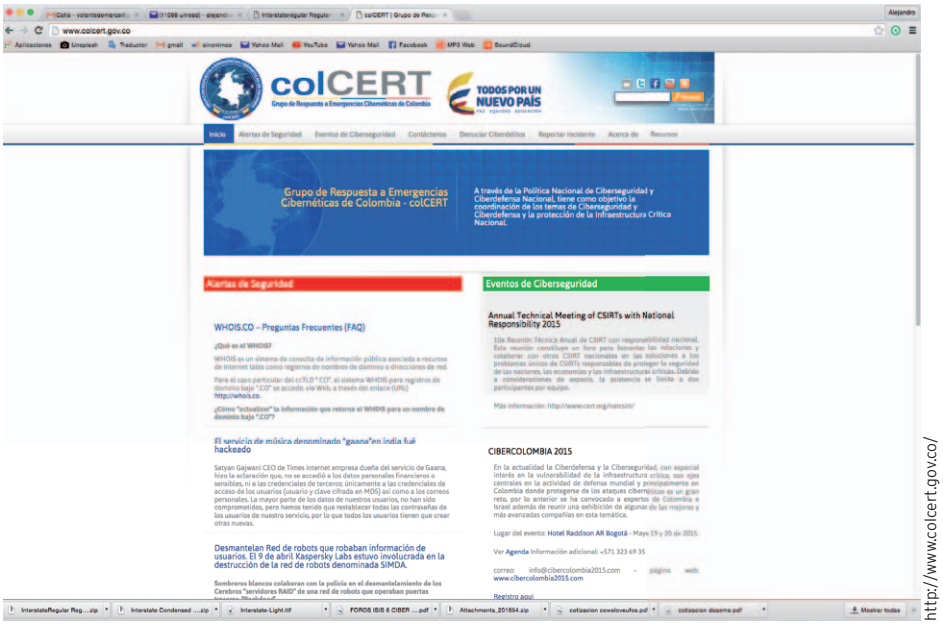
Coordinación, una práctica recomendable

Actuar en tiempo real, garantizar la contratación de expertos, crear mecanismos para que no se vayan a la empresa privada y generar alianzas entre las instituciones dedicadas a la ciberseguridad (Cert) estuvieron entre las recomendaciones de asistentes al foro.

Delegados de los Cert de Colombia, Ecuador, Guatemala, México y España hablaron de sus experiencias al frente de estos organismos que adoptaron su nombre de las siglas de *Computer Emergency Response Team*, de las mejores prácticas y de sus recomendaciones. Destacaron la coordinación como un procedimiento esencial para ser exitosos, así como la urgencia de retener al personal calificado con propuestas de carrera atractivas debido a que, por lo general, los funcionarios públicos se van a la empresa privada luego de que han sido muy bien entrenados.

Según Álvaro José Chávez, director del ColCert y director de la Seguridad Pública e Infraestructura del Ministerio de Defensa de Colombia, las alianzas han servido para detener ataques de cibercriminales tanto en esta nación como en otras latitudes. "A través de la red hemisférica de la OEA hay contacto con los 23 miembros, se interactúa con los otros Cert, se comparten buenas prácticas y *scripts* específicos y se hacen alianzas para la gestión de incidentes, de vulnerabilidades, se emiten alertas tempranas de dominios punto co no comerciales para inteligencia cibernética. Además, desarrollamos el proyecto Honeynet, para recopilar información de posibles atacantes".



http://www.colcert.gov.co/

La coordinación de los Cert de cada país es clave para compartir información que permita tomar acciones contra el crimen organizado que se mueve en la red.

> **"Es básica la formación en atención al usuario, porque los incidentes generan problemáticas y frustraciones en quien ha sido atacado, y saber guiarlo, tranquilizarlo y gestionar el asunto de la manera más adecuada conviene para la operatividad de la institución".**
>
> **José María de la Torre**

Ecuador: mejores prácticas son aprendizaje

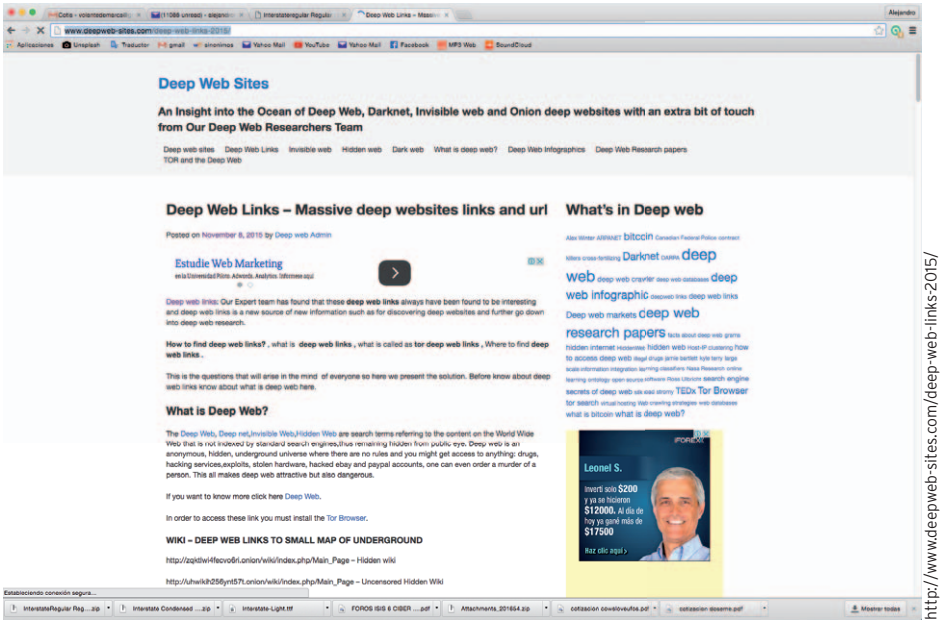
Los bajos presupuestos muchas veces limitan las acciones para adoptar los mecanismos de seguridad, dijo José María de la Torre. También recomendó actualizar constantemente la lista de contactos de los demás Cert para que al gestionar un incidente en otras latitudes se sepa a quién acudir.

Hay que darle al ente autoridad para exigir la atención de los problemas y es ideal que haga parte de la agencia de regulación de las telecomunicaciones. Se deben establecer protocolos de información de los sucesos que todo el equipo conocerá. Es básica la formación en atención al usuario porque los incidentes generan problemáticas y frustraciones en

quien ha sido atacado, y saber guiarlo, tranquilizarlo y gestionar el asunto de la manera más adecuada conviene para la operatividad de la institución. Otra lección aprendida es el establecimiento de la línea base para el tiempo de respuestas (SLA, *Service Level Agreement*). "La nuestra fue teórica, pero cuando la ajustamos a la realidad de los hechos, el Cert fue funcional", aseguró De la Torre.

En lo que tiene que ver con recurso humano, la contratación de los profesionales de seguridad debe ser acertada y para ello hay que tomarse el tiempo que sea necesario. El equipo requiere conocimiento básico técnico, pero también en idiomas, en negociación, en valores éticos, y debe recibir capacitación y especialización diversa y hacer seguimiento de las mejores prácticas. Por otra parte, es importante medir la capacidad de respuesta del grupo y recopilar estadísticas del trabajo para mejorarlo. Y luego de un incidente, generar unas preguntas para documentar lecciones aprendidas. Por otra parte, asegurar la permanencia de personal idóneo es uno de los mayores retos en lo concerniente al recurso humano.

> **"El uso de información histórica, del perfil técnico de los usuarios, junto con datos de sus hábitos financieros, sirvió para reducir en un 90 % los niveles de fraude en un banco de México y en un 50 % los falsos positivos".**
>
> **Gerardo González**



http://www.deepweb-sites.com/deep-web-links-2015/

Aunque no todo lo que se hace en la *deep web* es un delito, sí es un sitio propicio para el crimen porque es difícil rastrear este tipo de acciones.

"Hay que diseñar estrategias para retenerlos en el sector público", dijo.

Guatemala: responder en tiempo real

Una institución no debe cambiar la seguridad que ha implementado sino mejorarla, señaló Óscar Acevedo. Tal como los Cert europeos les dieron su apoyo al comenzar, los países de América Latina deben compartir lo aprendido. Esto facilita entender los ataques, categorizarlos y crear una base de datos de reputación, de manera que todos conozcan las IP de donde provienen y así frenar las acciones de los criminales. Las respuestas deben suceder en tiempo real.

México: protocolos sencillos, alta reducción de fraudes

Las metodologías adecuadas disminuyen sustancialmente los niveles de fraude a los clientes en las entidades financieras, señaló Gerardo González. Las más efectivas y transparentes se basan en su perfil o comportamiento: estadística, frecuencia, redundancia. El uso de información histórica, del perfil técnico de los usuarios, junto con datos de sus hábitos financieros, sirve para crear mecanismos de control de acceso altamente efectivo. El funcionario aseguró que el seguimiento de estos sencillos parámetros sirvió para reducir en un 90 % los niveles de fraude en un banco de México y en un 50 % los falsos positivos.

España: observar, orientar, decidir y actuar

La inteligencia tiene que ser más fina, debe ser de carácter permanente y permitir la anticipación a los hechos, afirmó Samuel Álvarez, director general del Grupo In-Nova que asesoró al Mando Conjunto de Ciberdefensa español.

Así mismo, mencionó las capacidades que deben tener los centros: prevención, mitigación, capacidad de resiliencia, evaluación dinámica del riesgo y fortalecimiento de la conciencia frente a este. Otras capacidades son toma de decisiones en tiempo real, defensa activa, colaboración e información compartida, análisis del *malware* y entrenamiento del personal que no duplique esfuerzos. Además, es necesaria una gran cooperación nacional e internacional, todo ello con un alto porcentaje de flexibilidad/gobernabilidad. En la creación del Mando Conjunto de Ciberdefensa español se utilizó el modelo de ODA gestado por un coronel estadounidense y que se resume en observar, orientar, decidir y actuar. ■