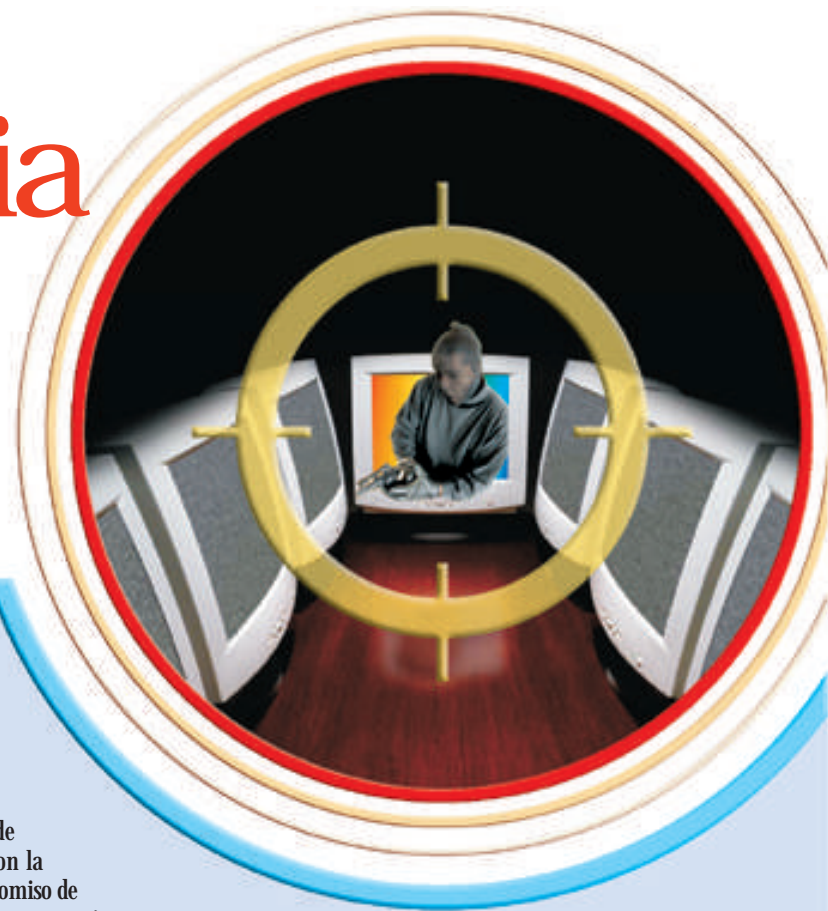


## CSIRT-Bolivia

*Accesos no autorizados, robo de información, fraude financiero, vandalismo web, ataques de virus y códigos dañinos, además de ataques de negación de servicios, son las prácticas más recurrentes de quienes buscan violar los sistemas de seguridad de alguna organización, ya sea por aventura, plagio o venganza.*

Por: Ramiro Mora  
Ingeniero Electrónico



**E**l crecimiento acelerado de las redes de computadoras conectadas a Internet y la diversidad de grupos de usuarios, hacen poco factible que una organización, por sí sola pueda proporcionar un soporte universal para solucionar problemas de seguridad. En este sentido, al interior de los gobiernos se están creando los Equipos de Respuesta a Incidentes de Seguridad Computacional o CSIRT (Computer Security Incident Response Team), por sus siglas en inglés.

Cuando llegan a ocurrir incidentes de seguridad computacional, se hace crítico para una institución responder de la manera más rápida posible al ataque. Y es que de la rapidez con la que se reconozca, analice y enfrente un problema, dependerá la limitación de los daños y de reducir los costos de recuperación de información. De ahí, la tendencia actual de contar con un grupo de profesionales especializados en el tema de la seguridad, en este caso un CSIRT.

De acuerdo al Centro de Coordinación CERT de la Universidad Carnegie Mellon de Pittsburgh, Estados Unidos ([www.cert.org](http://www.cert.org)), un CSIRT es una organización de servicio, responsable de recibir, revisar y responder frente a la notificación o descubrimiento de una contingencia de seguridad informática. Usualmente, sus servicios se realizan para una comunidad de usuarios definida. Por ejemplo, una entidad principal (una institución educacional o gubernamental) que abarque a una región o incluso un país.

### Red interamericana CSIRT de vigilancia y alerta

En la Segunda Conferencia Especializada sobre

Terrorismo realizada en Argentina, el 23 y 24 de noviembre de 1998 se concluyó con la adopción del Compromiso de Mar del Plata. Ese compromiso requería el establecimiento dentro de la Organización de los Estados Americanos de un "Comité Interamericano Contra el Terrorismo" integrado por las "autoridades nacionales competentes" de los estados miembros. Este esfuerzo fue respaldado además por los Jefes de Estado del hemisferio en el Plan de Acción de la Segunda Cumbre de las Américas en Santiago de Chile realizada el mismo año. La reunión posterior de la Asamblea General respaldó las recomendaciones y decisiones contenidas en el Compromiso de Mar Del Plata y estableció el Comité Iberoamericano Contra el Terrorismo – CICTE, mediante la resolución AG/RES. 1650 (XXIX-0/99).

El CICTE actúa como principal organización dentro del Sistema Interamericano para la coordinación de los esfuerzos destinados a proteger a los ciudadanos de los países miembros del flagelo del terrorismo. Funcionando a través del intercambio de información entre los principales líderes, los expertos en la materia y los encargados de tomar decisiones trabajan juntos para fortalecer la solidaridad y la seguridad hemisféricas.

Los objetivos básicos del CICTE, estipulados en el Compromiso de Mar del Plata, son:

- Mejorar el intercambio de información por las autoridades nacionales competentes,

incluyendo el establecimiento de una base de datos interamericana sobre cuestiones relacionadas con el terrorismo.

- Formular una propuesta para ayudar a los estados miembros a redactar la legislación apropiada contra el terrorismo en todos los Estados.
- Recopilar los tratados y acuerdos bilaterales, subregionales y multilaterales suscritos por los Estados miembros y promover la adhesión universal a las convenciones internacionales contra el terrorismo.
- Aumentar la cooperación en las fronteras y las medidas de seguridad relacionadas con la documentación de viajes.
- Desarrollar actividades de entrenamiento y manejo de crisis.

El primer período ordinario de sesiones del CICTE se realizó en Miami, Florida en Octubre de 1999 y durante el mismo se desarrolló un plan de trabajo. Una segunda sesión ordinaria planificada para realizarse en Bolivia en 2000 tuvo que ser cancelada a último momento. Ninguna sesión fue programada en 2001.



El cuarto período ordinario de sesiones del CICTE se llevó adelante en Montevideo, Uruguay entre el 28 y 30 de enero de 2004, donde se redactó la declaración de Montevideo, reafirmando de esta manera su condena al terrorismo en todas sus formas y manifestaciones por constituir una grave amenaza a la paz, seguridad internacional y al bienestar, seguridad, prosperidad y desarrollo de los Estados Miembros.

Para alcanzar los objetivos propuestos, es puesto en consideración un plan de trabajo denominado "Marco para establecer una red interamericana CSIRT de vigilancia y alerta", que fue presentado por la Embajadora Margarita Escobar, Presidenta del Grupo de Trabajo de la Comisión de Seguridad Hemisférica de la OEA, en la Tercera Sesión Plenaria celebrada el día 29 de enero de 2004. Con base a este documento se realizó un análisis, modificación y consenso en el Taller Para Practicantes en Materia De Seguridad Cibernética, desarrollado en Ottawa, Canadá entre el 29 y 30 de marzo de 2004, dando como resultado un nuevo documento titulado "Recomendaciones del Taller de practicantes en materia de seguridad cibernética del CICTE a la estrategia integral de seguridad cibernética", el que será presentado al CICTE y posteriormente en la asamblea de la OEA a llevarse adelante en junio de 2004

## Bolivia contra el terrorismo cibernético

El terrorismo, cualquiera sea su origen o motivación, no tiene justificación alguna y constituye una grave amenaza a los valores y principios que sustentan el orden interamericano y las instituciones y libertades democráticas protegidas y promovidas por la Carta de la OEA, la Carta Democrática Interamericana y otros instrumentos internacionales, incluidos los instrumentos internacionales de derechos humanos.

La importancia de que los Estados sometan a la justicia a los responsables de planificar, financiar y cometer actos de terrorismo; y que para continuar la lucha contra el terrorismo es imprescindible mejorar, de conformidad con la legislación nacional, el intercambio de información y experiencias entre las autoridades nacionales competentes, como un aspecto fundamental de la cooperación entre los Estados del Hemisferio.

Bolivia no puede quedar al margen de este proyecto que busca enfrentar de manera eficaz y eficiente al terrorismo en un campo totalmente nuevo como es el cibernético, es por esta razón que estamos en la obligación de identificar a la brevedad posible

un punto de contacto nacional, que permita el intercambio de información, y a la par trabajar en el desarrollo del CSIRT – Bolivia, con el apoyo de todas las organizaciones involucradas en este tema.

La Agencia para el Desarrollo de la Sociedad de la Información en Bolivia, conjuntamente la Cancillería de la República, están llevando adelante la conformación del CSIRT – Bolivia, que en las próximas semanas pondrá a disposición una página web informativa y un correo electrónico como punto de contacto para el envío y recepción de información relacionada con actividades terroristas, lo que permitirá realizar un trabajo coordinado con el resto de los CSIRTs que conforman la Red Iberoamericana de Vigilancia y Alerta ■

### WEBSITES

<http://www.cert.org>  
<http://www.arcert.gov.ar>  
<http://www.first.org>  
<http://www.rediris.es/cert>  
<http://www.adsib.gov.bo>  
<http://www.rree.gov.bo>

**La Paz**  
 Av. 6 de Agosto N° 2460  
 Telf: (591-2) 2441404  
 Fax: (591-2) 2442020  
 e-Mail: info@bis.cnb.net

**Cochabamba**  
 Av. Oquendo N° 654, Torres Sofer  
 Telf: (591-4) 4230888  
 Fax: (591-4) 4530777  
 Casilla 6029  
 e-Mail: info@albatros.cnb.net

**Santa Cruz**  
 C. Seoane N° 33, Edif.  
 Baldovinos 1er. piso, Of. 10  
 Telf: (591-3) 3326776  
 Fax: (591-3) 3322292  
 e-Mail: info@tucan.cnb.net

**Sucre**  
 Plaza 25 de Mayo, Multicentro  
 Céspedes, Of. 206A  
 Telf: (591-4) 6447202  
 Fax: (591-4) 6449555  
 e-Mail: info@pelicano.cnb.net  
<http://www.cnb.net>

Ahora con nuestra **Tarjeta PrePago...**  
 ...internet **más fácil.**



Incluye casilla de correo electrónico.  
 Sólo se paga los minutos de conexión.  
 Sin Contrato, sin cobros adicionales.  
 Acceso con llamada local desde cualquier computador, en  
 La Paz, Cochabamba, Santa Cruz y Sucre.

**COMPU.NET**  
 Calidad en Internet