

**3er CHAT del CELAES/FELABAN  
DELITOS POR INTERNET  
Agosto 31 de 2004**

**(Indicar cuales fueron los Países que participaron en este Chat)**

A continuación mostramos un resumen de los comentarios y conclusiones realizados en el chat organizado por Felabán y la Asobancaria Colombia, sobre delitos por Internet.

**Keylogger.**

Todos los países participantes en el chat, afirmaron tener conocimiento de casos de keylogger desde los café Internet. Adicionalmente, en Perú se reportó un caso de keylogger instalado de forma remota en un computador calificado como seguro, mediante el uso de un virus troyano.

Con el fin de contrarrestar esta problemática, los países han adoptado diferentes medidas de seguridad preventivas y correctivas y que incluyen:

- Protección de los servidores de la entidad y los equipos utilizados por los trabajadores, con el fin de impedir la instalación de programas no autorizados. (Venezuela, Ecuador, Colombia)
- Implementación de teclados virtuales en las páginas de Internet de las entidades. (Perú, Colombia)
- A través de un proveedor de servicios de Internet local, se ha establecido un acuerdo de identificación y bloqueo de las direcciones IP desde donde proceden las operaciones fraudulentas. (Perú)
- Realización de reuniones con la rama de investigación de la Policía Nacional, con el fin de identificar a los responsables de estos actos ilícitos. (Perú)
- Definición y publicación de medidas de seguridad preventivas dirigidas a clientes. (Colombia)

**Transferencias bancarias, pagos a terceros.**

Varios países reportaron tener información sobre fraudes por transferencias bancarias o pagos de servicios desde cuentas que son violadas obteniendo la información por diferentes medios.

Para contrarrestar esta modalidad de fraude, la principal medida tomada, ha sido la definición y publicación de medidas de seguridad preventivas dirigidas a clientes.

Adicionalmente, las entidades han implementado una serie de medidas que buscan disminuir la posibilidad de fraude a través de este canal, entre las que se encuentran:

- Establecimiento de límites para el pago de servicios.
- Inscripción obligatoria y previa de las cuentas desde donde se desea realizar los pagos de servicios o las transferencias.

- Realización de preguntas adicionales para confirmar la identidad del cliente una vez este ha ingresado su clave (esto incluye también los cajeros automáticos), tales como el día de nacimiento, algunos dígitos de su identificación personal, etc.

### **Impacto en los clientes.**

No obstante la problemática expuesta, todos los países afirmaron que no se ha presentado disminución alguna en el uso del canal Internet, como consecuencia de los delitos a través de este.

### **Certificados digitales.**

Varios países utilizan o están en proceso de implementar el uso de certificados digitales para las transacciones desarrolladas por sus clientes utilizando Internet.

### **Bloqueo de la clave.**

Los países participantes en el chat (con excepción de Venezuela), afirmaron que realizan bloqueos de la clave de Internet cuando se presentan tres intentos fallidos o por medida preventiva cuando se presentan operaciones que no corresponden al perfil del cliente. Esto motivado a que en Venezuela, tienen varios niveles de Claves, que a medida que el Usuario de la Web va interactuando y profundizando en Operaciones mas complejas, se Le van solicitando otras Claves, existen tres Niveles de Claves y las mismas las programa el usuario al ingresar por primera vez, para ello e le solicita información diversa y variada que solo esta en cuenta el dueño de la cuenta, adicionalmente, el Sistema tiene un filtro que no permite que se utilice la misma Clave en los tres niveles y tampoco que la Clave de Internet, sea igual a la de Cajeros Automáticos, ni a la de Atención Telefónica, todas estas Claves son diferentes.

### **Auditoria de Firewalls.**

En general, la auditoría de los logs de los firewalls la realizan las áreas de auditoría de sistemas o seguridad informática.