COOPERATIVA DE AHORRO Y CRÉDITO ABIERTA

San Antonio R.L.

Instructor: Mgr. Carlos José Rojas Mendoza.

Legitimación de ganancias ilícitas, financiamiento al terrorismo y/o delitos precedentes.
Recomendaciones de seguridad son las más indicadas
Unidad de Prevención y Cumplimiento.

Legitimación de ganancias ilícitas

Concepto.-

También conocido como lavado de activos o lavado de dinero consiste en tratar de ocultar o disfrazar el origen ilícito de bienes o recursos que provienen de actividades delictivas, buscando darles apariencia de legalidad. El objetivo de la operación consiste en hacer que estos fondos o activos obtenidos ilegalmente aparezcan como el resultado de actividades legítimas y circulen sin problema en el sistema financiero.

Legitimación de ganancias ilícitas

¿De dónde proviene?

El lavado de activos proviene de delitos como el narcotráfico, contrabando, extorsión, secuestro, trata de personas, estafa, tráfico de armas, entre otros.

Legitimación de ganancias ilicitas

¿Cómo funciona?

Un ejemplo claro del funcionamiento del lavado de activos es el siguiente: si un cliente realiza la cancelación de su crédito, que inicialmente tenía un plazo de 10 años pero lo cancela anticipadamente, el Banco le solicitará información y/o documentación que respalde el origen de los fondos con los cuales realizó el pago total del préstamo.

Si el cliente no proporciona los respaldos solicitados hace pensar que podría estar cometiendo el delito de lavado de dinero y podría ser señalado de violar la ley, de confirmarse la comisión del delito.

Legitimación de ganancias ilícitas

¿Y cómo funciona con los bienes?

El lavado de activos con propiedades funciona de la siguiente forma: El delincuente -con dinero ilícito- decide comprar un bien, por ejemplo, una vivienda, pero no a su nombre, sino al de otra persona que inocentemente puede prestarse para la adquisición del bien.

Legitimación de ganancias ilícitas

¿Qué recomendaciones de seguridad son las más indicadas?

· Se aconseja indagar siempre sobre la procedencia del dinero y bienes, sin importar si se trata de un familiar o de un amigo.

· No prestar su nombre, identificación o cuentas a terceras personas.

· Dude de negocios fáciles.

· Rechazar la cultura del dinero fácil.

· Exigir factura al realizar compras de bienes y servicios.

¿Qué es el Financiamiento del Terrorismo?

El Financiamiento del Terrorismo es cualquier forma de acción económica, ayuda o mediación que proporcione **apoyo financiero a las actividades de grupos terroristas.**

¿QUÉ ES LA UIF?

Es la Unidad de Investigaciones Financieras (UIF), que se encarga de normar el régimen de Lucha Contra el Lavado de Dinero y Financiamiento del Terrorismo en consulta con el Ministerio de Economía y Finanzas Públicas (MEFP) y las autoridades de supervisión; investigar los casos en los que presuma la comisión de delitos de Legitimación de Ganancias Ilícitas, financiamiento al terrorismo y otros de su competencia; y realizar el análisis, tratamiento y transmisión de información para prevenir y detectar los delitos señalados en el Artículo Nº 495 de la Ley Nº 393 de 21 de agosto de 2013.

BANCA ELECTRONICA

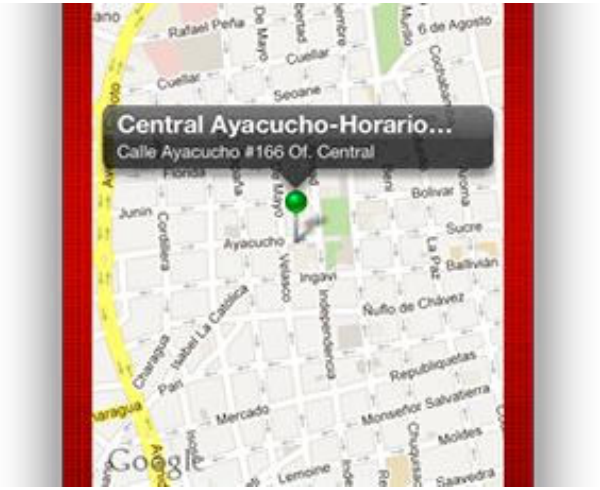
Concepto.-

Se la llama de esta manera puesto que es aquella a la cual se accede vía internet para hacer uso de los distintos servicios y productos que ofertan las Entidades Financieras.

También hace referencia al tipo de banca que se realiza por medios electrónicos como ser cajeros automáticos, teléfono celular inteligente (smartphone) y otras redes de comunicación.

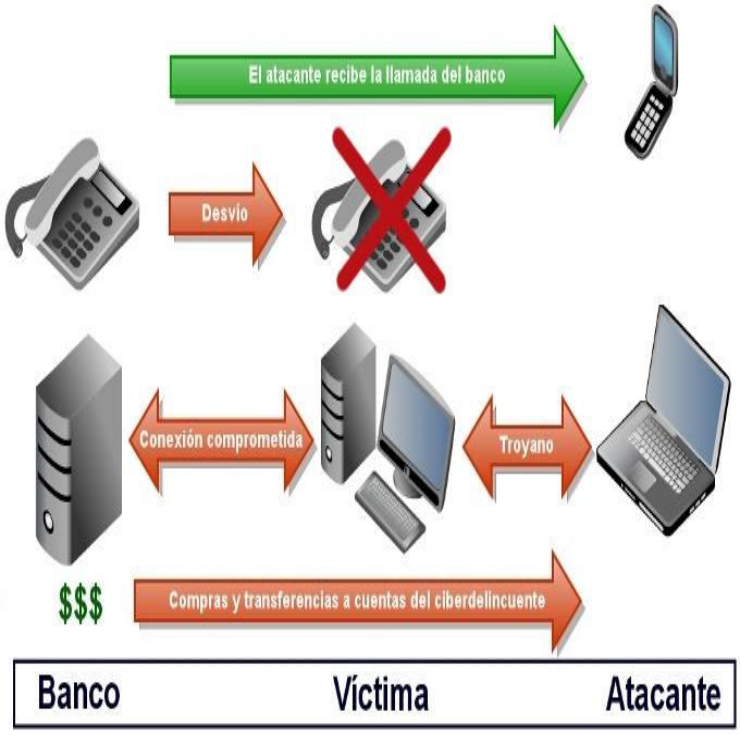
Ventajas y beneficios

- Comodidad y servicios de conveniencia, 24 horas al día, 7 días a la semana.
- Acceso global.
- Operaciones desde casa u oficina.
- Ahorro en tiempo.
- Oferta de productos y servicios personalizados.
- Seguridad al momento de realizar transacciones.



Desventajas y amenazas

- Su acceso y utilización es únicamente para clientes con cuentas aperturadas.
- Es recomendable una buena conexión a internet para evitar dejar a medias o sufrir cortes mientras se realiza una operación on line.
- Preocupación por la seguridad (virus, hackers, phishing, etc.) y por la información personal.
- Si se cometen errores al momento de autentificarse, el sistema bloquea su acceso puesto por seguridad, para recuperar sus claves debe dirigirse personalmente al Banc0.



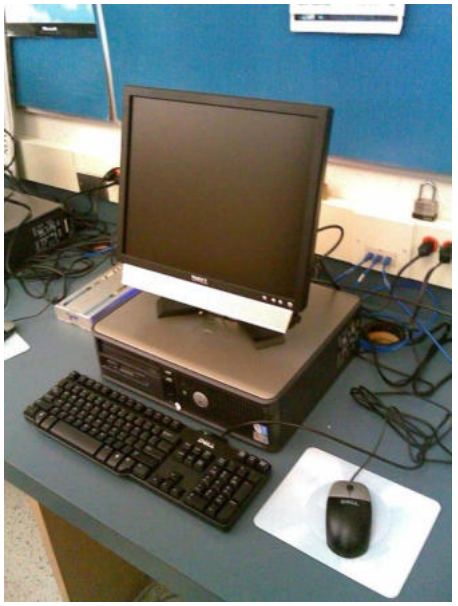
POSIBLES RIESGOS

- Si otra persona llega a conocer su clave secreta, podrá entrar a sus cuentas y realizar operaciones en su nombre
- Si la computadora o dispositivo móvil desde el que accede está infectado por un virus, puede permitir que otros accedan a sus cuentas y realicen operaciones.
- Si se facilita información confidencial (claves y datos personales a terceros) por ejemplo, dando respuesta a un e-mail que parecía enviado por su entidad bancaria, alguien podrá acceder a su cuenta

RECOMENDACIONES

- Proteja y cambie periódicamente sus contraseñas
- No abra ni responda e-mails de personas desconocidas
- No ingrese a sitios "no seguros" en internet
- Cierre siempre la sesión al concluir las operaciones de banca electrónica
- No entre a su banco desde computadoras públicas
- Ingrese siempre digitando la dirección de su entidad financiera

Transacciones seguras



Certificados de seguridad

- La Certificación Digital emitido por una empresa certificada empresa a certificar es quien dice ser. De esta forma, usted puede asegurarse que está comunicándose única y exclusivamente con la EIF.

PROTOCOLO SEGURO

- El canal de transmisión de información entre usted y EIF debería utilizar el protocolo de comunicación SSL (Secure Sockets Layer) basado en tecnología de encriptación.
- Este ambiente seguro, ayuda a proteger la confidencialidad de sus datos cuando realice operaciones bancarias en línea en nuestro sitio.

ENCRIPTACION DE DATOS

- La encriptación de datos, es un mecanismo por el cual, la información intercambiada entre el cliente y la EIF se transforma en una codificación ilegible, con una secuencia de caracteres de lenguaje particular, que esconden el significado real de la información. Cuando la información llega a destino, se realiza el proceso inverso donde el servidor de la EIF descifra la información recibida, transformándola en datos capaces de ser procesada.

NAVEGADORES RECOMENDADOS

- Las EIF les sugieren la utilización de los Navegadores Microsoft Internet Explorer 7.0 o uno superior, o también Firefox 2.0 o superior.
- Si Usted no está seguro acerca de la versión de su navegador, siga los siguientes pasos:
- Clickee sobre la opción "Ayuda" o "Help" en la barra de menú de su navegador.
- Seleccione la opción "Ayuda" / "Acerca de Mozilla Firefox".
- Se abrirá una ventana con la información sobre la versión de su navegador.

TIME OUT O CIERRE DE SESION AUTOMATICO

- Es recomendable cerrar la sesión antes de navegar por otros sitios o de apagar su PC. Le alertamos a no navegar por otros sitios durante su sesión abierta de operaciones bancarias ó en línea.
- Si usted olvida finalizar su sesión al utilizar el sitio de transacciones de la Banca por Internet, el sistema de la EIF lo realizará por usted cerrando la sesión automáticamente pasados los 60 segundos, más o menos, si es que no hubo actividad en el sitio.

Clave de Acceso ó PIN

- Es un número secreto emitido con alta seguridad por los sistemas del de la EIF y se le entrega en un sobre cerrado. Este código es absolutamente confidencial y solo debe ser de conocimiento suyo y de nadie más, porque ni la entidad lo sabe. Al ingresar por primera vez usted debe introducir esta clave de acceso que viene en el sobre, por única vez, puesto que después debe cambiarlo por una clave propia. La siguiente vez que ingrese debe utilizar esta clave que usted eligió. Por su seguridad después de 3 intentos fallidos de ingresar la clave, se bloquea el acceso definitivamente, debiendo solicitar personalmente en las oficinas y/o agencias el desbloqueo o reimpresión de la Clave de Acceso

PERFILES

- Para acceder al ambiente transaccional de la Banca por Internet se puede realizar con uno de los tres perfiles de usuario a disposición del interesado:
- Perfil A: Solo consultas.
- Perfil B: Consultas y transferencias entre cuentas propias.
- Perfil C: Consultas, transferencias entre cuentas propias y transferencias a cuentas de terceros.

Prevención de Fraude y Protección de Datos

- Ingrese a la página Web de forma segura, tipeando en el explorador, cada vez que ingresa. Nunca usar enlaces.
- Verifique el acceso a sitios seguros. La dirección de Internet (URL) de la página cuando la conexión se realiza en un ambiente seguro muestra "https" al principio, en lugar de "http".
- Internet Explorer muestra un candado cerrado en la parte inferior derecha al ingresar a una página segura. Haciendo clic en el candadito podrá comprobar la vigencia / validez del Certificado Digital y el tipo de encriptación.

- Firewall o Servidor de seguridad: Es un software o hardware que ayuda a impedir el paso a los hackers, virus y gusanos informáticos que intenten entrar en su equipo a través de Internet.
- Actualizaciones: Ayudan a proteger su computadora de vulnerabilidades, virus, gusanos y otros ataques dañinos conforme estas aparecen.
- Antivirus: Le ayuda a proteger su equipo contra los virus, gusanos, troyanos y otros invasores no deseados, que pueden hacer "enfermar" a su equipo.
- Para eliminar contraseñas almacenadas ingrese al menú "Herramientas" de su Internet Explorer, luego clic en "Opciones de Internet", haga clic en el tab de "General" Luego haga clic en el botón "Eliminar", busque la opción de contraseñas y haga clic en el botón eliminar, luego en "Aceptar". Para que se ejecute la actualización usted deberá cerrar su explorador de Internet y volver a abrirlo para que tome la nueva configuración.