

12304

ANEXO No. 3
Lineamientos de Seguridad Informática para el Operador Bancario

Las siguientes son condiciones generales que el OPERADOR BANCARIO deberá cumplir en cuanto a sus sistemas de información para todas las operaciones financieras:

- Toda transmisión electrónica de información, bien sea archivos descargables, correos electrónicos o archivos adjuntos a ellos, deberán estar cifrados bajo una estructura de llave pública y privada, cuyos certificados sean emitidos por una autoridad certificadora reconocida, de forma tal que se garantice la integridad, confidencialidad y el no repudio de la información. En caso de requerirse un licenciamiento para suplir esta condición, éste deberá ser proporcionado por el OPERADOR BANCARIO.
- EL OPERADOR BANCARIO deberá ponderar la exposición al riesgo financiero y operativo de los sistemas de transferencia y considerar, en consecuencia, las instancias internas de revisiones y autorizaciones previas que sean necesarias.
Para el adecuado control de los riesgos inherentes a la utilización de estos sistemas, es necesario que el OPERADOR BANCARIO cuente con profesionales capacitados para evaluarlos antes de su liberación y para mantener bajo vigilancia, mediante procedimientos de auditoría acordes con la tecnología utilizada, su funcionamiento, mantenimiento y necesidades de adecuación de los diversos controles computacionales y administrativos que aseguran su confiabilidad.
- Los procedimientos implementados por el OPERADOR BANCARIO para el portal y las comunicaciones con el ICBF, deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse claves y mecanismos de acceso al sistema y al tipo de operación, que permitan asegurar su autenticidad e integridad.
- EL OPERADOR BANCARIO debe mantener permanentemente abierto y disponible un canal de comunicación que permita al ICBF ejecutar o solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso o claves de autenticación. Cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real.
- EL OPERADOR BANCARIO deberá contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de identificar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deberán establecer y mantener, de acuerdo a la dinámica de los fraudes, patrones conocidos de estos y comportamientos que no estén asociados al ICBF.

Estos sistemas o mecanismos deberán permitir tener una vista integral y oportuna de las operaciones del ICBF, del no cliente (por ejemplo en los intentos de acceso), de los puntos de acceso (por ejemplo direcciones IP, Cajero Automático u otros), hacer el seguimiento

12304

y correlacionar eventos y/o fraudes a objeto de detectar otros fraudes, puntos en que estos se cometen, modus operandi, y puntos de compromisos, entre otros.

El OPERADOR BANCARIO deberá proporcionar un portal web para realizar todas las transacciones bancarias, descarga de reportes y archivos, el cual deberá cumplir con las siguientes características:

- Usar protocolo HTTPS.
- Utilizar SSL para asegurar las conexiones entre el browser y el portal bancario, bajo una estructura de llave pública y privada cuyos certificados digitales sean emitidos por una autoridad certificadora reconocida.
- Contar con una plataforma tecnológica que comprenda una encriptación sólida con algoritmos de encriptación modernos.
- La longitud de clave de los certificados digitales para el esquema de llave pública y privada es de mínimo 1024 bits.
- Los certificados digitales deberán tener periodos de vigencia no mayores a 1 año.
- No debe utilizar cookies para almacenar información de sesión ni credenciales de usuario, de forma local.
- No debe permitir que sesiones inactivas permanezcan abiertas por más de 5 minutos.
- Permitir el registro y seguimiento íntegro de las operaciones realizadas, deberá generar archivos que permitan respaldar los antecedentes de cada operación, necesarios para efectuar cualquier examen o certificación posterior, tales como fechas y horas en que se realizaron, contenido, identificación de los operadores, emisores y receptores, cuentas y montos involucrados, terminales desde los cuales se operó.
- Proveer un perfil de seguridad que garantice que las operaciones solo puedan ser realizadas por personal debidamente autorizado, resguardando la privacidad y confidencialidad de la información transmitida o procesada por ese medio.
- Contar con métodos de autenticación en el portal bancario, incluyendo además del uso de contraseñas seguras, la verificación de dirección IP pública desde donde se origina la conexión al portal, de forma tal que no se acepte log-in desde direcciones IP desconocidas que no pertenezcan al ICBF, con las credenciales de usuario asignadas al personal autorizado por la entidad.
- Toda transmisión de información, incluyendo la descarga de archivos desde el portal, debe realizarse por canales seguros. Dichos archivos deberán estar cifrados utilizando una estructura de llave pública y privada avalada por una autoridad certificadora reconocida, de forma tal que se pueda garantizar la confidencialidad y el no repudio de la información transmitida. En caso de necesitarse algún licenciamiento para suplir esta condición, éste deberá ser provisto por el OPERADOR BANCARIO.
- Reconocer la validez de la operación que el usuario realice.

12304

- Los sistemas de transferencia electrónica de fondos deberán generar la información necesaria para que el ICBF pueda conciliar los movimientos de dinero efectuados, tanto por terminales como por usuario habilitado, incluyendo, cuando corresponda, totales de las operaciones realizadas en un determinado período.

Contener los mecanismos de seguridad para controlar que se ejecuten todas las operaciones que se inician, debiendo estar en condiciones de detectar cualquier alteración o intervención a la información transferida, entre el punto en que ésta se origina y aquel en que es recibida por el destinatario.