PROTOCOLO GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL OPERADOR BANCARIO.

1. Propósito

Dar cumplimiento a los requerimientos de Seguridad de la Información en materia de la prestación del servicio como operador bancario y financiero requerido por el ICBF para el manejo integral de la operación de la Direccion Financiera.

2. Requerimientos:

- ✓ El operador bancario debe dar cumplimiento a las políticas de Seguridad y Privacidad de la Información y Seguridad Digital del ICBF, adoptadas mediante actos administrativos internos.
- ✓ El operador bancario debe implementar todos los requerimientos solicitados por la Superintendencia Financiera de Colombia a través de las circulares externas en materia de Seguridad y Privacidad de la Información, continuidad de la operación y Seguridad Digital (Ciberseguridad)
- ✓ El operador bancario deberá dar estricto cumplimiento a lo establecido en la ley 1581 de 2012 y 1712 de 2014 y sus decretos reglamentarios.
- ✓ El operador bancario deberá dar estricto cumplimiento a lo estipulado en la Matriz de requisitos legales suministrada por el ICBF, en materia de seguridad de la información, Seguridad y Salud en el Trabajo, Gestión Ambiental y Calidad.
- ✓ El ICBF y el Banco deben establecer un canal de comunicación de manera segura, para lo cual se debe establecer una VPN Site to Site entre el Banco y el ICBF.
- ✓ El Banco deberá colocar los archivos objeto del contrato, comprimidos en un archivo y cifrado por medio algoritmos de cifrado para las comunicaciones, deben ser como mínimo 3DES, SHA-1, IKE o de características superiores, en un servidor File Transfer Protocol Secure (FTPS) que dispondrá el ICBF para tal fin.
- ✓ La conexión al servidor FTPS del ICBF solo se podrá hacer vía VPN Site to Site.

PUBLICA

- ✓ Como plan de contingencia en caso tal de no lograr conexión entre las partes (Banco - ICBF), por problemas en la infraestructura del ICBF, éste dispondrá la forma de transmitir los archivos, activando su plan de continuidad del servicio.
- ✓ Como plan de contingencia en caso tal de no lograr conexión entre las partes (Banco - ICBF), por problemas en la infraestructura del Banco, éste dispondrá la forma de transmitir los archivos, activando su plan de continuidad del servicio, y garantizando el mismo nivel de seguridad.
- ✓ Los archivos transmitidos deben seguir los protocolos establecidos y en todo caso aplicando las reglas de seguridad y validación definidas para el sector financiero por el Departamento para la Prosperidad Social - DPS.
- ✓ Las credenciales de acceso al servidor FTPS serán suministrados por ICBF al Banco mediante un mecanismo de custodia de claves definido por ICBF.
- ✓ La configuración de la VPN Site to Site deberá hacerse de manera conjunta entre el Banco y el ICBF para garantizar la conexión exitosa de los involucrados; para esto se debe establecer una mesa de trabajo en conjunto con los analistas y administradores de la infraestructura de tecnología del ICBF.
- ✓ La conexión entre las partes debe estar disponible en los horarios y días que estipule el ICBF pudiendo llegar a ser 7x24 (7 días a la semana, 24 horas al día), para garantizar el consumo oportuno de los archivos producto del objeto contractual.
- ✓ Es responsabilidad del Banco garantizar la integridad, disponibilidad y confidencialidad de la información suministrada al ICBF desde su origen hasta su destino; por tanto, se debe enviar el código hash para verificar integridad del documento.
- ✓ El Banco debe suministrar al ICBF la información en el formato que lo exija.
- ✓ El Banco debe dar cumplimiento a las circulares en temas de transferencia de información, confidencialidad, integridad y disponibilidad dispuestas por la Superintendencia Financiera de Colombia.
- ✓ El Banco deberá disponer de mecanismos para descargar diariamente un reporte detallado de los giros y transferencias efectivamente realizados, así como aquellos rechazados, el cual deberá incluir al menos: fecha de la transacción, información

PÚBLICA

detallada del beneficiario (identificación y razón social), valor del giro, y en caso de rechazo, la identificación de la causal de rechazo.

- ✓ El Banco deberá entregar de manera cifrada y de acuerdo a los requerimientos que el ICBF estipule un reporte detallado que permita realizar la auditoria a las transacciones realizadas.
- ✓ El Banco deberá entregar de manera cifrada y como el ICBF estipule la información de los giros rechazados sobre operaciones ACH y CENIT.
- ✓ El Banco debe proporcionar al ICBF mecanismo con protocolos seguros para transferir electrónicamente los recursos desde las cuentas del ICBF en el banco, hacia cuentas del ICBF en otros bancos y las transferencias que el ICBF le deba realizar a las cuentas del Tesoro Nacional
- ✓ El Operador debe garantizar la confidencialidad de la información recolectadas a través de Planilla Integrada de Liquidación de Aportes (PILA), tanto asistida como electrónica, Recaudos por conceptos diferentes a PILA (régimen exceptuado PILA, cartera de fiscalización, venta de bienes, prueba de filiación, entre otros),
- ✓ El Banco deberá dar cumplimiento a la normatividad vigente, cualquiera que la adicione, modifique o derogue, emitidas por los entes reguladores del Estado Colombiano, en relación con el tratamiento de la información de datos personales, financieros y cualquiera que en el marco del contrato se gestione para el ICBF.
- ✓ El Banco debe garantizar que la información adquirida por otros medios distintos a los propios, cuenten con los niveles de confiabilidad, confidencialidad, integridad y no repudio de la misma y la transmisión de información que se vaya a proporcionar al ICBF entre el Banco y Terceros debe contar con los mecanismos de seguridad que se tienen entre el Banco y el ICBF.
- ✓ El Banco debe contar con las siguientes características de Seguridad y almacenamiento de Información.
    - La solución de almacenamiento de la información histórica debe contar con la integridad referencial necesaria.
    - La base de datos histórica de las transacciones debe estar disponible en el tiempo y los medios que el ICBF considere.
    - La entrega de las copias de seguridad se debe hacer de forma cifrada y confidencial, de acuerdo a los parámetros que el ICBF establezca.

PUBLICA

- ✓ El Banco deberá contar con políticas, metodologías de identificación, análisis y tratamientos de riesgos de seguridad de la información, en el marco del objeto contractual.
- ✓ El Banco deberá contar con gestión de los incidentes de Seguridad de la Información, en caso de presentarse un incidente en el marco del contrato deberá ser informado al ICBF detallando, la fuente, causas, remediaciones y acciones tomadas para mitigar el mismo.
- ✓ Toda transmisión electrónica de información bien sea archivos descargables, correos electrónicos o archivos adjuntos a ellos, deberán estar cifrados bajo una estructura de llave publica y llave privada, cuyos certificados sean emitidos por una autoridad certificadora reconocida, de forma tal que se garantice la integridad, confidencialidad y no repudio de la información. En caso de requerirse un licenciamiento para suplir esta condición, este deberá ser proporcionado por el Banco.
- ✓ El banco 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 banco cuente con profesionales capacitados para evaluarlos antes de su liberación y para mantener bajo vigilancia, mediante procedimientos de auditoria acordes con la tecnología utilizada, su funcionamiento, mantenimiento y necesidades de adecuación de los diversos controles computacionales y administrativos que aseguren su confiabilidad.
- ✓ Los procedimientos implementados por el banco para el portal y las comunicaciones con el ICBF, deberán impedir que tanto el originador como el destinatario, en su caso, desconozcan la auditoria 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 banco 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 deberá establecer y mantener, de

PÚBLICA

acuerdo con 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 oportunas de las operaciones del ICBF, del no cliente (por ejemplo, intentos de acceso), de los puntos de acceso (por ejemplo: direcciones IP's, Cajero automático, y otros), hacer seguimiento y correlacionar eventos y/o fraudes al objeto de detectar otros fraudes, puntos en que estos se cometen, modo de operación del fraude, y puntos de compromisos, entre otros.
- ✓ El banco deberá proporcionar un portal web para realizar todas las transacciones bancarias, descargas de reportes y archivos, el cual deberá cumplir con las siguientes características:
  - Protocolo de comunicación HTTPS.
  - Certificado de seguridad del sitio mínimo de 1024 bits
  - Modo de autenticación seguro (Teclado en pantalla, token, biométrico, etc.)
- ✓ El banco debe habilitar estándares, procesos y procedimientos de seguridad que cumplan o superen las establecidas en las circulares emitidas por las entidades gubernamentales en materia de seguridad de la información.
- ✓ Sobre los portales bancarios de acceso a través de la Internet, el operador bancario deberá implementar algoritmos y protocolos necesarios para brindar una comunicación segura.
- ✓ El operador bancario deberá realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicaciones usados en la realización de transacciones del ICBF. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.
- ✓ El operador bancario deberá poner a disposición de ICBF los mecanismos necesarios que reduzcan la posibilidad de que la información de las transacciones pueda ser capturada por terceros no autorizados durante cada sesión.
- ✓ El operador bancario deberá configurar a 3 minutos como el tiempo máximo de inactividad, después del cual deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.
- ✓ El operador bancario deberá informar al ICBF, el inicio de cada sesión, la fecha y hora del ultimo ingreso al canal electrónico.

PÚBLICA

- ✓ El operador bancario deberá garantizar al ICBF la Implementación de mecanismos que le permitan verificar constantemente que no sean modificados los enlaces (links) de su sitio web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.
- ✓ El operador debe establecer una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad

3. Control de Cambios del documento

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS	Autor (es) / Cargo / Dependencia
1.0	19/08/2015	Creación del documento	Andrés Díaz Molina / Seguridad de la información / DIT-SRT-SGSI
2.0	17/07/2018	Modificación de acuerdo con las circulares de la Superintendencia financiera de Colombia y las políticas de seguridad del ICBF	Andrés Díaz Molina / Seguridad de la información / DIT-SGSI

PÚBLICA