



**Superintendencia de Bancos
y Entidades Financieras**
Bolivia

CIRCULAR SB/ 436 /2003

La Paz, 4 DE JULIO DE 2003

DOCUMENTO: 584

Asunto: SOFTWARE / HARDWARE - DESARROLLO / MANTI

TRAMITE: 115815 - SF REQUISITOS MINIMOS SEGURIDAD INFORMA

Señores

Presente

**REF: REQUISITOS MÍNIMOS DE SEGURIDAD
INFORMÁTICA PARA LA ADMINISTRACIÓN DE
SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS
RELACIONADAS.**

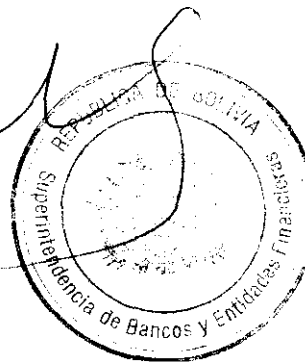
Señores:

Para su aplicación y estricto cumplimiento se adjunta a la presente copia fotostática de la Resolución, que aprueba y pone en vigencia la regulación prudencial referida a los Requisitos mínimos de seguridad informática para la administración de sistemas de información y tecnologías relacionadas en entidades financieras, la que será incorporada en el Título X, Capítulo XII de la Recopilación de Normas para Bancos y Entidades Financieras.

Asimismo, se comunica que la citada regulación se encuentra en la Recopilación de Normas disponible en la página www.supernet.bo.

Atentamente,

Fernando Calvo Unzueta
Superintendente de Bancos
y Entidades Financieras



Adj. Lo citado
YDR/VSM



RESOLUCION SB N° 066 /2003
La Paz, 04 JUL. 2003

VISTOS:

El proyecto de regulación prudencial referida a los **REQUISITOS MINIMOS DE SEGURIDAD INFORMATICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS EN ENTIDADES FINANCIERAS**, los informes IEN/D-48479 y D-48480 de 15 de octubre de 2002, emitidos por la Intendencia de Estudios y Normas y demás documentación que ver convino y se tuvo presente.

CONSIDERANDO:

Que, la Ley de Bancos y Entidades Financieras en su Art. 154 nurnerales 3, 7 y 8, modificada por la Ley N° 2297 de 20 de diciembre de 2001, dispone que la Superintendencia de Bancos y Entidades Financieras es la encargada de ejercer y supervisar el control interno y externo, exigiendo el cumplimiento de las disposiciones legales, normas tecnicas y reglarnentarias a todas las entidades publicas, privadas y mixtas que realicen intermediacion financiera en el país, debiendo elaborar y aprobar los reglarnentos de las normas de control y supervision sobre las actividades de intermediacion financiera y establecer sistemas preventivos de control y vigilancia.

Que, la promulgación de la Ley N° 2297 que incorpora modificaciones a la Ley de Bancos y Entidades Financieras, Ley No. 1488 de 14 de abril de 1993, otorga validez a las operaciones citadas en el Art. 3 de la mencionada ley cuando estas se realizan a traves de medios electronicos y reconoce que las mismas, asi como la informacion contenida y transmitida como rnensajes electronicos de datos, producen los mismos efectos legales, judiciales y de validez probatoria que un documento escrito con firma autografa, criterio coincidente con el recogido en el Art. 93 de la misma Ley 1488, habiendose encargado a la Superintendencia de Bancos y Entidades Financieras emitir disposiciones de seguridad para las operaciones y transmisiones electronicas efectuadas por las entidades de intermediacion financiera.

Que, es necesario introducir en las entidades de interrnediacion financiera y las empresas de servicios auxiliares financieros una cultura de seguridad informática en las transacciones y operaciones que realizan, por lo que es necesario contar con regulaciones prudenciales que establezcan los requisitos mínimos que las entidades de interrnediacion financiera y las empresas de servicios auxiliares financieros deben observar para adrninistrar los sistemas de informacion y la tecnologia que los soporta, los que van a ser utilizados en las operaciones de intermediacion financiera, transferencia electrónica de datos, transacciones electronicas de fondos, banca



Superintendencia de Bancos y Entidades Financieras Bolivia

electrónica y cajeros automáticos, con el proposito de minimizar el riesgo tecnologico.

Que, el documento elaborado se encuentra dividido en secciones para su mejor comprension. las que se refieren al Marco General, Requisitos minimos de seguridad informatica, Politicas, normas y procedimientos de seguridad informatica, Contrato con proveedores de tecnologias de la informacion y, Transferencias y transacciones electronicas, en las que se encuentran entre otras, disposiciones referidas a terminos que se van a utilizar en el documento a efectos de uniformizar su utilización en el sistema, se señala y definen **los** criterios basicos de informacion, la permision a las entidades de intermediacion financiera y a las empresas de servicios auxiliares financieros para suscribir contratos con proveedores de tecnologias de informacion, asi como con **los** clientes, señalando **los** aspectos que deben contener como minimo.

Que el funcionamiento adecuado de las diferentes areas de las entidades de intermediación financiera y empresas de servicios auxiliares financieros, es determinante en su estabilidad, porque garantiza eficiencia y efectividad en sus operaciones, otorga confiabilidad a la informacion que se genera y en el cumplimiento de las leyes y disposiciones vigentes, por lo que se les exige contar con un ambiente seguro y adecuado que garantice la continuidad operativa del negocio.

Que. efectuada la evaluación legal del proyecto por la Intendencia de Estudios y Normas, mediante informe IAJ/48480 de 15 de octubre de 2002, se concluye porque no existen observaciones legales al mismo al no contradecir disposiciones en vigencia y que por el contrario, constituye un instrumento que va a permitir a las entidades de intermediación financiera y a las empresas de servicios auxiliares financieros, adoptar acciones rápidas y eficientes para enfrentar, analizar, administrar y controlar **los** riesgos tecnológicos en la transmision de informacion y transferencia de fondos, en su **caso**, cuando las realicen a traves de medios electronicos,

Que, la Ley N° 2427 de 28 de noviembre de 2002, Ley del Bonosol, que crea la Superintendencia General del Sistema de Regulación Financiera (SIREFI), reconoce en el Art. 26 paragrafo II, las atribuciones de la Superintendencia de Bancos y Entidades Financieras establecidas en el Ley 1488, disposición que ha sido recogida en el Decreto Supremo N° 27026 de 6 de mayo de 2003, que establece que la Superintendencia de Bancos y Entidades Financieras tiene competencia privativa e indelegable para emitir regulaciones prudenciales relacionadas con las entidades de intermediacion financiera y servicios auxiliares financieros, correspondiendo, en consecuencia, cumplir con el mandato de la Ley de Bancos y Entidades Financieras

POR TANTO:

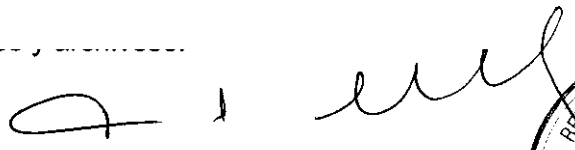
El Superintendente de Bancos y Entidades Financieras, con la facultad que le confiere la Ley N° 1488 de 14 de abril de 1993, y demas disposiciones complementarias:

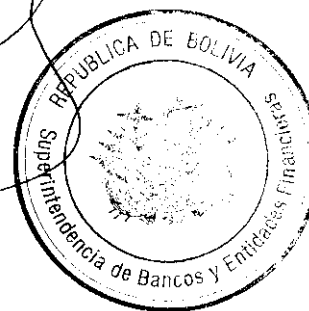


**Superintendencia de Bancos
y Entidades Financieras
Bolivia**

RESUELVE:

Aprobar y poner en vigencia la norma técnica que contiene los **"REQUISITOS MINIMOS DE SEGURIDAD INFORMATICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS EN ENTIDADES FINANCIERAS"**, en sus 5 Secciones, para su aplicación y estricto cumplimiento por parte de las entidades de intermediación financiera y empresas de servicios auxiliares financieros, conforme al texto que en anexo forma parte de la presente Resolución.


Fernando Calvo Unzueta
Superintendente de Bancos
y Entidades Financieras



YDR/SQB

RECOMPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

**CAPÍTULO XII: REQUISITOS MÍNIMOS DE SEGURIDAD
INFORMÁTICA PARA LA ADMINISTRACIÓN
DE SISTEMAS DE INFORMACIÓN Y
TECNOLOGÍAS RELACIONADAS****SECCIÓN 1: MARCO GENERAL**

Artículo 1° - Antecedentes Generales.- El crecimiento vertiginoso en los últimos años en Tecnologías de la Información y Telecomunicaciones, está cambiando la forma de hacer negocios en un mundo cada vez más globalizado y virtual.

Es por tanto que, las leyes, normativas, las políticas de estado, la regulación prudencial, las estrategias de las entidades financieras y de las compañías, deben adecuarse a estos tiempos modernos, donde la llamada Economía Digital (*E-Business, E-Commerce, E-Government*) crece en cifras exponenciales y nos trae a un tema de educación, cultura, resistencia al cambio que hay que administrar, para estar insertos en forma eficiente, confiable y segura en este mercado virtual.

En consecuencia con lo anterior, las entidades financieras y las empresas que prestan servicios auxiliares financieros, están viviendo este cambio y deben tomar acciones rápidas y eficientes para enfrentar, analizar, administrar y controlar los riesgos tecnológicos relacionados con las transferencias de información y transacciones de fondos realizadas por medios electrónicos, para lo cual las políticas, normas y procedimientos de seguridad informática y planes de contingencias tecnológicos deben brindar un ambiente seguro y adecuado que garantice la continuidad operativa del negocio y su permanencia en el tiempo.

Artículo 2° - Objeto.- El presente capítulo tiene por objeto establecer los requisitos mínimos que las entidades financieras y las empresas de servicios auxiliares financieros supervisadas por la Superintendencia de Bancos y Entidades Financieras (SBEF) deben cumplir para administrar los sistemas de información y la tecnología que los soporta, y que son utilizados en las operaciones de intermediación financiera, transferencia electrónica de datos, transacciones electrónicas de fondos, banca electrónica y cajeros automáticos con el propósito de minimizar el riesgo tecnológico, siendo estos requisitos mínimos de carácter enunciativo y no limitativo.

Artículo 3° - Ámbito de aplicación.- Se encuentran sujetos al ámbito de aplicación de la presente regulación prudencial, todas las entidades que realizan intermediación financiera y de servicios auxiliares financieros al amparo de lo dispuesto por la [Ley N° 1488](#) de 14 de abril de 1993, y modificada por la [Ley N° 2297](#) de 20 de diciembre de 2001, cuyo funcionamiento está autorizado por la [SBEF](#), y que realicen cualquier transferencia de información o transacción de fondos por medios electrónicos.

Artículo 4° - Definiciones.- Para efectos de la presente regulación prudencial, se usarán las

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

siguientes definiciones, siendo las mismas de carácter enunciativo y no limitativo:

- **Usuario:** Una persona, que utiliza uno o más sistemas informáticos, para lo cual debe estar identificado, autenticado y autorizado, previo a ser validado como usuario ya sea funcionario de la entidad (Interno) o cliente (Externo).
- **Medios de acceso a la información:** Son servidores de aplicación, computadores personales o de datos, terminales tipo cajero automático, las redes de comunicación, Internet, acceso telefónico o equipos inalámbricos.
- **Password:** Se denomina "password" o clave de acceso ó *PIN*, al conjunto de caracteres que una persona debe registrar para ser "reconocida" como usuario autorizado, y acceder a los recursos de un equipo computacional o red.
- **Electrónico:** Característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares.
- **Documento Electrónico:** Toda representación de un hecho, imagen o idea, que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
- **Firma Electrónica ó Firma Digital:** Cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un medio electrónico identificar formalmente a su autor.
- **Transferencia Electrónica de Información:** Es la forma de enviar, recibir o transferir en forma electrónica, datos, información, archivos, mensajes, entre otros.
- **Transacción Electrónica de Fondos:** Se entiende por todas aquellas operaciones realizadas por medios electrónicos que originen cargos o abonos de dinero en cuentas, tales como: traspasos automatizados de fondos efectuados por un cliente de una cuenta corriente a otra; órdenes de pago para abonar cuentas de terceros (proveedores, accionistas, etc.); utilización de tarjetas de débito en puntos de venta; recaudaciones mediante cargos a cuentas corrientes (servicios, impuestos, etc.); giros de dinero mediante Internet, cajeros automáticos, entre otros. En general, comprenden las descritas y cualquier otra operación que se efectúe por aquellos medios, en que un usuario habilitado para ello instruye o ejecuta movimientos de dinero en una o más cuentas.
- **Banca Electrónica o E-Banking:** Se refiere a las actividades de intermediación financiera realizadas por las entidades financieras autorizadas, que usan como medio de comunicación con sus clientes, las telecomunicaciones e Internet.
- **Plan de Contingencias Tecnológicas:** Conjunto de procedimientos alternativos, que

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

deberán entrar en funcionamiento al ocurrir una contingencia tal, que no permita a los servidores, procesos críticos y enlaces de comunicaciones, dar los servicios en forma normal y continua.

- **Plan Informático o de Tecnologías de Información y Comunicaciones:** Se refiere a la formalización de un plan anual, que incluye todos los proyectos tecnológicos, con sus respectivos recursos de *hardware*, *software*, telecomunicaciones y humanos, junto al presupuesto de inversiones y de gastos para la gestión integral.
- **Sitio de Respaldo o Site de Respaldo:** Es un lugar alternativo donde se instalan los equipos computacionales, tales como servidores, equipos de comunicaciones, impresoras, estaciones de trabajo, teléfonos, y espacio físico para usuarios críticos, etc., que se utilizarán en caso de una contingencia grave. Este sitio secundario o alternativo, contará con sus propios enlaces de comunicaciones, fuentes de energía, accesos seguros y ubicación geográfica distinta al sitio primario.
- **Servidor o Computador de Respaldo:** Un equipo con las mismas características técnicas que la máquina de producción normal que se usará en caso de falla de la máquina titular. Deberá permanecer actualizada en cuanto a sistema operativo y *software* de aplicación.
- **Respaldo para Contingencias:** Es un archivo magnético (Cinta, Disco ó CD) que contiene los archivos necesarios y suficientes, para recuperar un servidor, el mismo normalmente contiene el sistema operativo, motor y administrador de base de datos, compiladores, programas fuentes y objetos, cuentas de usuarios y archivos con datos críticos.
- **Respaldo ó Back-up:** Copia de datos e información almacenada en un medio magnético (Disco, CD, o cinta), se genera en forma rutinaria; con el propósito de utilizar dicha información o datos, en casos de emergencia o contingencia.
- **Registro de pistas de auditoria:** Registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoria.
- **Encriptación:** Proceso mediante el cual la información o archivos es alterada, en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarla al verla o copiarla, para ello se utiliza una clave en el origen y en el destino.
- **Procesos Críticos:** Referidos a procesos o sistemas que al dejar de funcionar, afectan la continuidad operativa del negocio.
- **Internet:** Red de redes de alcance mundial que opera bajo ciertos estándares y protocolos internacionales.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- **Intranet:** Similar al Internet, con la diferencia que los participantes se circunscriben a los límites de una red interna.
- **Página Web o Sitio Web:** Forma de presentar la información, cuando se está utilizando los sistemas de *Internet* o *Intranet*.
- **Sitio WAP:** Es un sitio en Internet accesado por equipos inalámbricos.
- **Hospedaje o Hosting:** Empresa que da el servicio de tener en un servidor el sitio WEB del cliente, con elementos de seguridad física y lógica.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS**SECCIÓN 2: REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA**

Artículo 1° - Responsable de la Seguridad Informática.- El Directorio u Órgano Equivalente, aprobará para uso obligatorio de la entidad financiera y de prestación de servicios auxiliares financieros, la Estrategia, Políticas y Normas de Seguridad Informática, considerando como mínimo las disposiciones establecidas en el presente capítulo. Es responsabilidad del Directorio u Órgano Equivalente, Gerencia General, y demás administradores responsables, tener formalizados por escrito, actualizados e implementados las políticas, normas y procedimientos, a ser aplicados en la administración y control de los sistemas de información y su tecnología que la soporta. La estrategia, las políticas, normas y procedimientos podrán ser solicitadas para su revisión, cuando la [SBEF](#) así lo requiera.

Artículo 2° - Características y criterios de la información.- Los datos que administren las entidades financieras y las empresas de servicios auxiliares financieros deben contener un alto grado de seguridad para cumplir con los objetivos de control y criterios básicos de información definidas por la [SBEF](#). Los criterios básicos se describen a continuación:

- **Confiabilidad:** Proveer información apropiada y confiable para el uso de las entidades financieras y empresas de servicios auxiliares financieros tanto interna como externamente.
- **Confidencialidad:** Protección de información sensible para que no se divulgue sin autorización.
- **Integridad:** Se refiere a la exactitud y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas de la actividad de la entidad financiera.
- **Disponibilidad:** Oportunidad de la información, cuando sea requerida.
- **Efectividad:** Adecuada información para desarrollar las actividades de las entidades financieras y empresas de servicios auxiliares financieros.
- **Eficiencia:** Proveer información suficiente a través del uso de los recursos de la mejor manera posible.
- **Cumplimiento:** Debida atención a las leyes, regulaciones y acuerdos contractuales que la entidad financiera y empresas de servicios auxiliares financieros deben realizar.

Artículo 3° - Políticas, normas y procedimientos.- El área de Tecnologías de la Información de la entidad financiera o empresa de servicios auxiliares financieros, para asegurar la continuidad operativa de esta, deberá tener formalizado por escrito, implementadas y actualizadas, las políticas, normas y procedimientos de seguridad informática para las áreas

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

fundamentales de la función informática, a saber:

- a) **Gestión:** Dirección, planificación, control y supervisión.
- b) **Operación:** Procesos y tareas propias del área informática.
- c) **Administración de usuarios.**
- a) **Gestión:** La gestión o administración directiva, deberá contener a lo menos, las políticas, normas y procedimientos respecto a:
 - i. Plan informático.
 - ii. Comité de informática.
 - iii. Comité operativo del área.
 - iv. Desarrollo y mantenimiento de sistemas.
 - v. Administración de contratos externos.
- b) **Operaciones:** El área de operaciones deberá contener a lo menos, las políticas, normas y procedimientos de:
 - i. Seguridad física de sala de servidores y el entorno que la rodea.
 - ii. Respaldos y recuperación de información.
 - iii. Registro de caídas de los sistemas o no disponibilidad de servicios que afecten la atención normal al público.
 - iv. Administración de cintoteca interna y externa.
 - v. Control y políticas de administración de antivirus.
 - vi. Administración de licencias de software y programas.
 - vii. Traspaso de aplicaciones al ambiente de explotación.
 - viii. Inventario de hardware y software.
 - ix. Seguridad de redes.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- Características, topología y diagrama de la red
 - Seguridad física de sites de comunicaciones
 - Seguridad y respaldo de enlaces.
 - Equipos de seguridad y telecomunicaciones.
 - Seguridad de acceso *Internet/Intranet*.
- c) **Administración de Usuarios:** El área de administración de usuarios deberá contener a lo menos, las políticas, normas y procedimientos para:
- i. Administración de privilegios de acceso a sistemas.
 - ii. Administración y rotación de *password*.
 - iii. Asignación y responsabilidad de *hardware* y *software*.
 - iv. Administración de estación de trabajo ó *PC*.
 - v. Uso de comunicaciones electrónicas.
 - vi. Administración y control de usuarios *Intranet/Internet*.

Artículo 4° - Plan de Contingencias Tecnológicas.- Las entidades financieras y las empresas de servicios auxiliares financieros deberán tener formalizado por escrito, actualizado, implementado y aprobado por el Directorio u Órgano Equivalente, un Plan de Contingencias Tecnológicas. El plan debe incluir al menos:

- Objetivo del plan de contingencias tecnológicas.
- Metodología del plan de contingencias tecnológicas.
- Procedimientos de recuperación de operaciones críticas.
- Descripción de responsabilidades e identificación de personal clave.
- Medidas de prevención.
- Recursos mínimos necesarios para la recuperación.
- Convenios realizados para la recuperación.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Artículo 5° - Pruebas del Plan de Contingencias Tecnológicas.- Las entidades financieras y empresas de servicios auxiliares financieros, deberán efectuar a lo menos 2 pruebas al año del Plan de Contingencias Tecnológicas de acuerdo al cronograma que la entidad financiera presente a la [SBEF](#) una vez que el Plan esté implementado formalmente. En estas pruebas debe participar el auditor interno. El resultado de éstas deberá estar disponible para las inspecciones efectuadas por la [SBEF](#).

De acuerdo al grado de complejidad en las operaciones y uso de las Tecnologías de Información en cada entidad financiera o empresa de servicios auxiliares financieros, la [SBEF](#) requerirá un cumplimiento, desarrollo y especificación mayor en cada uno de los puntos descritos en esta Sección.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS**SECCIÓN 3: CONTRATO CON PROVEEDORES DE TECNOLOGÍAS DE LA INFORMACIÓN**

Todos los contratos con proveedores externos son importantes, deben encontrarse formalizados de manera que permitan a las entidades financieras y empresas de servicios auxiliares financieros operar en todas sus áreas de negocio, así como en procesos del tipo Banca Electrónica ó *Internet* (hospedaje del sitio *WEB* o *WAP*) y otros como mantenimiento de equipos, soporte de sistemas operativos, externalización de especialistas informáticos, aseo y limpieza.

Artículo 1° - Contratación de Proveedores Externos de Tecnologías.- Las entidades financieras y empresas de servicios auxiliares financieros al contratar los servicios de proveedores externos de tecnologías de:

1. Procesamiento de datos o ejecución de sistemas en lugar externo. Para la contratación de empresas encargadas del procesamiento de datos o ejecución de sistemas en lugar externo, la entidad financiera o empresa de servicios auxiliares financieros debe considerar al menos los siguientes aspectos:

1.1. Que es deber del Directorio u Órgano Equivalente, Gerencia General, y demás administradores responsables de la entidad de intermediación financiera o empresa de servicios auxiliares financieros solicitante, asegurarse que la empresa proveedora cuente con la necesaria solidez financiera, una organización y personal adecuados, con conocimiento y experiencia en el procesamiento de datos, servicios bancarios, telecomunicaciones, como asimismo de que sus sistemas de control interno y procedimientos de seguridad informática, respondan a las características del servicio que se desea contratar.

1.2. Que la infraestructura tecnológica y los sistemas que se utilizarán para la comunicación, almacenamiento y procesamiento de datos, ofrecen suficiente seguridad para resguardar permanentemente la continuidad operacional y la confidencialidad, integridad, exactitud y calidad de la información y los datos. Asimismo, verificar que las condiciones garantizan la obtención oportuna de cualquier dato o información que necesite, sea para sus propios fines o para cumplir con los requerimientos de las autoridades competentes, como es el caso de la información que en cualquier momento puede solicitarle la [SBEF](#).

1.3. Que es responsabilidad del Directorio u Órgano Equivalente y el Gerente General de la entidad financiera o empresa de servicios auxiliares financieros, la suscripción del contrato con la empresa proveedora, el que entre otras cosas deberá especificar:

- a.** La naturaleza y especificaciones del servicio de procesamiento contratado.
- b.** La responsabilidad que asume la empresa proveedora, para mantener políticas,

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

normas y procedimientos que garanticen la seguridad informática, el secreto bancario y la confidencialidad de la información, en conformidad con la legislación boliviana, asimismo, para prevenir pérdidas atrasos o deterioros de la misma.

- c. La responsabilidad que asume la empresa proveedora de tecnologías en caso de ser vulnerados sus sistemas, por atentados computacionales internos o externos.
- d. La facultad de la entidad financiera o de la empresa de servicios auxiliares financieros, para practicar evaluaciones periódicas en la empresa proveedora del servicio, directamente o mediante auditorías independientes.

2. Desarrollo y mantenimiento de programas, sistemas o aplicaciones. Para la contratación de empresas encargadas del desarrollo y mantenimiento de programas, sistemas o aplicaciones, la entidad financiera o empresa de servicios auxiliares financieros debe considerar al menos los siguientes aspectos:

- 2.1.** Que es deber de la entidad financiera o empresa de servicios auxiliares financieros, asegurarse que la empresa contratada cuente con la necesaria solidez financiera, organización y personal adecuado, con conocimiento y experiencia en el desarrollo de sistemas y/o en servicios de intermediación financiera, asimismo de que sus sistemas de control interno y procedimientos de seguridad informática, responden a las características del servicio que se desea contratar.
- 2.2.** Que la infraestructura tecnológica, sistemas operativos y las herramientas de desarrollo, referidos a licencias de software, que se utilizarán estén debidamente licenciados por el fabricante o representante de *software*.

Artículo 2° - Relación Contractual con el Proveedor Externo de Tecnologías.- El contrato con el proveedor externo de tecnologías deberá contener como mínimo las siguientes cláusulas:

- 1. Programas Fuente.-** Al término del proyecto se deberá entregar bs programas fuente al cliente.
- 2. Propiedad intelectual.-** Se debe aclarar a quien pertenecerá la propiedad intelectual en el caso de desarrollo de programas, sistemas o aplicaciones.
- 3. Plataforma de Desarrollo.-** Se deberá indicar en detalle la plataforma de desarrollo que utilizará el proveedor, servidor, sistemas operativos y las herramientas de desarrollo, tal como lenguaje de programación y motor de base de datos.
- 4. Formalización de Recursos Humanos.-** El proveedor deberá tener el contrato del

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

personal que participa en el proyecto, actualizado y con cláusulas de confidencialidad para el manejo de la información. Adicionalmente, deberá enviar al cliente (entidad financiera o empresa de servicios auxiliares financieros) el currículum de todos los participantes en el proyecto, indicando al menos antecedentes profesionales y personales.

5. **Cronograma y plan de trabajo.-** Se debe indicar los tiempos de desarrollo por cada etapa en forma detallada, incluyendo las pruebas de programas.
6. **Atrasos y Riesgos.-** Con la finalidad de proteger a la entidad financiera o empresa de servicios auxiliares financieros, junto a las cláusulas normales de condiciones de pago se deben establecer multas por atrasos en la entrega. Al mismo tiempo, indemnización por daños y perjuicios, en caso de fraudes o atentados cibernéticos.
7. **Acceso remoto.-** En caso de que el proveedor sea autorizado a ingresar en forma remota a los servidores del cliente, deberá registrarse y cumplir las normas, políticas y procedimientos de la entidad financiera o empresa de servicios auxiliares financieros en lo referido a la seguridad de información.

Artículo 3° - Seguridad Informática del Proveedor.- Adicionalmente, el proveedor deberá tener formalizados las políticas, normas y procedimientos de seguridad informática, tales como:

- Desarrollo de sistemas de información y programas.
- Mantenimiento de sistemas y programas.
- Seguridad física sala de servidores.
- Respaldos y recuperación de información.
- Respaldo y recuperación de bases de datos.
- Administración de cintoteca interna y externa.
- Control y políticas de administración de antivirus.
- Administración de licencias de software y programas.
- Traspaso de aplicaciones al ambiente de explotación (producción).
- Administración y control de equipos de seguridad.
- Plan de contingencias tecnológicas.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Será de responsabilidad de la entidad financiera o de la empresa de servicios auxiliares, verificar la seguridad informática del proveedor a través de una metodología que cumpla con este objetivo.

Asimismo, la entidad financiera o la empresa de servicios auxiliares deberá mantener los documentos y antecedentes de los contratos suscritos con empresas proveedoras de servicios de tecnología de información a disposición de la [SBEF](#).

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS**SECCIÓN 4: TRANSFERENCIAS Y TRANSACCIONES ELECTRÓNICAS****Artículo 1° - Requisitos de los sistemas de transferencia y transacción electrónica.-**

Para habilitar un sistema de transferencia electrónica de información o transacción electrónica de fondos del tipo Banca Electrónica, las entidades financieras o empresas de servicios auxiliares financieros, deben adquirir e implementar elementos de hardware y software necesarios para la protección y control de su plataforma tecnológica, adicionalmente y en forma complementaria, deberán considerar el cumplimiento de los siguientes requisitos mínimos:

- a) **Seguridad del Sistema**, el sistema debe proveer un perfil de seguridad que garantice que las operaciones, sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o confidencialidad de la información transmitida o procesada por ese medio.

Los procedimientos deberán asegurarse que tanto el originador como el destinatario, en su caso, conozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, debiendo utilizarse las políticas, normas y procedimientos indicados en la [Sección 2](#) y en el [Artículo 3° de la presente Sección](#), que permitan asegurar su autenticidad e integridad.

- b) **Canal de Comunicación**, la entidad financiera o empresa de servicios auxiliares financieros, debe mantener permanentemente abierto y disponible un canal de comunicación que permita al usuario realizar consultas y 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.
- c) **Difusión de Políticas de Seguridad**, la entidad financiera o empresa de servicios auxiliares financieros, deberá difundir sus políticas de seguridad, relativas al tema de transferencias electrónicas al interior de la entidad.
- d) **Certificación**, la existencia de las páginas *Web* utilizadas por las entidades financieras o empresas de servicios auxiliares financieros, deberá estar avalada por una certificadora internacional.
- e) **Continuidad Operativa**, se refiere a procesos alternativos que puedan asegurar la continuidad de todos los procesos definidos como críticos relacionados con los servicios de transferencia electrónica de fondos. Es decir, las instalaciones y configuraciones de los equipos, sistemas y de las redes deben garantizar la continuidad de las operaciones frente a eventos fortuitos o deliberados, debiendo considerarse lo previsto en la [Sección 2, Artículos 4° y 5°](#).
- f) **Disponibilidad de la Información (Informes)**, los sistemas de transacción electrónica de

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

fondos deberán generar la información necesaria para que el cliente 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.

- g) **Registro de pistas de control**, los sistemas utilizados, además de permitir el registro y seguimiento íntegro de las operaciones realizadas, deberán generar archivos que permitan respaldar los antecedentes de cada operación electrónica, necesarios para efectuar cualquier seguimiento, examen o certificación posterior, tales como, fechas y horas en que se realizaron, contenido de los mensajes, identificación de los operadores, emisores y receptores, cuentas y montos involucrados, terminales desde los cuales realizó sus operaciones.

Artículo 2° - Contrato formal.- Deberá celebrarse un contrato entre la entidad financiera o empresa de servicios auxiliares financieros, y el cliente o usuario, en el cual queden claramente establecidos los derechos y responsabilidades de cada una de las partes que intervienen en este tipo de operaciones electrónicas. Este contrato deberá contener de manera enunciativa y no limitativa, los siguientes puntos:

- a) El usuario o cliente, será responsable exclusivo del uso y confidencialidad del *Password*, Clave de acceso ó *PIN*, que utilizará en sus operaciones. Se indicará, el bloqueo automático de su clave después de tres intentos fallidos y el procedimiento para desbloqueo.
- b) Debe detallarse el tipo de operaciones que puede efectuar el cliente.
- c) Debe quedar establecido el horario y consideraciones de cierre diario de cada entidad financiera o empresa financiera de servicios auxiliares, junto al procedimiento alternativo en caso de no-disponibilidad del servicio.
- d) Hacer conocer al usuario o cliente las medidas de seguridad que ha tomado la entidad financiera o empresa de servicios auxiliares financieros para la transferencia electrónica de información y transacción electrónica de fondos.
- e) Los sistemas que permitan ejecutar transacciones de fondos, además de reconocer la validez de la operación que el usuario realice, deben controlar que los importes girados no superen el saldo disponible o el límite que se haya fijado para el efecto, salvo la existencia previa de contratos de anticipo o adelanto en cuenta, debiendo cumplir para tal efecto con las formalidades del [Código de Comercio](#) y reglamentación vigente.

Artículo 3° - Encriptación de mensajes y archivos.- Para que una entidad financiera o empresa de servicios auxiliares financieros, efectúe transferencias electrónicas de información y transacciones electrónicas de fondos, deberá tener implementado un software de encriptación que garantice como mínimo que las operaciones realizadas por sus usuarios internos o externos sean

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

realizadas en un ambiente seguro y no puedan ser observadas por usuarios no autorizados.

Artículo 4° - Transferencia como documento.- La generación de documentos electrónicos que constituyen documentación de carácter oficial, para el cumplimiento de disposiciones legales de la [SBEF](#) deberá cumplir con los requisitos mínimos descritos en el presente Capítulo.

Artículo 5° - Operaciones interbancarias.- Las transacciones electrónicas de fondos interbancarias estarán regidas por el reglamento del sistema de pagos de alto valor, del [Banco Central de Bolivia](#), mientras que, las transferencias electrónicas de información de estas operaciones estarán regidas por el Reglamento de Operaciones Interbancarias contenido en el [Título IX, Capítulo IV](#) de la Recopilación de Normas para Bancos y Entidades Financieras.

Artículo 6° - Sanciones.- Las entidades financieras y empresas de servicios auxiliares financieras, que están bajo el ámbito de aplicación de la presente norma y que incumplan con lo descrito en el [Artículo 2° de la Sección 2](#) y [Artículo 4° de la presente Sección](#), estarán sujetas al régimen de sanciones del [Título XIII, Capítulo I, Sección 1](#) de la Recopilación de Normas para Bancos y Entidades Financieras.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

SECCIÓN 5: DISPOSICIONES TRANSITORIAS

Artículo 1° - Adecuación y Cronograma.- Las entidades financieras y empresas de servicios auxiliares financieros, deberán cumplir con todos los requisitos mínimos que se requieren en este capítulo hasta el 31 de enero de 2004. Adicionalmente deberán enviar su cronograma para el cumplimiento y adecuación a la presente hasta el 31 de julio de 2003.