CIRCULAR
CNBS No.119/2005

SISTEMA FINANCIERO
Toda la República

Señores:

Nos permitimos transcribir a ustedes, la Resolución aprobada por la Comisión Nacional de Bancos y Seguros, que literalmente dice:

"RESOLUCIÓN No.1301/22-11-2005.- La Comisión Nacional de Bancos y Seguros,

CONSIDERANDO: Que de conformidad con las facultades legales concedidas a la Comisión Nacional de Bancos y Seguros, respecto a las instituciones del sistema financiero y demás instituciones supervisadas, ésta emitirá las normas prudenciales que deberán cumplir las mismas, basándose en la legislación vigente y en los acuerdos y prácticas internacionales.

CONSIDERANDO: Que conforme a lo establecido en el Artículo 50 de la Ley del Sistema Financiero, las instituciones del sistema financiero podrán ofrecer y prestar todos los productos y servicios los mencionados en el Artículo 46 de dicha Ley por medios electrónicos; así como que la Comisión emitirá normas de carácter general para regular las operaciones que efectúen y servicios que presten las instituciones por medios electrónicos.

CONSIDERANDO: Que conforme lo establecido en la Ley de la Comisión Nacional de Bancos y Seguros, ésta se encuentra sujeta a ciertos criterios, entre los cuales se señala el de promover la adopción de buenas prácticas en la administración de los riesgos inherentes a las actividades que realizan las instituciones supervisadas.

POR TANTO: Con fundamento en los artículos 1, 6, 13 y 14 de la Ley de la Comisión Nacional de Bancos y Seguros; y, 50 de la Ley del Sistema Financiero; en sesión del 22 de noviembre de 2005, resuelve:

1. Aprobar las siguientes:

NORMAS PARA REGULAR LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO

CAPÍTULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto

Las presentes normas, tienen por objeto regular la administración de las tecnologías de información y comunicaciones utilizadas por las instituciones del sistema financiero; asimismo, regular los servicios financieros y operaciones realizadas por medio de redes electrónicas de uso externo e interno.

La Junta Directiva o Consejo de Administración de las instituciones del sistema financiero, en adelante Junta o Consejo, deberán prestar la debida importancia a la administración del riesgo derivado de los sistemas de información, tomando en cuenta que su continuidad, desarrollo y funcionamiento constituyen el elemento central para su operatividad y su manejo administrativo y financiero.

ARTÍCULO 2.- Alcance

Las presentes normas están en concordancia con los principios del Comité de Basilea y el estándar internacional ISO/IEC 17799:2000, emitidos en materia de banca electrónica y administración de la Seguridad Informática y constituyen una guía general para la documentación formal e implementación de la seguridad en las tecnologías de información y comunicaciones de las instituciones del sistema financiero.

Estas disposiciones son de obligatorio cumplimiento para las demás instituciones supervisadas por la Comisión, en lo que les sea aplicable, en función de su tamaño y complejidad.

ARTÍCULO 3.- Definiciones

Para los efectos de aplicación de la presente normativa y bajo la perspectiva de la tecnología de información, deberán considerarse las siguientes definiciones:

1) **Ataques de Denegación de Servicio:** Envío de solicitudes a servidores o equipos de comunicación que provoquen saturación en sus memorias para que de esta forma dejen de funcionar temporalmente y no presten los servicios que tengan configurados.

2) **Ataques de Diccionario:** Prueba de combinaciones de todos los usuarios y contraseñas posibles basados en un diccionario en español, inglés o cualquier otro idioma, para ingresar de manera ilegal a un sistema informático.

3) **Ataques de Fuerza Bruta:** Prueba de combinaciones de todos los usuarios y contraseñas posibles basados en todos los caracteres posibles, para ingresar ilegalmente a un sistema informático.

4) **Banca Electrónica:** Servicios y operaciones proporcionados a clientes por medios electrónicos conectados al sistema de producción, utilizando tecnologías, como: telefonía, Internet, celulares, o una combinación entre redes de comunicaciones.

5) **Canal de Comunicación:** Métodos tecnológicos para la comunicación entre los usuarios de banca electrónica y las instituciones del sistema financiero entre otros Internet, Telefonía, etc.

6) **La Comisión o CNBS:** Comisión Nacional de Bancos y Seguros.

7) **Contraseña Segura o Fuerte:** Contraseñas de uso informático que deben cumplir con las especificaciones de la política de contraseñas de la institución y que sean difíciles o casi imposibles de adivinar o hurtar.

8) **Discontinuidad de Servicio Significativo:** Incapacidad de continuar prestando los servicios definidos como críticos por la Alta Gerencia, y sin los cuales se vería seriamente afectada la continuidad en el mercado.

9) **Hash:** Cadena de caracteres generada por un algoritmo de encriptación, el cual proporciona un valor estadísticamente único para un conjunto de datos de entrada. Bajo esta técnica se comprobará la validez de los datos recibidos o, como en el caso de las contraseñas, cifrar una información en un sólo sentido.

10) **Localizador Uniforme de Recursos (URL):** Cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos en Internet.

11) **Memoria Caché:** Memoria a la que una computadora puede acceder más rápidamente que a la memoria normal de la computadora (Memoria RAM), la computadora primero busca información en la memoria caché y luego en la RAM.

12) **No Repudio:** Cualidad o característica de una determinada comunicación, a través de la cual se protege a las partes de la comunicación frente a la negación de que dicha comunicación haya ocurrido. Existe no repudio cuando se produce el efecto legal o práctico de dicho atributo o característica.

13) **Pared de Fuego (Firewall):** Dispositivos de Seguridad (Hardware o software) utilizados para restringir el acceso en un ambiente de redes informáticas interconectadas, que permiten el acceso a ciertos servicios previamente definidos.

14) **Penetración Significativa:** Ataques a una red informática que alteren la disponibilidad, integridad y confidencialidad de la información sensitiva de la institución.

15) **Procedimientos Almacenados (Stored Procedure):** Conjunto de instrucciones u órdenes precompiladas, escritas en un lenguaje propietario como PL/SQL para Oracle database o PL/PgSQL para PostgreSQL, que pueden ser llamados usando el nombre que se les haya asignado. Son esencialmente cajas negras.

16) **Red de Producción:** Red que está compuesta por computadoras, servidores, archivos, bases de datos, equipos de comunicación, dispositivos de seguridad, etc., que contienen y transmiten datos reales y oficiales de una institución.

17) **Servidor:** Computadora que presta servicios de red a los usuarios de la misma. Estos servicios pueden ser bases de datos, impresión, antivirus, correo electrónico, aplicaciones, etc.

18) **Sesión:** Es el periodo de tiempo transcurrido desde que un usuario o un equipo informático inicia conexión, con otro equipo previa presentación de credenciales, hasta el momento que la conexión finaliza.

19) **Sistema de Detección de Intrusos (IDS):** Dispositivo o programa de cómputo que de acuerdo a una base de datos, detecta patrones que son conocidos mundialmente como ataques o intentos de intrusión a redes y computadoras, enviando alertas y presentando reportes.

20) **Tecnologías de Información y Comunicaciones (TIC):** Recursos tecnológicos usados para crear, almacenar, intercambiar y usar información en sus diferentes formatos (datos, voz, imágenes, videos, presentaciones, etc.)

21) **Tercerización (Outsourcing):** Contrato mediante el cual una compañía provee servicios a otra. Estos servicios podrían ser provistos dentro de la misma institución.

22) **Tercerización Significativa:** Tercerización de servicios que son de carácter vital para una compañía, ya que si estos servicios fallan provocarían un impacto en la continuidad del negocio.

23) **Valor SALT:** Valor generado al azar, que es usado para modificar el hash de una contraseña, el cual previene las colisiones de contraseñas, es decir si más de un usuario selecciona la misma contraseña, la cadena de caracteres generada utilizando un valor SALT será diferente.

CAPITULO II

SUPERVISIÓN Y ADMINISTRACIÓN

SECCIÓN I

DE LA ADMINISTRACIÓN

ARTÍCULO 4.- Políticas de Administración

La Junta o Consejo deberá tener como mínimo una reunión anual para establecer o revisar las políticas y procedimientos sobre la administración tecnológica y seguridad de la información, que conlleven a la correcta toma de decisiones. Asimismo, deberá conocer y discutir, por lo menos cuatro (4) veces al año, los informes que sobre este particular le presente la Gerencia General. Lo tratado en dichas reuniones, deberá quedar registrado en el libro de actas correspondiente.

ARTÍCULO 5.- Políticas de las Tecnologías de Información y Comunicaciones

Las políticas mencionadas en el Artículo anterior deberán incluir al menos temas como:

a) Seguridad de la información incluyendo:

- Uso de Internet;
- Uso del Correo Electrónico;
- Uso de las estaciones de Trabajo;
- Proceso Antivirus;
- Adquisición de Hardware y Software;
- Seguridad de Contraseñas;
- Seguridad de la Información Sensitiva;
- Seguridad de Servidores;
- Seguridad de equipos de comunicación;
- Seguridad en redes inalámbricas (Si existen);
- Seguridad en Redes con Terceros;
- Acceso y Configuración remotos;
- Administración de respaldos; y,
- Administración de dispositivos móviles de almacenamiento magnético.

b) Procesos de respaldo y recuperación en caso de un desastre y situaciones de mal funcionamiento de uno o varios componentes del sistema de información;

c) Tercerización (outsourcing);

d) Mantenimiento y desarrollo de sistemas; y,

e) Documentación de todos los procesos que se desarrollan en el área de TIC.

ARTÍCULO 6.- Nombramiento de Ejecutivo Especializado

La Gerencia General deberá nombrar un ejecutivo especializado, responsable de todos los asuntos relacionados con las tecnologías de la información. Este ejecutivo deberá tener al menos formación profesional sobre la administración de las tecnologías de información en materia de comunicaciones, sistemas operativos, desarrollo de software, base de datos, entre otros y deberá tener experiencia comprobada en el campo de la informática.

ARTÍCULO 7.- Unidad Responsable

Dentro de la estructura organizacional, la unidad responsable de administrar los aspectos tecnológicos y de seguridad de la información deberá contar con el manual de puestos para el personal de TIC, que deberá incluir los perfiles de puestos y la segregación de funciones y de autoridad.

Asimismo, la unidad responsable deberá estructurar un programa de capacitación de acuerdo con las prioridades de la administración, que permita maximizar las contribuciones que brinde el personal del área de TIC. Esta capacitación deberá incluirse en el presupuesto anual y ser consistente con los requerimientos mínimos de la organización.

Para la consecución de los objetivos planteados, la institución supervisada deberá procurar que la unidad antes mencionada se encuentre en un nivel razonable

de independencia funcional dentro de la estructura organizacional.

ARTÍCULO 8.- Establecimiento de Políticas y Estrategias

La Gerencia General deberá definir y proponer a la Junta o Consejo, los procesos críticos para los cuales es necesario establecer las políticas y estrategias de tal forma que se asegure la integridad y continuidad de las operaciones. Asimismo, las medidas y mecanismos para la difusión óptima de dichas políticas.

El Administrador de Seguridad Informática deberá proponer a la Gerencia General las políticas y estrategias correspondientes.

Los eventos calificados deberán ser comunicados a la Gerencia General, al Administrador de Seguridad Informática y las dependencias involucradas, para su respectivo análisis y tomar las medidas correctivas necesarias.

SECCIÓN II

PROCEDIMIENTOS

ARTÍCULO 9.- Procedimientos Formales

La institución deberá desarrollar, implementar, actualizar y documentar procedimientos formales en relación a la planeación, organización, adquisición, implementación, entrega de servicios por medios tecnológicos, soporte y monitoreo; y deberá ser diligente en su ejecución y divulgación.

SECCIÓN III

HISTORIAL Y MONITOREO

ARTÍCULO 10.- Mantenimiento de Registros

La institución deberá mantener registros de las auditorías a los sistemas automatizados, basados en un análisis de riesgos, en bitácoras automatizadas registrando los accesos, transacciones y consultas realizadas tanto a los sistemas de información como a los dispositivos de comunicaciones y seguridad. Estos registros deberán como mínimo identificar la persona, lugar, tiempo y las acciones relacionadas con el aplicativo utilizado.

ARTÍCULO 11.- Período de Resguardo

La institución deberá resguardar los registros previstos en el Artículo anterior. El periodo de resguardo será de 5 años para las transacciones y 6 meses para la consulta.

ARTÍCULO 12.- Mantenimiento de Bitácoras

La institución, si así lo determina, podrá mantener informados a sus clientes y empleados de la existencia del mantenimiento de bitácoras que registrarán todas las actividades con los sistemas de información de la institución.

Con respecto a las disposiciones del Artículo 8, el sistema de administración de registros deberá crear las alertas correspondientes para las autoridades internas y externas, especialmente en los casos de actividades externas no autorizadas y también aquellas actividades excepcionales realizadas por los diferentes tipos de usuarios.

SECCIÓN IV

AUDITORÍA INTERNA

ARTÍCULO 13.- Auditoría de Sistemas

La Auditoría Interna de la institución deberá auditar la Tecnología de Información y Comunicación (TIC) a fin de verificar la integridad, disponibilidad y confidencialidad de la información. La persona(s) encargada(s) de auditar las TIC deberá contar con experiencia y entrenamiento calificado para llevar a cabo este tipo de auditorías basadas en las mejores prácticas existentes en el mercado tales como COBIT e ISO-17799.

La institución deberá proveerle a la Auditoría Interna las herramientas necesarias para la realización y control del ambiente de la TIC.

ARTÍCULO 14.- Responsabilidad del Auditor Interno

El Auditor Interno será responsable de que, aun en el caso de que la Auditoría de Sistemas sea llevada a cabo por medio de la Tercerización (outsourcing) se cumplan las disposiciones contenidas en las Normas Mínimas para el Funcionamiento de las Unidades de Auditoría Interna de las Instituciones del Sistema Financiero y en las presentes normas.

SECCIÓN V

ADMINISTRACIÓN DE RIESGOS

ARTÍCULO 15.- Factores de Riesgo

La institución deberá realizar sus auditorías de sistemas basadas en un análisis de riesgos y cumpliendo las normativas existentes. Esta auditoría

deberá incluir todos los riesgos potenciales en la administración de las Tecnologías de Información y Comunicaciones, incluyendo al menos los factores siguientes:

- Los usuarios externos e internos del sistema de información;
- El ambiente del sistema, la operatividad del sistema y sus implicaciones sobre el negocio;
- Los niveles de acceso y la sensibilidad de la información;
- La calidad de la información;
- La Tercerización (outsourcing);y,
- Planes de contingencia y recuperación ante desastres.

ARTÍCULO 16.- Proceso de Auditoría Basada en Riesgos

El proceso de auditoría basada en riesgos deberá ser permanente y se revisará de acuerdo a los cambios en los factores de riesgos.

La institución deberá, conforme a la administración y análisis de riesgos, tomar las medidas necesarias para minimizar los impactos negativos en toda su infraestructura de Tecnologías de Información y Comunicaciones.

SECCIÓN VI

SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 17.- Administrador de Seguridad Informática

La Junta o Consejo deberá nombrar a un Administrador de Seguridad Informática, el cual deberá estar subordinado a la Gerencia General de la institución.

Las funciones de este Administrador de Seguridad Informática serán definidas evitando conflictos de interés, por tanto deberá ser independiente del ejecutivo especializado responsable de la administración de las Tecnologías de Información y Comunicaciones.

ARTÍCULO 18.- Perfil de Responsabilidades

La Gerencia General de la institución deberá definir las funciones y las responsabilidades del Administrador de Seguridad Informática. Dichas funciones y responsabilidades comprenderán como mínimo las siguientes:

- Proponer a la institución las políticas, normas y procedimientos de seguridad informática;
- Documentar e implementar las políticas, normas y procedimientos de seguridad informática aprobadas por la Junta o Consejo;
- Verificar que los usuarios de los distintos sistemas y recursos tecnológicos cumplan con las políticas, normas y procedimientos aprobados;
- Tomar las acciones correctivas que garanticen la seguridad informática requerida, una vez que se hayan identificado violaciones;
- Identificar e implementar herramientas de seguridad informática que aseguren que la información y el equipamiento, no sean utilizados en perjuicio de la institución y los usuarios;
- Controlar el uso indebido de programas (utilitarios) o herramientas que permiten la manipulación de los datos en los diferentes sistemas; y,
- Desarrollar por lo menos una vez al año, evaluaciones de seguridad a las tecnologías de información y comunicaciones de la institución.

La institución deberá proveer al Administrador de Seguridad Informática los recursos necesarios y capacitación continua para que cumpla sus funciones.

ARTÍCULO 19.- Separación de Ambientes

La institución deberá procurar separar físicamente y lógicamente los ambientes de producción, desarrollo y pruebas.

CAPÍTULO III

INVESTIGACIÓN DE SEGURIDAD

SECCIÓN ÚNICA

ARTÍCULO 20.- Evaluaciones de Seguridad

Las evaluaciones de seguridad deberán medir la eficiencia de los medios de protección e incluir

propuestas para corregir las vulnerabilidades. Sus resultados deberán presentarse a la Gerencia General en un reporte detallado con recomendaciones, que incluya un sumario ejecutivo con los principales hallazgos.

ARTÍCULO 21.- Implementación de Cambios

Previo a la implantación de cambios en: el ambiente de producción; los sistemas de alto riesgo definidos por la administración; y los servicios financieros por medios electrónicos, deberá realizarse una evaluación de seguridad. Asimismo, cuando ocurran cambios significativos en el ambiente tecnológico en que operan los sistemas de información, o se implementen nuevos sistemas.

ARTÍCULO 22.- Otras Pruebas de Seguridad

Para evitar conflictos de interés y poder tomar las medidas cautelares correspondientes, las instituciones podrán realizar otras pruebas por entes o profesionales externos.

ARTÍCULO 23.- Informe de Seguridad

La Gerencia General, para minimizar los riesgos, deberá implementar las recomendaciones contenidas en el informe de seguridad, y establecer un cronograma de actividades a realizar.

CAPÍTULO IV

CONTROL DE ACCESO, ENCRIPTACIÓN Y SEGURIDAD EN LA RED

SECCIÓN I

CONTROL DE ACCESO

ARTÍCULO 24.- Identificación de Acceso

La institución deberá asignar una identificación única y personal de cualquier usuario con acceso al sistema de información, como una condición previa a la autorización de acceso.

ARTÍCULO 25.- Reglas y Procedimientos para Acceso

La institución deberá determinar las reglas y el procedimiento para dicha identificación, así como para el otorgamiento de autorizaciones a terceros que accedan a los componentes de la tecnología de información. Estas reglas deberán tomar en cuenta los riesgos derivados de las responsabilidades y autorizaciones dadas a los usuarios de acuerdo a su agrupación, así como la sensibilidad de la información y los derechos a las aplicaciones y a cualquier otro componente de la tecnología.

La institución deberá implementar mecanismos para la administración, control y monitoreo de las autorizaciones del sistema.

ARTÍCULO 26.- Clasificación de Grupos y Asignación de Perfiles de Usuarios

Las instituciones deberán adoptar una clasificación de grupos y asignación de perfiles de usuarios internos y externos atendiendo su relación con las unidades internas, procesos y servicios.

ARTÍCULO 27.- Control de Acceso

Las políticas de control de acceso a los sistemas de información deberán establecerse cumpliendo con las disposiciones vigentes y las mejores prácticas internacionales.

Las instituciones deberán utilizar tecnologías que combinen la identificación y la autenticación del usuario, con el objeto de garantizar la confidencialidad e integridad de la información, el no repudio del usuario, controlar los accesos de alto riesgo a los sistemas de información, y en todos los casos de acceso remoto a los equipos tecnológicos realizados por los empleados y terceros.

ARTÍCULO 28.- Tiempo de Expiración

La institución deberá fijar el tiempo de expiración de una sesión, cuando iniciada la misma no se hayan ejecutado actividades después de cierto período de tiempo, determinado mediante un análisis de riesgos o de acuerdo a las mejores prácticas internacionales.

SECCIÓN II

ENCRIPTACIÓN Y SEGURIDAD EN LA RED

ARTÍCULO 29.- Encriptación de Información

La institución deberá determinar, de acuerdo a un análisis de riesgos, la necesidad de encriptar la información a ser transmitida y almacenada.

ARTÍCULO 30.- Certificación de la Identidad del Sitio de Internet

La institución deberá tomar las medidas necesarias para certificar la identidad del sitio de Internet y evitar posibles imitaciones. Asimismo, deberá proveer y capacitar a sus clientes con las metodologías y mecanismos apropiados de identificación en el acceso al sitio de Internet.

ARTÍCULO 31.- Conexión de Internet

La conexión de Internet de la institución se realizará en los siguientes casos:

1) Conexión al Internet por parte de empleados, con sujeción a lo establecido en los artículos 32 y 33 de estas normas;

2) Servicios financieros por medios electrónicos, conforme lo dispuesto en los artículos 40 al 67 de las presentes normas; y,

3) Cualquier otro caso aprobado, con anticipación, por la Comisión.

ARTÍCULO 32.- Operaciones Autorizadas

La Gerencia General de la institución deberá determinar las operaciones que sus empleados podrán realizar para la utilización del Internet, así como cumplir con los requerimientos del siguiente Artículo.

ARTÍCULO 33.- Requisitos de Conexión de Internet

Para que las estaciones de trabajo de los empleados tengan acceso al Internet deberán estar conectadas únicamente al Internet, o a una red que esté conectada exclusivamente al Internet a través de servidores separados de la red de producción. Tampoco debe existir conectividad simultánea entre la estación de trabajo y los sistemas de producción de la institución, ni acceso a información sensitiva.

La conexión a Internet deberá estar controlada por los medios indicados en el Artículo 34 y con propósitos exclusivos de navegación y de correo electrónico, sin poder descargar archivos.

No obstante lo dispuesto en el párrafo anterior, la institución que mantenga una completa segregación de su red interna, producción e Internet, podrá descargar archivos de Internet, con los controles adecuados.

ARTÍCULO 34.- Resguardo de la Conexión de Internet

La conexión de la red de la institución hacia Internet deberá encontrarse asegurada por lo menos con: un antivirus, un filtro de contenido, un Sistema de Detección de Intrusos (IDS) a nivel de red y un firewall.

ARTÍCULO 35.- Contraseñas de Acceso

Las instituciones del sistema financiero deberán otorgar a los auditores de sistemas de esta Comisión, contraseñas de acceso irrestricto a todas las aplicaciones y objetos de sus sistemas con derechos de solo lectura, en los servidores de producción y desarrollo; así como a todos los maestros, transaccionales e históricos que los auditores requieran.

Las contraseñas otorgadas no deberán tener fecha de caducidad, sin embargo las instituciones podrán eliminarlas una vez que los auditores de sistemas finalicen la auditoría.

Adicionalmente las instituciones deberán activar bitácoras de auditoría en las áreas de comunicaciones, sistema operativo y de base de datos para supervisar las actividades que realiza el personal de la Comisión. Dichas bitácoras deberán detallar las direcciones IP asignadas a cada computadora y el nombre de usuario; así como, remitidas en archivos electrónicos a la Gerencia de Informática de la Comisión, cuando sea requerido por la ésta.

CAPITULO V

PLAN DE CONTINUIDAD DEL NEGOCIO

SECCIÓN ÚNICA

ARTÍCULO 36.- Plan de Contingencias

La institución deberá mantener un plan de contingencias detallado para recuperar y operar su tecnología de información en los casos de mal funcionamiento y desastres. Dicho plan deberá enmarcarse en los principios de respaldo y recuperación descritos en el Artículo 37.

La institución deberá examinar y revisar su plan de contingencias atendiendo los cambios que han ocurrido desde la revisión anterior. Dicha revisión deberá realizarse como mínimo cada dos (2) años, así como cada vez que ocurran cambios significativos.

Asimismo, al menos anualmente y cuando ocurran cambios significativos, la institución deberá realizar y documentar pruebas de sus procesos de respaldo y recuperación.

Los equipos de almacenamiento de los respaldos de información o los respaldos en sí deberán estar localizados en un lugar distante y distinto en donde se generó la copia de la información original.

La institución deberá tomar las medidas que aseguren la posibilidad de reconstruir la información, tanto de las copias de respaldo, como de la información retenida en medios que ya no son utilizados.

ARTÍCULO 37.- Principios de Respaldo y Recuperación

La administración de la institución deberá reunirse anualmente para discutir los principios de respaldo y recuperación, así como tomar decisiones y documentar detalladamente, con base en un análisis de riesgos, los siguientes temas:

1) Definición de las situaciones de mal funcionamiento y de desastre para todas las unidades organizacionales y las implicaciones en las operaciones subsistentes de la institución.

2) Definición de los procesos vitales del negocio, los sistemas de información relevantes para la operación continua, la manera en que podría garantizar la continuidad del negocio en el caso de un mal funcionamiento y desastre, y definir todo el software, hardware y componentes de comunicaciones relacionados.

3) Aspectos de recuperación y respaldo, que incluyan las rutinas de respaldo, su duración, frecuencia, medio, tiempo máximo de estar fuera de servicio y el proceso para volver a prestar los servicios que la Gerencia General haya definido como críticos para la continuidad del negocio.

4) Relación de dependencia en entidades externas, para volver a prestar el servicio de sus sistemas de información en el caso de una interrupción, así como el tiempo de recuperación requerido por la institución para retornar a la operatividad normal en sus sistemas de información.

Dentro del contexto de la discusión, deberá tomarse una decisión sobre los procedimientos de respaldo (incluyendo quien lo hace y su documentación), así como las inversiones en las facilidades de respaldo, para los sistemas importantes que fueron definidos en las disposiciones del numeral 2) anterior del presente Artículo.

CAPITULO VI

LA TERCERIZACIÓN

SECCIÓN ÚNICA

ARTÍCULO 38.- Tercerización

La institución podrá contratar con una entidad externa, la realización de las siguientes actividades: la administración, procesamiento y resguardo de las operaciones de información, así como el desarrollo de sus sistemas, servicios de consultoría, patentes y otros servicios relacionados con las TIC.

Cuando se trate de la realización de las actividades siguientes, la contratación con terceros deberá ser hecha del conocimiento de la Comisión previo a la suscripción del contrato respectivo:

(1) La Tercerización de sistemas centrales; y,

(2) El almacenamiento de información de cualquier tipo, con respecto a los clientes de la institución, en sistemas que no se encuentran dentro de su control exclusivo.

La contratación de las actividades antes enunciadas se considerará como una forma de Tercerización Significativa. En tal caso, la Comisión podrá formular observaciones relacionadas con la seguridad, confiabilidad y eficiencia en la prestación del servicio al público. En este y en todos los demás casos de Tercerización Significativa, la institución deberá cerciorarse de la experiencia, capacidad y la viabilidad económica del proveedor de los servicios. Asimismo, deberá examinar, con antelación, la idoneidad de sus cualidades y calificaciones para desempeñar los servicios requeridos.

ARTÍCULO 39.- Contrato Escrito de Tercerización

La Tercerización deberá realizarse por medio de un contrato escrito.

Con respecto a la Tercerización Significativa, el contrato deberá contener, como mínimo, los temas siguientes:

1) Las responsabilidades de todas las partes, incluyendo las de los sub-contratistas.

2) Una introducción, alcance del trabajo, formas de comunicación, pistas y funcionamiento, administración de los problemas, compensación, obligaciones y responsabilidades de los clientes, garantías y arreglos, fianzas, derechos sobre la propiedad intelectual y de información confidencial, cumplimiento y jurisdicción legal sobre el contrato, causas de terminación, generalidades, firmas y, por último, cronogramas.

3) Las obligaciones de confidencialidad y seguridad de la información, así como las situaciones de emergencia.

4) Arreglos para la terminación del contrato y como resolver disputas. Dentro de este contrato deberá mencionar los acuerdos que habiliten a la institución para operar y mantener la actividad de la Tercerización, en situaciones en que la entidad externa quiera cesar con el servicio.

5) Las facultades suficientes para que la actividad del proveedor de servicios para la institución pueda ser auditada por la institución contratante y por la CNBS respecto de los servicios contratados.

6) El procedimiento por el cual la institución pueda obtener los datos, los programas fuentes, los manuales, y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad del procesamiento.

7) Exigir una completa separación de datos del cliente respecto de los del proveedor o de cualquier otra institución.

Lo dispuesto en el presente Artículo no exime, a la institución, de responsabilidad por cualquier actividad ilegal efectuada por el proveedor con respecto de los servicios contratados.

CAPITULO VII

SERVICIOS FINANCIEROS POR MEDIOS ELECTRÓNICOS

SECCIÓN I

SERVICIOS Y OPERACIONES DE BANCA ELECTRÓNICA

ARTÍCULO 40.- Servicios y Operaciones de Banca Electrónica

Los servicios y operaciones de banca electrónica, permitirán a los clientes obtener información de sus cuentas, realizar operaciones o dar instrucciones para realizar transacciones en su nombre, a través de los sistemas electrónicos conectados al sistema de producción de la institución.

ARTÍCULO 41.- Niveles de Servicios

Los servicios de banca electrónica se categorizarán en distintos niveles, e incluirán los servicios de los niveles que les preceden.

- **Nivel de Servicio 1:** Transferir información desde la institución hacia el cliente (estados de cuentas).

- **Nivel de Servicio 2:** Transacciones y actividades en las cuentas del cliente de la institución, como son: transferencia hacia depósitos, adquisición de fianzas, transferencia de cuenta a cuenta, solicitud de chequeras y cualquier otra transacción similar.

- **Nivel de Servicio 3:** Transacciones definidas, por adelantado, por el cliente, en beneficio de una lista de beneficiarios.

- **Nivel de Servicio 4:** Transacciones en beneficio de cuentas, que no están incluidas en uno de los niveles de servicios antes mencionados.

Cuando los servicios de banca electrónica incluyan la posibilidad de actualizar información particular o personal del cliente, la institución será responsable de verificar la información antes de ser aplicada a las bases de datos de producción.

SECCIÓN II

CONTRATACIÓN PARA PROVEER LOS SERVICIOS DE BANCA ELECTRÓNICA

ARTÍCULO 42.- Contrato de Prestación de Servicios

El contrato de servicios de banca electrónica, deberá ser firmado por el cliente permitiéndole seleccionar el nivel de servicio que requiera. La institución le otorgará a cada cliente los medios de identificación para poder conectarse a los servicios de banca electrónica, de acuerdo a las políticas de seguridad de la institución.

Cuando se utilicen contraseñas como mecanismo de control de acceso, las instituciones deberán capacitar a sus clientes en la creación y administración de contraseñas seguras o fuertes.

La institución no deberá ofrecer servicios de banca electrónica a sus clientes, utilizando medios que intencionalmente eviten que reciba servicios similares de otra institución o de otros proveedores de servicios o de información.

SECCIÓN III

REVELACIÓN DE INFORMACIÓN

ARTÍCULO 43.- Revelación de Información

El contrato de servicio deberá contener las condiciones, responsabilidades, excepciones y riesgos de la utilización de los servicios que la institución provee a través de su banca electrónica.

Asimismo, deberá revelarle al cliente los principios de seguridad que la institución haya adoptado para minimizar tales riesgos, así como recomendar a sus

clientes las maneras de protegerse contra estos riesgos. Adicionalmente, deberá informar a sus clientes que los aspectos antes mencionados no disminuyen la responsabilidad correspondiente a cada uno, según sea el caso.

SECCIÓN IV

MEDIOS DE IDENTIFICACIÓN Y AUTORIZACIÓN

ARTÍCULO 44.- Medios de Identificación

En cumplimiento a las disposiciones establecidas en el Artículo 24, la institución deberá determinar los medios de identificación para cada cliente que tenga autorización de acceso a los servicios.

El mecanismo de identificación de acceso para la Red de Cajeros Automáticos (ATMs) y de terminales de servicio deberá incluir como mínimo dos (2) de los siguientes tres (3) requisitos:

(1) Algo que conoce el cliente;

(2) Algo que le pertenece al cliente; y,

(3) Algo que identifique físicamente al cliente (característica biométrica, por ejemplo huella digital, iris del ojo, voz, etc.).

Cuando la identificación se realice por los medios de identificación provistos en el numeral (2) anterior, la institución deberá aplicar una tecnología que prevenga la posibilidad que instituciones no autorizadas reconstruyan datos a que se refiere dicho numeral.

ARTÍCULO 45.- Definición del Perfil de Usuario de Banca Electrónica

El perfil del usuario de banca electrónica deberá definirse con los permisos y accesos conforme lo establecido en el contrato de servicios.

SECCIÓN V

ADMINISTRACIÓN DE LAS CONTRASEÑAS

ARTÍCULO 46.- Asignación de Contraseña de Acceso

La contraseña inicial se le otorgará al cliente en forma personal y ésta será confidencial para terceros.

La contraseña inicial deberá ser otorgada al cliente en la institución o por cualquier otro canal de comunicación seguro que la institución esté utilizando.

Para activar una cuenta de usuario la institución deberá implantar los mecanismos que garanticen el no repudio por parte del cliente.

ARTÍCULO 47.- Cambios de Contraseñas

La institución deberá realizar los cambios de las contraseñas de los usuarios en los casos siguientes:

(1) Inmediatamente después de la primera conexión. El programa deberá pedirle al cliente cambiar su contraseña inicial.

(2) Periódicamente, de acuerdo al tiempo definido en la política de seguridad definida por la institución.

ARTÍCULO 48.- Cancelación de Contraseñas de Acceso

La institución deberá cancelar las contraseñas de sus usuarios cuando ocurra alguno de los siguientes casos:

(1) Si pasa un período de tiempo, el cual no debe ser superior a treinta (30) días y la contraseña inicial no ha sido utilizada;

(2) Cuando el usuario lo requiera o cuando la institución sospeche que la contraseña fue utilizada sin la respectiva autorización;

(3) Después de un número de intentos fallidos para entrar al sistema. Éste número deberá ser determinado por la institución, el cual no deberá exceder más de cinco (5) intentos fallidos; y,

(4) Después de seis (6) meses de no utilizar las contraseñas en los sistemas para los que fueron creados.

Una institución podrá desbloquear contraseñas inhabilitadas debiendo identificar plenamente al usuario que lo solicite. En todo caso, deberá cumplirse con lo dispuesto en el Artículo 46.

SECCIÓN VI

MEDIDAS DE CONTROL

ARTÍCULO 49.- Aplicación de Medidas de Control de Banca Electrónica

Las disposiciones de esta sección aplican al software de banca electrónica desarrollado por terceros (outsourcing) o internamente por la institución.

ARTÍCULO 50.- Validaciones

Las aplicaciones deben efectuar validaciones en todos los campos de entrada ubicados en las formas de las mismas, las validaciones deben incluir como mínimo controles de longitud máxima y mínima permitida, así como caracteres permitidos en los campos. La aplicación no debe ejecutar instrucciones directamente a la base de datos, en lugar de esto se deberán utilizar mecanismos alternos, como procedimientos almacenados.

Todas las transacciones de los usuarios deben ser almacenadas en una bitácora que permita revisiones.

ARTÍCULO 51.- Proceso de Encriptación

El proceso de encriptación de las contraseñas debe realizarse a través de algoritmos de encriptación mundialmente aceptados y que no se hayan descifrado; también debe incluir un Valor SALT para proteger la contraseña contra ataques de diccionario o fuerza bruta. En el código de la aplicación no debe estar escrita ninguna contraseña o llave para encriptar contraseñas.

ARTÍCULO 52.- Implementación de Controles

La aplicación debe implantar controles que minimicen el riesgo que la sesión de un usuario pueda ser obtenida o interceptada por un tercero para obtener acceso al sistema con credenciales previamente ingresadas.

La identificación o administración de la sesión debe ser llevada a cabo por la aplicación y no por el Servidor de Internet de la institución, la aplicación debe generar un número único y aleatorio de sesión para cada nueva sesión.

La aplicación debe eliminar las sesiones inactivas después de determinado período de tiempo.

ARTÍCULO 53.- Separación de Servidores

La base de datos de la institución debe estar en un servidor separado del servidor de Internet o servidor de aplicaciones.

ARTÍCULO 54.- Proceso de Autenticación de Usuario

Para autenticar a un usuario la aplicación deberá en la medida de lo posible solicitar además del usuario y la contraseña, un campo de control con letras y números aleatorios que el usuario debe ingresar a fin de evitar ataques de denegación de servicio automatizado.

En caso de no cumplir con el párrafo anterior, el nombre de usuario no debe ser una dirección de correo electrónica o algún valor que pueda ser adivinado y utilizado para efectuar ataques de diccionario o fuerza bruta.

Esta página de ingreso y en general todas la páginas del aplicativo deben transmitir la información a través de un canal seguro, que garantice que la información no se envíe en claro y que el usuario tenga certeza de quien le solicita sus credenciales.

Si el usuario ingresó sus credenciales en forma equivocada, la aplicación deberá presentar un mensaje de error genérico, por ejemplo “Acceso no Autorizado” y no presentar mensajes descriptivos como “Usuario no Existe” o “Contraseña Incorrecta”.

Para evitar que un atacante obtenga información que le ayude a conocer detalles particulares de la tecnología utilizada y así enfocar sus acciones, la aplicación debe capturar y manejar todos los mensajes y condiciones de error que puedan presentarse durante una sesión, incluyendo mensajes del sistema operativo o de la base de datos.

ARTÍCULO 55.- Medidas de Resguardo para Información Útil

Las aplicaciones deben asegurar que ningún parámetro con información útil para un posible atacante viaje a través del navegador del cliente y así evitar que estos parámetros puedan ser manipulados, incluyendo las consultas a nivel de URL.

ARTÍCULO 56.- Acceso Restringido

La aplicación debe asegurar que los usuarios de la misma tengan acceso solamente a las funciones, recursos y datos que están específicamente autorizados a acceder.

ARTÍCULO 57.- Acceso al Sistema de Banca Electrónica

En cada acceso al sistema de banca electrónica, la pantalla deberá mostrar al cliente, detalles del tiempo de su última conexión y la dirección IP de donde se conectó.

ARTÍCULO 58.- Impresión y/o Resguardo de Instrucciones

El usuario podrá, hasta donde sea posible, guardar y/o imprimir en tiempo real, todos los por menores de la instrucción que fue dada.

ARTÍCULO 59.- Medidas para Evitar Accesos no Autorizados

La institución deberá tomar las medidas que estén dentro de su control para evitar el acceso no autorizado. También deberá proteger la exposición de información, tal como la relativa a la cuenta del cliente, prevenir que se pueda guardar la contraseña en el explorador de Internet, prevenir que se puedan almacenar las páginas de Internet en la memoria caché y otros datos y mecanismos que expongan los datos sensibles del cliente.

SECCIÓN VII

OPERACIONES DE BANCA ELECTRÓNICA A FAVOR DE TERCEROS, POR MEDIO DE UNA LISTA DE BENEFICIARIOS

ARTÍCULO 60.- Transacciones de Banca Electrónica a Favor de Terceros

Las transacciones a favor de terceros, que realice un cliente por medios electrónicos deberán sujetarse a techos o topes que deberán ser definidos en la forma siguiente:

- Los topes o techos serán determinados por la institución y/o cliente para aplicar a las transacciones que acrediten las cuentas de los beneficiarios a que se refiere el Artículo 61.

- Los techos o topes para las transacciones que acrediten a otras cuentas se sujetarán al procedimiento descrito en el Artículo 62.

ARTÍCULO 61.- Transmisión de Datos

Cuando el cliente imparta una instrucción para efectuar un pago a un tercero a través del servicio de banca electrónica, la institución deberá requerirle que especifique las particularidades del beneficiario y la naturaleza y frecuencia de pago.

La institución deberá transmitir los datos del pagador y cuando fuese posible, la naturaleza y frecuencia de pago, así como presentarlos claramente en el resumen de la cuenta del beneficiario.

ARTÍCULO 62.- Establecimiento de Techos para las Operaciones Autorizadas

Los montos máximos de las transacciones para acreditar a otras cuentas, serán determinados para cada cliente por la institución, y deberán ser respetados tanto por el cliente como por la institución.

ARTÍCULO 63.- Lista de Beneficiarios

La institución deberá mantener almacenada en medios electrónicos, una lista de beneficiarios por cada cliente que use el servicio de banca electrónica, la cual deberá ser aprobada y actualizada por el cliente.

Al cliente se le deberá permitir enviar las modificaciones de la lista de beneficiarios directamente a la institución o en forma electrónica, según lo considere más conveniente la institución. El envío electrónico estará condicionado a la utilización de tecnología provista en el segundo párrafo del Artículo 27.

ARTÍCULO 64.- Actualización de Lista de Beneficiarios

El cliente deberá mantener actualizada su lista de beneficiarios y todas sus particularidades, incluyendo los techos o topes de los pagos a favor de cada beneficiario. Cada institución deberá informar a sus clientes las implicaciones en caso de que el cliente no mantenga actualizada la lista.

SECCIÓN VIII

CORREO ELECTRÓNICO

ARTÍCULO 65.- Correo Electrónico

La institución deberá determinar los tipos de operaciones que sus clientes podrán realizar por medio de correo electrónico.

La institución deberá tomar en cuenta el grado de necesidad de inequívoca identificación de un cliente enviando correo electrónico, de autenticación y de aseguramiento de los contenidos del mensaje, preservando la confidencialidad en la información y el no repudio, conforme a los tipos de operaciones señaladas en el párrafo anterior.

ARTÍCULO 66.- Procedimiento Formalizado

La institución deberá contar con un procedimiento formalizado para mantener comunicaciones electrónicas con los clientes.

ARTÍCULO 67.- Envío de Normas de Revelación de Información

La institución podrá hacer llegar a sus clientes, por medio de correo electrónico o por su sitio de Internet, las notificaciones que sus políticas o normas de revelación de información le permitan, así como cualquier otra información relacionada a las obligaciones de confidencialidad y estas notificaciones deberán estar estipuladas en el contrato que el usuario firma según lo establecido en los artículos 42 y 43. Adicionalmente, deberán cumplirse a cabalidad los siguientes términos y condiciones:

(1) La terminación de los servicios a requerimientos del cliente.

(2) La existencia de mecanismos o medios que permitan a la institución determinar inequívocamente si el cliente recibió el correo.

(3) La transmisión de correo de la institución hacia el cliente deberá hacerse a través de un ambiente seguro, tomando las medidas apropiadas que protejan la confidencialidad de la información.

CAPÍTULO VIII

OPERACIONES ESPECIALES

SECCIÓN ÚNICA

ARTÍCULO 68.- Remisión de Información

La institución deberá llevar registros, estadísticas y a la vez comunicar a la Comisión, los siguientes temas y eventos:

1) Eventos excepcionales tales como: intentos de ataques y penetraciones significativas, así como todos los incidentes de penetración a los sistemas; inoperatividad del sistema central o de producción, operación del plan de emergencia o cualquier otro similar;

2) La discontinuidad de servicios significativos para sus clientes, como consecuencia de un cierre no planificado de los sistemas computarizados que dure más de un día de trabajo;

3) El establecimiento de una sociedad relacionada o auxiliar que se ocupe del campo de las tecnologías de información de la institución; para lo cual requerirá autorización previa de la Comisión conforme a la norma sobre sociedades auxiliares o de servicios esenciales a las actividades de intermediación financiera;

4) La decisión de anticipar cambios significativos sobre las políticas de administración de las tecnologías de información, la migración y conversión de sus sistemas centrales computarizados; y,

5) La decisión de expandir los niveles de servicio o una nueva iniciativa de proporcionar servicios financieros por Medios Electrónicos.

ARTÍCULO 69.- Programa de Reporte de Eventos

Los reportes señalados en los numerales 1) y 2) del Artículo anterior, deberán ser registrados utilizando el Programa de Reporte de Eventos que está a disposición de las instituciones supervisadas en la red de interconexión financiera de la CNBS.

Los reportes mencionados en el Artículo 68 numerales 3) al 5) y la comunicación a que se refiere el Artículo 70, deberán ser enviadas a la Comisión con la documentación que soporta tal evento.

Los reportes establecidos en los numerales 1) y 2) del Artículo anterior, deberán enviarse dentro de los siguientes tres días hábiles a la fecha en que hubiere ocurrido el evento. Los reportes establecidos en los numerales 3) al 5) del mismo, deberán ser enviados con treinta (30) días de anticipación a su entrada en funcionamiento.

CAPÍTULO IX

BANCA DEL EXTERIOR Y MEDIDAS DE SEGURIDAD

SECCIÓN I

BANCA DEL EXTERIOR

ARTÍCULO 70.- Aplicación Especial

La aplicación de las presentes normas a las instituciones subsidiarias de instituciones extranjeras o miembros de Grupos Financieros extranjeros que operan en el territorio nacional, podrá adaptarse a sus necesidades particulares previa comunicación a la Comisión, cuando utilicen sistemas, medios, o procedimientos establecidos en o por sus casas matrices.

ARTÍCULO 71.- Banca del Exterior

Cuando las presentes normas se apliquen a las instituciones subsidiarias de instituciones extranjeras o miembros de Grupos Financieros extranjeros que operan en el territorio nacional, se incorporarán las siguientes modificaciones al texto:

a) La expresión “tecnologías de información y comunicaciones”, deberá completarse con la frase “que incluyan las interfaces de estos sistemas con el sistema de la institución extranjera”.

b) La siguiente expresión deberá añadirse como segundo párrafo al Artículo 21: “Una copia del Reporte Detallado deberá ser enviado para el conocimiento de la persona responsable de la seguridad de información de la institución matriz”.

c) Deberá agregarse al Artículo 37 de estas normas: "La institución bancaria o financiera extranjera deberá tener almacenado, en todo tiempo, en sus sistemas de información en Honduras, la información personal de todos los cuentahabientes, de los representantes legales, de los derechos de firma, así como de los saldos actuales de las cuentas que se manejan en Honduras".

SECCIÓN II

MEDIDAS DE SEGURIDAD

ARTÍCULO 72.- Controles de Seguridad

Para proteger sus sistemas las instituciones deberán incorporar como mínimo en todas sus redes los controles de Seguridad siguientes:

a) Sistemas de Detección y/o Prevención a nivel de todas sus redes que generen alertas oportunas a los administradores de la red, para que se tomen las medidas pertinentes.

b) Un Antivirus Corporativo actualizado tanto en las estaciones de trabajo fijas y portátiles como en los servidores.

c) Un mecanismo que actualice automáticamente los sistemas operativos, base de datos y programas de oficina. Estas actualizaciones deberán probarse primero, en ambientes controlados para prevenir que la instalación de las actualizaciones produzca interrupción o discontinuidad de las operaciones normales de la institución.

CAPÍTULO X

DISPOSICIONES FINALES Y TRANSITORIAS

SECCIÓN ÚNICA

ARTÍCULO 73.- Plazo de Adecuación

Las instituciones del sistema financiero tendrán un plazo de un (1) año, contado a partir de la entrada en vigencia de las presentes normas, para adecuarse a su cumplimiento.

ARTÍCULO 74.- Continuidad de Contratos

Las instituciones del sistema financiero deberán darle continuidad hasta su vencimiento de conformidad con los términos pactados a actividades contratadas antes de la entrada en vigencia de las presentes normas.

ARTÍCULO 75.- Vigencia

Las presentes normas entrarán en vigencia a partir de la fecha de su publicación en el diario oficial "La Gaceta".

2. La presente Resolución es de ejecución inmediata."

ANA CRISTINA DE PEREIRA
Presidenta

FRANCISCO ERNESTO REYES
Secretario a.i.