REPÚBLICA BOLIVARIANA DE VENEZUELA
SUPERINTENDENCIA DE BANCOS Y
OTRAS INSTITUCIONES FINANCIERAS

NORMATIVA

de Tecnología de la Información, Servicios Financieros Desmaterializados, Banca Electrónica, Virtual y en Línea para los Entes Sometidos al Control, Regulación y Supervisión de la Superintendencia de Bancos y Otras Instituciones Financieras

Caracas, marzo 2007

TABLA DE CONTENIDO

I.- HOJA DE APROBACIÓN

Unidad Usuaria: Áreas de Tecnología, Sistemas, Informática de los sujetos sometidos al control, supervisión del Organismo

Fecha de Elaboración: mayo de 2003

Fecha de Vigencia:

Versión: 1.1

El presente documento será un instrumento válido para establecer los lineamientos básicos que deberán cumplir los sujetos sometidos a la supervisión, control y regulación de la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) en la implantación y uso de Tecnología de la Información, así como, en la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual.

Diseñado y Revisado	
Coordinación de Gestión Organizacional Edgar Uzcátegui Coordinador Firma: Fecha:	Gerencia de Planificación Janette Salomón M. Gerente Firma: Fecha:
Elaborado	**Revisado**
Gerencia de Riesgo Tecnológico Franki Medina Gerente (E) Firma: Fecha:	Gerencia General de Tecnología Eduardo Monasterio Gerente General Firma: Fecha:
Revisado	**Conformado**
Consultoría Jurídica María García Consultor Jurídico Firma: Fecha:	Intendencia Operativa William Grillet Intendente Firma: Fecha:
Legalizado por:	
Trino A. Díaz Superintendente Firma: Fecha:	

II.-Introducción

Objetivo	La presente Norma tiene como objetivo establecer los lineamientos básicos que deberán cumplir los sujetos sometidos a la supervisión, control y regulación de la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) en la implantación y uso de Tecnología de la Información, así como, en la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual.
Responsable y Modificaciones	Las modificaciones y/o actualizaciones de la presente normativa deberán contar con el visto bueno de la Gerencia General de Tecnología y la Gerencia de Riesgo Tecnológico, oída la opinión del Órgano Consultor de este Organismo.
Ubicación	El presente documento normativo deberá estar en un lugar accesible, para ser consultado por los interesados.

El Superintendente de Bancos y Otras Instituciones Financieras, en uso de las facultades que le confiere los artículos 223, numeral 2 en concordancia con el 235 numeral 9 del Decreto con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras, dicta la presente normativa:

NORMATIVA DE TECNOLOGÍA DE LA INFORMACIÓN, SERVICIOS FINANCIEROS DESMATERIALIZADOS, BANCA ELECTRÓNICA, VIRTUAL Y EN LÍNEA PARA LOS ENTES SOMETIDOS AL CONTROL, REGULACIÓN Y SUPERVISIÓN DE LA SUPERINTENDENCIA DE BANCOS Y OTRAS INSTITUCIONES FINANCIERAS

TITULO I
DISPOSICIONES GENERALES

CAPITULO I
OBJETO Y ÁMBITO DE APLICACIÓN

Artículo 1: La presente Norma tiene por objeto regular la implantación y uso de Tecnología de la Información de los sujetos sometidos a la supervisión, control y regulación de la SUDEBAN, así como, de la prestación de servicios financieros desmaterializados, banca en línea, electrónica y virtual, con el fin de coadyuvar a minimizar las brechas entre los riesgos de negocio, las necesidades de control y aspectos técnicos orientados a asegurar los servicios de atención al cliente interno y externo; obligándolos a cumplir con los requerimientos de confiabilidad, efectividad, eficiencia, confidencialidad, integridad, disponibilidad y cumplimiento de la información.

Artículo 2: Las disposiciones de la presente normativa se aplicarán a los sujetos sometidos a la supervisión, control y regulación de la SUDEBAN, en lo adelante Entes supervisados, a saber: Bancos Universales, Bancos de Desarrollo, Bancos Comerciales, Bancos de Inversión, Bancos Hipotecarios, Arrendadoras Financieras, Fondos del Mercado Monetario, Casas de Cambio, Entidades de Ahorro y Préstamo y Bancos Estatales, Empresas Emisoras y Operadoras de Tarjetas de Crédito, exceptuando aquellas Instituciones establecidas o por establecerse por el Estado que tengan por objeto crear, estimular, promover y desarrollar el sistema microfinanciero del país para atender la economía popular y alternativa, tal como está previsto en el Decreto con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras.

CAPITULO II
DE LAS DEFINICIONES

Artículo 3: A los efectos de la presente normativa, se entiende por:

a. **Administración Integral de Riesgo**: Conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgos a que se encuentran expuestas las Instituciones Financieras.

b. **Administrador de Base de Datos:** Responsable del mantenimiento y control de las bases de datos, así como, de la administración del diccionario de datos, la aplicación, el método de acceso a las bases y estructuras de datos y de cualquier otra actividad asociadas a éstas.

c. **Amenaza:** Posibles eventos que pueden desencadenar un incidente en la Institución Financiera, produciendo daños materiales o pérdidas inmateriales en sus activos y en las operaciones normales del negocio, interrumpiendo en algunos casos los servicios que prestan.

d. **Arquitectura de Información:** Disciplina que organiza conjuntos de información, permitiendo que cualquier persona los entienda y los integre a su propio conocimiento, de manera simple.

e. **Autenticación:** Proceso de comprobación de la identidad de una persona, de un usuario emisor o receptor de información.

f. **Banca en línea**: Incluye todos los sistemas, equipos, servicios y productos que son ofrecidos a los usuarios de las Instituciones Financieras a nivel de sus agencias, oficinas y sucursales.

g. **Banca Electrónica:** Sistemas, equipos, productos y servicios ofrecidos por las Instituciones Financieras a través del uso de Internet Banking, cajeros automáticos (ATM), puntos de ventas (POS), dispensadoras de chequera, sistemas de atención de reclamos y otros servicios que se encuentren automatizados a través de plataformas de cómputo.

h. **Banca Virtual ("Internet Banking"):** Conjunto de productos y servicios ofrecidos por los bancos, entidades de ahorro y préstamo y demás Instituciones Financieras, para realizar por medios electrónicos, magnéticos o mecanismos similares, de manera directa y en tiempo real las operaciones que tradicionalmente suponen la realización de llamadas telefónicas o movilizaciones de los usuarios a las oficinas, sucursales o agencias.

i. **Base de Datos:** Sistema formado por un conjunto de datos almacenados en discos o cualquier otro medio magnético que permite el acceso directo a ellos, encontrándose estructurados de manera fiable y homogénea, organizados independientemente, accesibles en tiempo real, compartidos por usuarios concurrentes que tienen necesidades de información diferentes y no predecible en el tiempo.

j. **Cableado Estructurado:** Infraestructura de cable única y completa destinada a transportar, a lo largo y ancho de un edificio, las señales que emite un emisor de algún tipo de señal hasta el correspondiente receptor.

k. **Configuración Base:** Adaptación básica de una aplicación, sistemas o equipos al resto de los elementos del entorno y a las necesidades específicas del usuario.

l. **Control de Acceso:** Conjunto de procedimientos usados para limitar el acceso de los usuarios a los diferentes recursos de un sistema o equipos.

m. **Control Interno:** Conjunto de políticas, normas, procedimientos, planes, métodos, principios y mecanismos de verificación y evaluación adoptados por la Institución para evaluar en forma preventiva, detectiva y correctiva las actividades, operaciones y actuaciones, así como, la administración de la información y los recursos, a fin de que se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

n. **Cortafuego ("firewall"):** Equipo o bloque de instrucciones de programación interpuesto como barrera en un sistema informático o una red local con el propósito de prevenir o aminorar los graves daños que podrían derivarse de su uso erróneo o malintencionado.

o. **Diccionario de Datos:** Descripciones de los archivos, campos y variables usados en un sistema de administración de datos.

p. **Encriptación:** Técnica usada para transformar los datos y deformar su contenido mediante la aplicación de un código secreto con el objeto de evitar que sean conocidos por personas no autorizadas durante su transmisión por canales de comunicaciones o en su almacenamiento en soportes de acceso público.

q. **Componentes Físicos ("hardware"):** Son todos los componentes materiales de los computadores y sus periféricos (discos, memoria, impresoras, entre otros).

r. **Infraestructura de Comunicaciones:** Conjunto de dispositivos empleados para transmitir señales en la forma de un mensaje entre un remitente y un destinatario. Para alcanzar el destino final se usan componentes de transmisión y técnicas de conmutación o distribución de mensajes. Los componentes de transmisión definen el medio real de la transmisión y las técnicas de codificación o de canalización de los datos.

s. **Internet:** Red informática global que permite la conexión entre sí de dos o mas computadores situados en cualquier lugar del mundo a través de los canales y líneas telefónicas.

t. **Lenguaje de Programación:** Esquema de notación normalizada utilizada para la escritura de programas informáticos.

u. **Misión Crítica:** Aquellas aplicaciones, sistemas, procesos, operaciones, equipos y cableado que en caso de falla o paralización parcial o total pueden ocasionar pérdidas incalculables o severas que afecten la continuidad operativa del negocio.

v. **Niveles de Escalamiento:** Distintas etapas que deberán ser definidas por el personal de Tecnología de Información para manejar y resolver los problemas, incidencias o eventos que puedan afectar el nivel de servicio y/o la operatividad de las aplicaciones, sistemas o equipos de misión crítica de la Institución. En cada nivel que se defina, deberán establecerse las acciones a ejecutar, el personal involucrado en cada etapa y los mecanismos que han sido definidos para contactarlos.

w. **Operaciones de los Sistemas de Información:** Comprende la administración, control y monitoreo de las actividades realizadas en las áreas de planificación, producción y operaciones del área de Tecnología de la Información.

x. **Plataforma Tecnológica:** Agrupación de equipos, aplicaciones y sistemas destinados a ofrecer productos y servicios a través del uso de los recursos tecnológicos disponibles, a una comunidad de usuarios, públicos y privados, tanto a nivel local, regional como nacional.

y. **Paneles de Patcheo ("patch panels"):** Dispositivos empleados para interconectar diferentes puntos de una red.

z. **Perímetro de Seguridad**: Delimitación de un espacio físico por medio de una barrera (pared, puerta de acceso controlado, entre otros.). El emplazamiento y la fortaleza de cada barrera dependerá de los resultados de la evaluación de riesgo realizada.

aa. **Plan de Contingencias Tecnológicas:** Conjunto de operaciones, procesos y procedimientos probados que aseguran la continuidad estratégica de la plataforma tecnológica ante interrupciones graves del servicio.

bb. **Procedimientos de Recuperación**: Involucra el conjunto de actividades que agrupadas a través de un plan son necesarias para restaurar los servicios definidos por la Institución como críticos, así como, las comunicaciones y la capacidad normal de procesamiento y almacenamiento.

cc. **Proveedor de Tecnología:** Persona natural o jurídica que ofrece a un tercero los servicios de asesoría, soporte, mantenimiento, almacenaje, procesamiento, comunicación, programación, diseño y cualquier otra actividad relacionada con Tecnología de la Información.

dd. **Red:** Sistema de comunicación de datos que enlaza dos o más computadores y dispositivos periféricos.

ee. **Red de Área Local (LAN):** Segmento de red que tiene conectada estaciones de trabajo y servidores, generalmente dentro de la misma zona.

ff. **Red de Área Metropolitana (MAN**): Red que se expande por ciudades o provincias y se interconecta mediante diversas instalaciones públicas o privadas.

gg. **Red de Área Extensa (WAN):** Redes que se extienden sobrepasando las fronteras de las ciudades, provincias o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas o privadas, microondas y satélites.

hh. **Red Inalámbrica (wireless):** Sistema de comunicación de datos flexible que emplea la transmisión de radio frecuencia y la luz infrarroja para transmitir datos en forma inalámbrica.

ii. **Registros o Trazas de Auditoria:** Archivo protegido contra escritura que almacena información en forma secuencial de las transacciones u operaciones que son ejecutadas por los usuarios de los sistemas de información.

jj. **Riesgo:** Posibilidad de que se produzca un acontecimiento que conlleve a pérdidas materiales en el resultado de las operaciones y actividades que desarrollen las Instituciones Financieras.

kk. **Riesgo Tecnológico:** Se define como la posible pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en los equipos, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios o financieros con los clientes.

ll. **Segmento de Red o Subred:** Conjunto de dispositivos o equipos que comparten un medio físico de transmisión y utilizan técnicas de comunicación comunes.

mm. **Seguridad Lógica:** Consiste en la aplicación de barreras y controles internos que resguarden el acceso a los datos y que garanticen que sólo permita a las personas autorizadas acceder a ellos, manteniendo registros que lo evidencien.

nn. **Servicios Desmaterializados:** Los servicios al público que presten las Instituciones Financieras a través de medios en los cuales el soporte documental sea sustentado a través de transacciones electrónicas.

oo. **Software:** es un conjunto de programas, documentos, procedimientos y rutinas asociados con la operación de un sistema de cómputo.

Artículo 4: Se consideran como criterios básicos de calidad de la información aquellos asociados a los siguientes aspectos:

a. **Confiabilidad:** Nivel de veracidad y exactitud de los datos contenidos en los sistemas de información.

b. **Confidencialidad:** Protección de la información sensible contra la divulgación no autorizada.

c. **Disponibilidad:** Accesibilidad a la información en el tiempo y la forma cuando esta sea requerida.

d. **Efectividad:** Información relevante y pertinente para los procesos del negocio que se presenta en forma correcta, coherente, completa y oportuna.

e. **Eficiencia:** Obtención de la información a través del uso de los recursos de forma más productiva y menos costosa.

f. **Integridad**: Precisión y suficiencia de la información, así como, su validez acorde con las pautas fijadas por la Institución y regulaciones externas.

g. **Cumplimiento:** se refiere al acatamiento de las leyes y reglamentaciones a las que están sujetas las Instituciones sometidas a la supervisión, control, fiscalización y regulación de esta Superintendencia.

TITULO II
PLANEACIÓN ESTRATÉGICA Y ORGANIZACIÓN DE LOS RECURSOS DE INFORMACIÓN

CAPITULO I
DEPENDENCIA FUNCIONAL E INFRAESTRUCTURA DEL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN

Artículo 5: La Alta Gerencia del Ente supervisado, debe garantizar que el área de Tecnología de la Información posea independencia funcional de las áreas usuarias.

Artículo 6: La infraestructura del área de Tecnología de la Información debe ser consistente con la naturaleza y complejidad de las operaciones que realiza el Ente supervisado.

CAPITULO II
POLÍTICAS, NORMAS Y PROCEDIMIENTOS

Artículo 7: Las políticas, normas y procedimientos del área de Tecnología de la Información deben documentarse, formalizarse y circularizarse, asegurando que estas se mantengan adecuadamente actualizadas.

CAPITULO III
COMITÉ DE DIRECCIÓN Y PLANIFICACIÓN DE LOS SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN

Artículo 8: El Ente supervisado debe conformar un Comité de Dirección y Planificación de los Servicios de Tecnología de la Información, que coordine todo lo concerniente a la planeación y ejecución de las actividades relacionadas con el área tecnológica.

Parágrafo Único:

El Comité de Dirección y Planificación de los Servicios de Tecnología, debe incluir entre sus miembros a representantes de las áreas de Tecnología, Administración Integral de Riesgos, Auditoría de Sistemas y Gerentes de las unidades usuarias.

Durante la creación de dicho comité deberán definirse sus funciones y actividades, así como, la periodicidad de las reuniones de trabajo en las cuales se documentarán las decisiones y acuerdos establecidos, mediante actas que se mantendrán archivadas durante un periodo no menor a dos (2) años.

CAPITULO IV
PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍA DE LA INFORMACIÓN

Artículo 9: El Ente supervisado deberá establecer un proceso de planificación de Tecnología de la Información acorde con los objetivos del negocio, destacando que su elaboración será a través del uso de una metodología formal y consistente con la realidad de la Institución.

En este sentido, la Alta Gerencia de los servicios de Tecnología de la Información debe efectuar un seguimiento continuo de las tendencias tecnológicas, así como, a las regulaciones emitidas por esta Superintendencia que regulen su funcionamiento, de modo que estas sean consideradas al momento de elaborar y actualizar la planificación estratégica de tecnología.

Artículo 10: El Plan Estratégico de Tecnología debe ser documentado, aprobado y permitir una supervisión continúa que asegure el logro de las metas y actividades del área tecnológica, clasificando los proyectos principales en planes a corto y largo plazo. Para ello, deberá incorporar los respectivos cronogramas de implantación.

Artículo 11: En el plan a corto plazo se incluirán todos los proyectos cuya ejecución y término abarque un periodo no mayor a doce (12) meses, es decir, un (1) año.

Artículo 12: El plan a largo plazo comprende todos los proyectos cuya ejecución y finalización se extiendan en un plazo mayor a un (1) año.

Artículo 13: En forma previa al desarrollo o modificación del plan estratégico de Tecnología de la Información, el Comité de Dirección y Planificación de los Servicios de Tecnología de la Información debe coordinar la elaboración de un diagnóstico de los sistemas existentes que apoyen el proceso de toma de decisiones en términos de:

a. Nivel de automatización de negocio.

b. Funcionalidad.

c. Estabilidad.

d. Complejidad.

e. Costos operacionales.

f. Fortalezas y debilidades.

g. Análisis financiero costo/beneficio

CAPITULO V
DEL PERSONAL DEL ÁREA DE TECNOLOGÍA DE INFORMACIÓN

Artículo 14: El área de Tecnología de la Información en conjunto con Recursos Humanos debe identificar, organizar, capacitar y desarrollar a los usuarios finales en el uso efectivo de la tecnología, seguridad, riesgos y responsabilidades relacionadas con el desarrollo normal de sus actividades.

Artículo 15: El área de Recursos Humanos del Ente supervisado, debe establecer procedimientos formales para la selección y reclutamiento del personal de tecnología, en los cuales deben contemplar la

participación de la Alta Gerencia del área de Tecnología de la Información.

Artículo 16: El área de Recursos Humanos del Ente supervisado debe documentar en un Manual Descriptivo de Cargos las funciones, actividades y responsabilidades inherentes del personal de Tecnología de Información, así como, la descripción del perfil técnico y de las competencias que debe tener el ocupante de cada cargo.

TITULO III
OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN

CAPITULO I
DOCUMENTACIÓN, PLANIFICACIÓN DE LAS OPERACIONES Y PROCESAMIENTO DE LA INFORMACIÓN

Artículo 17: Los sujetos que se encuentran bajo la supervisión de esta Superintendencia, deben elaborar y mantener actualizada la documentación que sustente las actividades que se realizan en el centro de procesamiento de datos.

Artículo 18: La Institución Financiera debe establecer procedimientos que aseguren la continuidad del procesamiento durante los cambios de turno de los operadores, así como, garantizar el registro cronológico de información en las trazas de auditoria.

Artículo 19: El Ente supervisado deberá asegurar que la programación de tareas y procesos mantengan una secuencia eficiente, maximizando el uso de los recursos y su utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio.

Artículo 20: La Institución deberá asegurar la existencia de un registro cronológico y trimestral de los procesos ejecutados en el centro de procesamiento de datos, que permita la revisión y evaluación oportuna de la información inherente a los eventos de excepción que afecten la planificación diaria, mensual y semestral.

Artículo 21: La planificación de los procesos y actividades que se desarrollan dentro del centro de procesamiento de datos, deben estar adecuadamente documentadas, contemplando como mínimo, los siguientes aspectos:

a. Procedimientos que contemplen los comandos o instrucciones que ejecutan los operadores en el ambiente productivo de cada uno de los computadores y equipos periféricos existentes.

b. Registros automáticos de la ejecución de los cronogramas de trabajos, eventos de excepción y la generación de trazas de auditoria.

c. Procesos de mantenimiento y monitoreo sobre los registros automatizados de las operaciones.

d. Funcionalidad de los programas o procesos que componen los cronogramas de trabajo automatizados (en línea o en lotes).

e. Controles que se aplican para asegurar la correcta ejecución de los cronogramas de trabajo previamente agendados.

f. Mecanismos definidos para la adecuada comprobación del cierre contable y la distribución de la información a los usuarios.

g. Procedimientos que aseguren la continuidad del procesamiento en línea o en lotes.

h. Niveles de escalamiento, en caso de presentarse eventos de excepción, fallas o incidencias.

Artículo 22: Las estrategias de procesamiento de información deberán revisarse trimestralmente o cada vez que surjan cambios en las plataformas tecnológicas de misión crítica, para asegurar que los nuevos servicios o modificaciones a los existentes, no han invalidado los procesos ya definidos.

CAPITULO II
RESPALDOS Y RESGUARDO DE LA INFORMACIÓN

Artículo 23: El Ente supervisado, deberá realizar respaldos de archivos, bases de datos, sistemas operativos y demás software necesario para el adecuado funcionamiento de los equipos y aplicaciones de misión crítica con una frecuencia diaria, semanal y mensual.

Artículo 24: Se deben documentar las políticas, normas y procedimientos que aseguren la ejecución periódica de los respaldos de la información y de los sistemas de misión crítica, con la finalidad de garantizar la continuidad del negocio.

Los medios de almacenamiento masivo contentivo de las aplicaciones e información de misión crítica deben ser probados periódicamente para garantizar que cumplen con los requerimientos establecidos en los planes de continuidad del negocio. Adicionalmente, para el resguardo de los respaldos se deberán considerar los siguientes controles:

a. La información resguardada deberá poseer un nivel adecuado de protección física y ambiental, consistente con los estándares aplicados en el centro de procesamiento de datos principal. Los controles aplicados a los dispositivos en la cintoteca principal deben extenderse para cubrir el sitio de resguardo.

b. Diseñar, formalizar y actualizar periódicamente los procedimientos de restauración de los dispositivos de almacenamiento con la finalidad de garantizar su buen estado y funcionamiento, así como, la eficacia de los procesos respaldados.

c. Los medios de respaldo deben probarse periódicamente, a fin de garantizar la confiabilidad de los mismos con relación a su eventual uso en casos de emergencia.

d. Los procedimientos de restauración deben probarse al menos dos (2) veces al año para garantizar su eficacia e idoneidad.

e. Los medios de almacenamiento masivo deberán encontrarse adecuadamente identificados, a través de una codificación que maneje como mínimo la fecha de generación del respaldo, nombre de la aplicación, tipo de información y periodo que se está respaldando. El proceso de etiquetado deberá ser consistente con los procedimientos establecidos para tal fin, razón por la cual, deberán mantenerse actualizados.

Artículo 25: La información respaldada debe ser resguardada en un mobiliario especializado (cintoteca, discoteca o bóveda.) con adecuadas características de clasificación y distribución de los dispositivos de almacenamiento que permitan una búsqueda expedita de la información.

Artículo 26: Disponer de centros de resguardo interno y externo, destacando que este último debe poseer una ubicación remota, a una distancia suficiente como para evitar daños provenientes de una situación de emergencia o desastre (terremoto, inundación o incendio) en la sede principal, todo ello para garantizar la continuidad de las operaciones.

El centro de resguardo externo debe retener al menos diez (10) generaciones o ciclos de la información de misión crítica de la Institución.

Artículo 27: Los centros de resguardo de la información, tanto interno como externo, deben estar dotados de una adecuada seguridad física y ambiental, que garantice la protección de la información y los sistemas de misión crítica de daños, deterioro, hurto o robos con el fin de asegurar que pueda recuperarse una vez ocurrido un desastre o falla en los equipos que los almacenan.

Artículo 28: El traslado de los dispositivos de almacenamiento entre los centros de resguardo debe efectuarse con adecuados controles de seguridad (precintos, bitácoras de salida y entrada, personal autorizado, entre otros aspectos) que minimicen la exposición de la información contenida en los mismos.

TITULO IV
CONTRATACIÓN DE PROVEEDORES EXTERNOS

CAPITULO I
PROVEEDORES EXTERNOS

SECCIÓN PRIMERA
EVALUACIÓN Y SELECCIÓN DE LOS PROVEEDORES EXTERNOS DE TECNOLOGÍA DE INFORMACIÓN

Artículo 29: Se debe mantener un procedimiento documentado y formalizado para realizar la selección de los proveedores externos de Tecnología de Información y asegurar que estos se encuentren adecuadamente calificados sobre la base de una evaluación de su capacidad de prestación del servicio requerido, antes de proceder a la contratación.

En este sentido, deberán considerarse los aspectos que a continuación se detallan:

a. La naturaleza y especificaciones del servicio contratado.

b. Los requisitos funcionales y técnicos de los artículos o servicios a ser adquiridos.

c. Los costos totales de la adquisición, compra, implantación, alquiler o arriendo (incluyendo el asociado a los honorarios de consulta) de los sistemas, aplicaciones o equipos adicionales.

d. El nivel de soporte y capacitación a ser proporcionados por el proveedor.

e. La estabilidad financiera del proveedor, así como el producto o servicio a ser proporcionado y el tiempo para la entrega, terminación o implantación.

f. Garantizar que el proveedor cuente con una adecuada solidez financiera, la reputación y habilidad para cumplir con las obligaciones adquiridas, así como, las políticas y los controles para el manejo de los riesgos asociados al servicio prestado.

g. Experiencia y capacidad de la empresa proveedora en el procesamiento de datos y servicios bancarios que respondan a las características del servicio que se desea contratar.

h. El diseño de políticas adecuadas para la asignación de responsabilidades por motivo de irregularidades en la ejecución del servicio contratado.

SECCIÓN SEGUNDA
DEL CONTRATO DE SERVICIOS TECNOLÓGICOS

Artículo 30: El contrato con el proveedor externo de tecnología deberá contener como mínimo las siguientes cláusulas:

a. Garantía de acceso a los programas fuentes, en caso de quiebra del proveedor o situaciones contingentes que así lo requieran, las cuales deberán quedar claramente expresadas en el mencionado documento.

b. Especificaciones sobre la propiedad de los activos de información empleados durante la contratación del servicio (aplicaciones o sistemas propietarios, equipos, licencias, entre otros aspectos).

c. Establecer la protección, privacidad y confidencialidad de los activos informáticos del Ente supervisado que serán accedidos y manejados por el proveedor de servicios.

d. Indicar en forma pormenorizada las características de la plataforma de desarrollo que será utilizada por el proveedor (tales como equipos, sistemas o aplicaciones, lenguaje de programación y motor de base de datos), así como, las políticas de seguridad, respaldos y traslado de información a otros ambientes.

e. Indicar el tiempo de desarrollo por cada etapa definida en forma detallada, incluyendo las pruebas de los programas desarrollados.

f. Establecer cláusulas de indemnización por daños y perjuicios, en caso de fraudes o sabotajes cibernéticos.

g. La responsabilidad que asume la empresa proveedora para mantener políticas, normas y procedimientos que garanticen la seguridad informática, el secreto bancario, la confidencialidad de la información, así como, aquellas tendentes a prevenir pérdidas, atrasos o deterioros de los datos, en conformidad con lo establecido en la legislación venezolana.

h. La facultad del Ente supervisado para practicar evaluaciones periódicas directas de las actividades efectuadas por la empresa proveedora del servicio, mediante auditorías independientes, incluyendo aquellas requeridas por esta Superintendencia.

i. Que la infraestructura tecnológica, los sistemas operativos y las herramientas de desarrollo, que se utilizarán estén debidamente licenciados por el fabricante o representante de software, según sea el caso.

j. Que la infraestructura tecnológica y los sistemas que se utilizarán para la comunicación, almacenamiento y procesamiento de datos, ofrezcan suficiente seguridad para asegurar la continuidad operacional y la confidencialidad, integridad, exactitud y calidad de la información. De igual forma, deberán considerarse las condiciones que garantizan la obtención directa y oportuna de cualquier dato o información que se necesite, sea para sus propios fines o para cumplir con los requerimientos de las autoridades competentes.

Artículo 31: El Ente supervisado deberá mantener los documentos y antecedentes de los contratos suscritos y vigentes con empresas proveedoras de servicios de tecnología de información a disposición de esta Superintendencia.

Artículo 32: Los contratos deben establecer claramente la "no existencia" de limitaciones para las actuaciones por parte esta Superintendencia para la visitar las instalaciones de los proveedores de servicios de tecnología de información, acceder a la información y a toda la documentación técnica relacionada para la verificación del cumplimiento de los aspectos contemplados en estas normas.

Artículo 33: La Alta Gerencia establecido con la Vicepresidencia o Gerencia de Informática, Sistemas o Tecnología del Ente supervisado, son los principales responsables sobre el control de las actividades que han sido delegadas mediante el contrato establecido con terceros.

SECCIÓN TERCERA
CONTROL Y SEGUIMIENTO DE LAS ACTIVIDADES Y PROCESOS EJECUTADOS POR EL PROVEEDOR.

Artículo 34: Se debe garantizar que el recurso humano del Ente supervisado esté técnicamente capacitado, para ejercer un control eficiente sobre las actividades que desarrolla el proveedor externo.

Artículo 35: La Vicepresidencia, Dirección o Gerencia de Informática, Sistemas o Tecnología del Ente supervisado debe monitorear a través de un proceso continuo, el adecuado cumplimiento de los contratos por parte de terceros para asegurar que cumplan con los términos y condiciones estipulados en el contrato. En este sentido, deberán documentar la evaluación realizada, así como, el seguimiento continuo de los servicios prestados.

Adicionalmente, deberán definir procedimientos efectivos que permitan la selección y el monitoreo de la calidad y cumplimiento de servicio por parte de los proveedores e implantar los mecanismos que aseguren la integridad y la confidencialidad de la data o información del Ente supervisado y de sus clientes.

SECCIÓN CUARTA
TERCERIZACIÓN DE SERVICIOS

Artículo 36: Cuando el Ente supervisado contrate a una persona natural o jurídica residenciada fuera del territorio de la República Bolivariana de Venezuela para efectuar determinadas actividades o servicios, los requerimientos de seguridad, administración y el control de todos los activos informáticos involucrados en el servicio de tercerización, deben ser contemplados en un contrato celebrado entre las partes. Este documento deberá considerar en adición a los ya contemplados en el artículo 31 de la presente normativa, los siguientes aspectos:

a. El cumplimiento a las regulaciones emanadas por los Entes u Organismos Contralores del Estado.

b. Las disposiciones que serán implementadas para garantizar que las partes involucradas en la tercerización, cumplirán las responsabilidades asociadas a la seguridad de la información.

c. Los mecanismos empleados para asegurar y comprobar la integridad y confidencialidad de la información manejada por las partes involucradas.

d. Los controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso de los usuarios autorizados a la información sensible.

e. Las actividades empleadas para garantizar la disponibilidad de los servicios contratados ante la ocurrencia de desastres.

f. Los niveles de seguridad física que se asignarán al equipamiento tercearizado.

g. El derecho a la auditoria por parte del Ente supervisado, auditores externos y esta Superintendencia.

h. La representación legal del proveedor de servicios ubicada o residenciada en el territorio nacional.

Artículo 37: El almacenamiento de los datos y la administración de la seguridad lógica de los recursos de Tecnología de la Información son responsabilidad absoluta del Ente supervisado, por tal razón, es competencia expresa e ineludible de éste, es decir, indelegable dentro del servicio de tercerización contratado.

TITULO V
SEGURIDAD DE LA INFORMACIÓN

CAPITULO I
POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS INFORMÁTICOS

Artículo 38: El Ente supervisado debe administrar adecuadamente la seguridad lógica de los recursos de Tecnología de la Información, incluso aquellos que sean administrados o custodiados por terceros. En consecuencia deberá establecer, formalizar e informar las políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, operativos y de base de datos.

De igual forma, deberán incluir entre sus políticas y procedimientos aquellos que permitan hacer un seguimiento a las transacciones operaciones que sean ejecutadas sobre los activos informáticos.

Artículo 39: En la estructura organizacional del Ente supervisado, debe existir un área de seguridad de la información independiente de las unidades de Tecnología de la Información, Auditoria de Sistemas y Riesgo, estableciéndose como mínimo las siguientes funciones:

a. Definir y mantener actualizadas las políticas de seguridad de la información.

b. Aplicar y asegurar el cumplimiento de las políticas de seguridad de la información definidas.

c. Administrar el acceso a los sistemas operativos, bases de datos, aplicaciones, cortafuego, enrutadores, proxys, equipos computacionales y de telecomunicaciones empleados por el Ente supervisado, incluyendo aquellos administrados y custodiados por terceros.

d. Monitorear los procesos de control de cambio y pases a producción de los sistemas y aplicaciones productivas.

e. Realizar el control y seguimiento continuo a los accesos efectuados a los activos de información.

f. Establecer políticas, normas y procedimientos que regulen, controlen y aseguren el seguimiento continuo de la utilización del correo electrónico e Internet y todas aquellas transacciones que son ejecutadas a través de los diferentes canales electrónicos empleados por los clientes.

CAPITULO II
CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN

Artículo 40: Los empleados del Ente supervisado deben firmar un acuerdo de confidencialidad y la no divulgación de la información, como parte de sus términos y condiciones iniciales de empleo.

Parágrafo Único:

El personal temporal o contratado, así como los usuarios externos deben firmar el acuerdo de confidencialidad y la no divulgación de la información, antes de que se les otorgue el acceso a las instalaciones de procesamiento de la información. Por otra parte, no deberán tener acceso a las bases de datos del Ente supervisado, en procura de mantener la confidencialidad de la información del cliente

Artículo 41: El Ente Supervisado deberá establecer un esquema de referencia de clasificación o categorización relativa a la confidencialidad de los datos según su nivel de sensibilidad (información confidencial, pública, privada, entre otros).

Artículo 42: Los accesos a los sistemas, aplicaciones o bases de datos deben administrarse a través del uso de perfiles definidos y documentados, los cuales estarán asociados a los cargos, roles o actividades desempeñadas por los usuarios.

Las normas y procedimientos establecidos para la asignación de los accesos deben estar debidamente documentados y formalizados.

Artículo 43: La unidad de seguridad de los activos de información deberá garantizar que los operadores de turno no tengan acceso al ambiente de producción definido en los computadores y servidores de misión crítica del Ente supervisado.

Artículo 44: El Ente supervisado debe establecer políticas y procedimientos para regular, controlar y monitorear la utilización y acceso al correo electrónico e Internet, así como, a los enrutadores, cortafuego (firewall) y proxys. De igual forma, deberá generar reportes de auditoria sobre intentos de violaciones a las redes o equipos, detección de posibles delitos informáticos que atentan contra la confidencialidad de los clientes, uso de utilitarios sensitivos y las actividades de los usuarios con atributos de administración y accesos especiales.

Artículo 45: Definir mecanismos que permitan restringir al personal no autorizado el tráfico de datos entrantes y salientes a los recursos tecnológicos de la red. De igual forma, será necesario efectuar pruebas de penetración, tanto internas como externas, en periodos no mayores a un (1) año.

Artículo 46: Establecer dentro de su plataforma de red, aplicaciones que faculten la prevención, detección y eliminación de virus informáticos. El Ente supervisado, deberá asegurarse de la oportuna actualización de la base de datos de virus.

Artículo 47: Restringir el acceso a utilitarios sensitivos que permitan modificar datos en el ambiente de producción, para lo cual deberán documentar, sustanciar y justificar cuando ocurra el evento.

Artículo 48: La plataforma tecnológica del Ente supervisado, debe ser auditada por medio de evaluaciones internas y externas en períodos no mayores a un (1) año. Para ello, el área de auditoria de sistemas deberá definir un plan de trabajo anual que sustente las actividades que serán efectuadas para asegurar el adecuado control interno asociado al uso de la Tecnología de Información.

CAPITULO III
GENERACIÓN DE REGISTROS DE AUDITORIAS

Artículo 49: Se deben mantener activos los registros o pistas de auditoría generadas por las aplicaciones y sistemas de misión crítica, particularmente en aquellos casos en los cuales exista modificación o alteración de la información almacenada en las bases de datos productivas. De igual forma, deberán

asegurar el almacenamiento de los mencionados registros por un periodo de un (1) año.

Por otra parte, las pistas de auditoria deberán ser revisadas por el área de seguridad de la información y auditoría de sistemas, para lo cual será necesario generar informes que reflejen posibles brechas o vulnerabilidades identificadas. Estos informes deberán generarse anualmente y deben ser entregados a esta Superintendencia, cuando así sea requerido.

CAPITULO IV
SEGURIDAD FÍSICA

Artículo 50: El Ente supervisado debe contar con una cobertura o una provisión de seguros para los principales equipos de cómputo y telecomunicaciones que permita mitigar los posibles riesgos existentes (incendio, huelga, motín, impacto de rayo, explosión, implosión, humo, gases o líquidos corrosivos, corto circuito, variaciones de voltaje, robo, asalto y fenómenos naturales).

Artículo 51: Los materiales de construcción del edificio en el cual se almacena el centro de datos, incluyendo paredes, techo y pisos deben ser de materiales no combustibles.

Artículo 52: Las paredes del centro de procesamiento de datos deben extenderse desde la estructura del piso a la del techo del edificio y no desde pisos elevados o techos falsos, con el fin de impedir una entrada subrepticia a las áreas sensibles de la citada instalación.

Artículo 53: Instalar como mínimo un sistema de supresión de fuego de contacto seco en el cuarto en el que se encuentra el computador central y especialmente dentro de la cinto o discoteca.

Artículo 54: Garantizar el mantenimiento adecuado de los detectores y sistema de alarma contra incendio, así como de las salidas de emergencia, paneles de distribución eléctrica y de potencia, aire acondicionado, suministros de potencia ininterrumpibles (UPS), plantas eléctricas, entre otros aspectos.

Artículo 55: Se debe contar con un sistema de seguridad eléctrica que proteja de las variaciones de voltaje al computador central, sus periféricos y a los equipos de comunicación de datos. Por otra parte, el cuarto de comunicaciones debe mantener instalado supresores de corrientes, protectores de las líneas de datos, barras de tierras, entre otros aspectos. De igual forma, debe estar libre de contactos e instalaciones eléctricas en mal estado.

Artículo 56: Se debe ubicar el panel de distribución del sistema eléctrico en un área segura e inaccesible a personas no autorizadas.

Artículo 57: Garantizar la redundancia de los equipos de aire acondicionado instalados en el centro de procesamiento de datos.

Artículo 58: Los centros de procesamiento de datos y telecomunicaciones tanto principales como alternos, deben contar con mecanismos adecuados para la detección y extinción de incendios que aseguren la integridad del personal que reside dentro o cerca de estas instalaciones, así como, la de los activos de información. De igual forma, las mencionadas áreas deben contar con dispositivos de control de la humedad y del clima, mantenerse libres de material inflamable. En este sentido, se deberán realizar simulacros sobre los posibles eventos de contingencia que podrían presentarse en estas instalaciones.

Parágrafo Único:

El Ente Supervisado debe asegurar la existencia de procedimientos que regulen las condiciones ambientales de las instalaciones de los centros de procesamiento de datos y telecomunicaciones, tanto

principales como alternos, a fin de asegurar que estos proporcionen un ambiente físico conveniente para su funcionamiento y protejan los activos de información y al personal adscrito al área de Tecnología de la Información contra peligros naturales o fallas humanas.

Artículo 59: Los centros de procesamiento de datos y telecomunicaciones, deben mantenerse separados y claramente definidos por perímetros físicos. De igual forma, deben mantenerse continuamente monitoreados cubriendo para ello, todo el perímetro de sus instalaciones.

Artículo 60: El cableado de comunicaciones debe estar debidamente protegido por canaletas, así como identificado o etiquetado. Por otra parte debe estar separado de los cables de electricidad.

Artículo 61: Los centros de procesamiento de datos y telecomunicaciones, tanto principales como alternos, deben ser resguardados por adecuados controles de acceso, para lo cual se deben considerar los siguientes aspectos:

a. Utilizar controles de autenticación para el acceso de personal autorizado (tarjeta, número de identificación personal -PIN-, carnet, biometría, entre otros).

b. Restringir el acceso a personal no autorizado a las mencionadas instalaciones. Por otra parte, las actividades ejecutadas por los visitantes deben ser supervisadas o inspeccionadas, así como encontrarse registradas en las bitácoras definidas para tal fin.

c. Revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas o restringidas.

Artículo 62: Las instalaciones internas o externas en las cuales se guardan, almacenan y custodian los respaldos de información, deben mantener niveles de seguridad similares a los definidos para los centros de datos.

Artículo 63: Los listados y documentación de datos, programas y sistemas deben estar resguardados con adecuadas medidas de seguridad. Se debe definir un procedimiento para determinar la destrucción o desecho de los reportes generados, una vez cumplido su periodo de retención, vigencia o uso.

TITULO VI
PLAN DE CONTINGENCIA TECNOLÓGICA

CAPITULO I
ALCANCE Y CONTENIDO DEL PLAN DE CONTINGENCIA

Artículo 64: La Alta Gerencia del Ente Supervisado debe asegurar la existencia de un plan de contingencias tecnológicas aprobado, formalizado, actualizado, implementado y probado. El plan debe incluir como mínimo los siguientes aspectos:

a. Objetivo y alcance del plan definido.

b. Metodología empleada para su diseño.

c. Identificación de procesos críticos.

d. Clasificación de los sistemas, aplicaciones, software y equipos (críticos, vitales, sensitivos, etc.).

e. Prioridad y estrategia de recuperación que involucre cada plataforma de Tecnología de Información en la cual se almacenan y procesan las aplicaciones o datos que soporten una función critica del negocio.

f. Detalle de cada uno de los procedimientos definidos para la recuperación de operaciones criticas. Sobre este aspecto deberá considerarse el manejo de distintos escenarios para cada tipo de incidencia que pueda afectar el funcionamiento y operatividad del Ente supervisado.

g. Localización de los medios de respaldos, así como, del personal autorizado para accederlos.

h. Identificación del personal contacto por área y descripción de sus responsabilidades.

i. Niveles de escalamiento para el manejo y resolución de las fallas existentes o detectadas.

j. Recursos humanos, financieros y tecnológicos mínimos y necesarios para la recuperación de la operatividad el negocio.

k. Documentación asociada a los contratos o convenios realizados con terceros o proveedores externos de tecnología de información para apoyar el proceso de recuperación.

l. Establecimiento del período de recuperación critico para los recursos de información, en el cual debe restablecerse el procesamiento del negocio, antes de que se experimenten perdidas significativas o inaceptables.

Artículo 65: El Ente supervisado, debe contar con procedimientos documentados de respaldos y recuperación de la información en instalaciones distintas a las del centro de procesamiento de datos habitual. De igual forma, deberá contar con una planificación detallada de la cantidad, frecuencia, lugares apropiados de almacenamiento tanto internos como externos, inventarios detallados, responsables y la forma en la cual se administran los medios magnéticos. Estos procedimientos deben prever, como mínimo la generación de dos (2) copias de resguardo, manteniendo el almacenamiento de una (1) de ellas en un edificio ubicado a una distancia razonable del centro de procesamiento de datos.

Artículo 66: El Ente supervisado debe efectuar al menos un (1) simulacro anual del plan de contingencias tecnológicas, con resultado exitoso en todas sus dimensiones. En caso contrario, debe realizar las pruebas que sean necesarias hasta cumplir con los objetivos establecidos en el citado plan.

Esta prueba se realizará de acuerdo al cronograma que presente el Ente supervisado a esta Superintendencia, destacando que una vez que el plan esté implementado formalmente, debe participar el auditor interno del Ente supervisado. Los resultados de estas pruebas deberán estar disponibles para las inspecciones efectuadas por este Organismo.

De acuerdo al grado de complejidad en las operaciones y uso de las Tecnologías de Información en cada Ente supervisado esta Superintendencia, requerirá el cumplimiento, desarrollo y especificación mayor de cada uno de los puntos descritos en el plan de contingencias tecnológicas.

CAPITULO II
MANTENIMIENTO Y REEVALUACIÓN DEL PLAN DE CONTINGENCIAS TECNOLÓGICAS

Artículo 67: Para garantizar el mantenimiento y actualización de los planes de contingencias tecnológicas los mismos deben revisarse y actualizarse periódicamente para garantizar su eficacia permanente. Se deben incluir procedimientos en el programa de administración de cambios de la Organización para garantizar que se aborden adecuadamente los tópicos asociados a las contingencias tecnológicas.

En este sentido, debe asignarse a las unidades responsables de la tecnología del Ente supervisado la responsabilidad de las revisiones periódicas del plan de contingencias tecnológicas, la identificación de

cambios en las disposiciones relativas al negocio aún no reflejadas en dicho plan en aras de asegurar la adecuada y oportuna actualización del mencionado plan.

TITULO VII
MANTENIMIENTO E IMPLANTACIÓN DE LOS SISTEMAS DE INFORMACIÓN

CAPITULO I
MODELO DE LA ARQUITECTURA DE INFORMACIÓN, DICCIONARIO DE DATOS Y REGLAS DE SINTAXIS DE DATOS

Artículo 68: La información almacenada en los sistemas de información deberá ser consistente con las necesidades del Ente supervisado y debe ser identificada, capturada y comunicada en la forma y dentro de períodos que permitan a los responsables llevar a cabo sus tareas. Asimismo, la función de sistemas de información deberá crear y actualizar regularmente un modelo de arquitectura de información, abarcando los modelos de datos corporativos y los sistemas de información asociados. El modelo de arquitectura de información deberá ser consistente con el plan a largo plazo definido por el área de Tecnología de Información.

Artículo 69: La función de servicios de tecnología de la información del Ente supervisado, debe asegurar la creación y la continua actualización de un diccionario de datos corporativo que incorpore las reglas de sintaxis de datos de la Institución.

Artículo 70: El Ente supervisado, debe establecer políticas y procedimientos para el diseño, desarrollo e implantación de sistemas de información eficaces, seguros y que impidan modificaciones no autorizadas. Asimismo, será necesario que estos se ajusten al cumplimiento de las leyes, reglamentos y las normativas vigentes aplicables. En este sentido, la Institución debe:

a. Implementar una metodología para el ciclo de vida del desarrollo de sistemas de información, que asegure su calidad y satisfaga los requerimientos del usuario. Para ello, será necesario asegurar la funcionalidad del sistema desarrollado o modificado y garantizar que este sea revisado y aprobado por las unidades funcionales usuarias afectadas y la Alta Gerencia.

b. Definir áreas y recursos que permitan una adecuada separación de los ambientes de trabajo computacionales, comúnmente denominados desarrollo, pruebas o calidad y producción, así como, la restricción de acceso al personal de desarrollo, mantenimiento de sistemas y operaciones al ambiente de producción.

c. Establecer procedimientos de control de cambios de los programas asociados a los sistemas de información productivos, que permitan su adecuada transferencia, así como la de archivos, estructuras de datos, definiciones de diccionario de datos, órdenes de ejecución de programas, entre otros aspectos.

Artículo 71: La puesta en producción de programas, archivos o estructuras de datos debe ser realizada por personal que no tenga vinculación alguna con el área de desarrollo y mantenimiento de sistemas. En este sentido, deberán definirse procedimientos automatizados que aseguren la correspondencia entre los programas "fuentes" y "ejecutables". Se destaca que estos procedimientos deben encontrarse debidamente documentados y contar con los manuales correspondientes al área de operaciones.

Artículo 72: El Ente supervisado debe definir políticas y procedimientos relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, de tal forma que sea posible asegurar que permanezcan completos, precisos y válidos

Artículo 73: El Ente supervisado debe mantener actualizada la documentación técnica que contenga como mínimo los siguientes aspectos: objetivos, alcances, diagrama del sistema, registro de modificaciones, lenguaje de programación, manejador de las bases de datos empleados, descripción del hardware y software, su interrelación, interconexión o interfase con otras aplicaciones o rutinas, descripción de las pantallas que permiten la modificación directa de datos de producción (cambios de parámetros, fórmulas, tasas, datos, entre otros aspectos).

CAPITULO II
CONTROL DE ACCESO A LAS BIBLIOTECAS QUE ALMACENAN LOS PROGRAMAS FUENTES

Artículo 74: El Ente supervisado debe mantener un control estricto sobre el acceso a las bibliotecas que almacenan los programas fuentes, considerando como mínimo los siguientes aspectos:

a. Las bibliotecas de programas fuentes no deben encontrarse almacenadas en el mismo ambiente en el cual residen los sistemas productivos de la Institución.

b. Se deberá designar a un bibliotecario que se responsabilice por la administración de los programas fuentes de las aplicaciones, destacando que este proceso podrá ser automatizado, para lo cual deberán generarse las pistas de auditoria pertinentes.

c. El acceso a las bibliotecas que almacenan los programas fuentes por parte del personal de Tecnología de Información debe ser limitado, destacando que deberán documentarse las actividades que se ejecutarán sobre las citadas librerías, así como, el cargo del personal que podrá acceder a ellas.

d. Los programas en desarrollo o mantenimiento no deben ser almacenados en las bibliotecas de los programas fuentes, mientras no son certificada y aprobada su funcionalidad y operatividad.

e. La actualización de las bibliotecas de programas fuentes y la distribución de éstos a los programadores, sólo debe ser ejecutada por el bibliotecario designado, con la autorización de la máxima autoridad a la cual reporta la cual debe estar adscrita a Tecnología de Información.

f. Los listados de programas deben ser almacenados en un ambiente seguro, preferiblemente en las bibliotecas definidas para tal fin.

g. Mantener un registro de auditoria de todos los accesos a las bibliotecas que almacenan los programas fuentes.

h. Las antiguas versiones de los programas fuentes deben ser archivadas con una clara indicación de las fechas en las cuales se encontraban operativos, indicando además el software de soporte, el control de tareas, las definiciones de datos, entre otros aspectos.

i. El mantenimiento y la copia de las bibliotecas de los programas fuente deben estar sujeta a estrictos procedimientos de control de cambios.

CAPITULO III
DESARROLLO EXTERNO DE SOFTWARE.

Artículo 75: Cuando se tercea riza el desarrollo de software, se deben considerar los siguientes aspectos:

a. Establecer formalmente los acuerdos asociados al uso de licencias, propiedad de códigos y derechos de propiedad intelectual.

b. Certificación de la calidad y precisión del trabajo efectuado.

c. Definición de acuerdos de custodia de los programas fuentes que permitan a la Institución mitigar los riesgos de dependencia o continuidad de operaciones, en caso de quiebra del proveedor externo de tecnología de información.

d. Los derechos por parte de la Institución a realizar auditorias de la calidad y precisión del trabajo requerido y realizado.

e. Establecimiento de los requerimientos contractuales con respecto a la calidad del código.

f. Realización de pruebas previas a la instalación para detectar códigos troyanos, bombas lógicas, entre otros.

g. Suministro de la documentación del diagrama de entidad / relación, así como, manuales de especificaciones técnicas, de instalación y de usuarios finales.

h. La restricción de accesos al ambiente productivo por parte del proveedor del software o cualquier otro al cual se contraten sus servicios.

Artículo 76: Debe existir un comité técnico que supervise los procesos de control de cambio ejecutados en el Ente supervisado. Éste deberá estar conformado como mínimo por el personal supervisorio de las áreas de desarrollo o mantenimiento de sistemas, planificación y producción, así como, de auditoria y de seguridad de la información.

Por otra parte, el referido comité deberá asegurar que los procesos de control de cambio y pases de programas a producción sean ejecutados por un área distinta al que los desarrolló.

Este comité tendrá como objetivo principal la evaluación de las solicitudes de incorporación de nuevos programas, procesos o equipos al ambiente productivo de la Institución, así como, las implantaciones que demandan los proyectos y procesos de mantenimiento de la infraestructura existente, destacando que será necesario medir el impacto que cada caso puede generar sobre la continuidad operativa del negocio.

Artículo 77: La metodología del ciclo de vida de desarrollo de sistemas debe incluir normas asociadas al estudio de factibilidad de los requerimientos realizados y contemplar la formalidad en el procedimiento de respuesta al usuario respecto a la procedencia de su solicitud. Dicho estudio debe ser realizado por el comité técnico de control de cambio, con la finalidad de determinar la viabilidad presupuestaria, tecnológica y si el mismo está acorde con las necesidades del negocio.

Artículo 78: Si el requerimiento realizado a Tecnología de Información es procedente, se deberán formalizar los detalles, definir su alcance, las etapas que deberá contemplar y las fechas de inicio y culminación de cada una. Todos los acuerdos establecidos deben ser documentados y firmados, tanto por el personal que integra el comité, como el usuario en señal de aceptación.

Artículo 79: La máxima autoridad de Tecnología de Información debe asegurar que todos los requerimientos de cambios, mantenimiento de sistemas internos y aquellos provistos por terceros, están sujetos a procedimientos formales. Los cambios deben clasificarse, priorizarse y contar con procedimientos específicos para administrar urgencias.

Artículo 80: Una vez culminados los desarrollos requeridos deberán efectuarse pruebas unitarias e integrales, en la cual deben participar tanto el personal usuario como miembros del comité técnico de

control de cambio, con la finalidad de garantizar su adecuado funcionamiento y que se adaptan a los acuerdos establecidos. Finalizadas dichas pruebas en forma satisfactoria, las mismas deben ser documentadas y firmadas por los participantes en señal de conformidad y certificación.

CAPITULO IV
ADMINISTRACIÓN DE LAS BASES Y ESTRUCTURAS DE DATOS

Artículo 81: Los administradores de bases de datos son responsables de supervisar el uso de las estructuras, la conservación de los registros, la ejecución de funciones estadísticas, el control de acceso a las estructuras de datos y programas que pueden accederlas y cualquier otra función que involucre su monitoreo permanente.

Artículo 82: El administrador de base de datos debe asegurar el estricto cumplimiento de los requisitos de seguridad globales del sistema administrativo de las bases de datos, destacando que estos deben ser consistentes con las políticas establecidas y monitoreadas por la unidad de seguridad de los activos de información.

Artículo 83: Sólo el administrador de base de datos tiene la autoridad para hacer cambios a la biblioteca del sistema administrativo de bases de datos.

Artículo 84: El administrador de base de datos debe restringir la inclusión directa de datos en las estructuras sin la aprobación del área usuaria de la aplicación, auditoría y la unidad de seguridad de los activos de información, destacando que toda carga con las mencionadas características, deberá documentarse, justificarse y autorizarse por las unidades competentes.

Artículo 85: El administrador de base de datos deberá establecer procedimientos escritos para la recuperación de las bases y estructuras de datos, en caso de una destrucción total o parcial.

Por otra parte, deberá documentar los mecanismos de seguridad definidos para las estructuras de datos, la protección contra la destrucción accidental o deliberada, y de accesos no autorizados. Estos procedimientos deben incluir los accesos concurrentes al sistema y la forma de solucionar aquellos requerimientos conflictivos que causen incidentes adversos a los esperados. Se destaca que los procedimientos deberán ser revisados y avalados por el personal de auditoría de sistemas y la unidad de seguridad de los activos de información y custodiados adecuadamente a fin de evitar accesos irrestrictos.

Artículo 86: El administrador de bases de datos debe aprobar en conjunto con el comité de control de cambios todas las modificaciones mayores al software del sistema de administración de base de datos, de igual forma, deberá validar cualquier cambio y aceptar formalmente la incorporación de nuevas versiones.

Artículo 87: La Alta Gerencia de Tecnología de Información debe asegurar la existencia de controles y procedimientos especiales para prevenir el acceso a las bases de datos cuando no estén bajo el control del software del sistema de administración de base de datos. De igual forma, deberá controlar el acceso a la biblioteca del referido sistema y a cualquier otra documentación de los programas de utilería, aplicación de los usuarios u otro recurso.

Artículo 88: Se establecen como controles mínimos necesarios para asegurar la integridad de las bases de datos, los siguientes:

a. Definir normas para la definición, control, actualización y monitoreo de las bases y estructuras de datos, para lo cual deberán definirse mecanismos que aseguren su continuo cumplimiento.

b. Implementar con la frecuencia del caso, copias de seguridad de las estructuras y bases de datos, así como, los procedimientos de recuperación para asegurar la disponibilidad de la base de datos.

c. Establecer diferentes niveles de control de acceso para los rubros de datos, tablas y archivos a fin de prevenir ingresos inadvertidos o no autorizados a las citadas estructuras.

d. Asegurar que sólo el personal autorizado puede actualizar las bases de datos.

e. Establecer los controles para manejar los problemas de acceso concurrente.

f. Garantizar la corrección, integridad y consistencia de los elementos de los datos y de las relaciones en la base de datos.

g. Usar puntos de verificación de las bases de datos para reiniciar el procesamiento después de una falla del sistema en el flujo de trabajo que minimice la pérdida de datos y los esfuerzos de recuperación.

h. Efectuar la reorganización de las estructuras y base de datos, a fin de reducir el espacio de disco no usado y verificar las relaciones definidas.

i. Asegurar el cumplimiento de los procedimientos definidos para la reestructuración de las base de datos cuando se hagan los cambios lógicos, físicos y de procedimientos.

j. Emplear herramientas de monitoreo de desempeño de las estructuras y bases de datos para garantizar su eficiencia.

Artículo 89: Se deben implantar y monitorear continuamente los controles del software que es utilizado para limitar el acceso a las estructuras y bases de datos, específicamente aquellos asociados a:

a. Registrar las solicitudes de acceso para identificar la estación de trabajo, la hora y el operador o usuario que realizó la solicitud de ingreso.

b. Bloqueos de acceso de los usuarios a las estructuras y bases de datos que no son necesarios para el desempeño de sus funciones.

c. Limitar severamente los cambios y actualizaciones a los archivos de las bases de datos con respecto a diversos usuarios.

d. Registrar las transacciones de accesos y cambios para control, auditoria y recuperación.

e. Controlar severamente el acceso cuando se esta depurando o reorganizando el contenido de una estructura o base de datos, o cuando se sintetizan los datos.

a. Limitar la cantidad de personas que tienen acceso a las bases de datos de prueba.

Artículo 90: Asegurar que las bitácoras de las bases o estructuras de datos de las aplicaciones críticas contengan los siguientes registros:

a. Todos los datos borrados de las bases de datos.

b. Origen (interno o externo) de todas las transacciones.

c. Utilización de la base de datos por personas distintas a los usuarios que tienen accesos autorizados a la aplicación.

d. Violaciones de seguridad con respecto a las bases de datos.

e. Reorganizaciones o sintetizaciones de las bases de datos.

f. Uso de las utilerías de las bases de datos.

g. Estado del sistema que pueda ser requerido para reinicio o cambio de datos erróneos.

Artículo 91: La Alta Gerencia de Tecnología de Información debe asegurar la existencia de manuales de procedimientos e instrucciones de operación para todos los programas de aplicación que acceden a las estructuras y bases de datos.

Artículo 92: La Alta Gerencia de Tecnología de Información debe asegurar la existencia de documentación escrita que detalle los estándares de documentación para todos los programas de las aplicaciones desarrolladas (internas o externas). La mencionada documentación debe ser revisada con el administrador de base de datos antes de la puesta en producción del programa.

Por otra parte, deberán encontrarse documentados los estándares de prueba de programas que especifiquen criterios para generar datos de prueba para las bases de datos. Adicionalmente, deberán asegurar la revisión de los resultados generados y la retención de los mismos.

Artículo 93: El Ente supervisado debe garantizar la existencia de procedimientos escritos que delineen los procesos de respaldo y recuperación que deben usarse si fallan las bases de datos o si estas son destruidas parcial o totalmente.

Artículo 94: Sólo el personal autorizado del área de Tecnología de Información debe tener acceso al lugar en el cual se encuentran almacenados los archivos de las bases de datos. En este sentido, deberán definirse y documentarse claramente los cargos, las funciones y actividades que éste tendrá sobre las mencionadas estructuras.

Artículo 95: El diccionario de datos deberá ser empleado para mantener un control efectivo sobre todas las definiciones, así como, el rastreo de los datos a través de las aplicaciones que lo emplean.

Parágrafo Único

El administrador de base de datos es el responsable por el desarrollo y supervisión continua del diccionario de datos.

Artículo 96: El Ente supervisado debe asegurar que los procedimientos de recuperación y respaldo sean probados en los programas de la aplicación antes de su implementación. Estos procedimientos deben delinear la recuperación de las bases de datos y la de las transacciones, así como, el reinicio de los programas de la aplicación, el software del sistema, el control de las transacciones, del sistema operativo, entre otros aspectos. Esto involucra la recuperación de las bases de datos en sus interrelaciones con los programas específicos de la aplicación.

TITULO VIII
REDES
CAPITULO I
INFRAESTRUCTURA DE LAS REDES

Artículo 97: La Alta Gerencia de Tecnología de la Información debe asegurarse que los planes de adquisición de hardware y software reflejen las necesidades identificadas en el plan estratégico de Tecnología de la Información.

Artículo 98: Antes de la implantación de un nuevo hardware o software, el Ente supervisado debe evaluar el impacto de la implantación en los sistemas existentes para así minimizar cualquier interrupción de los sistemas de información como resultado del proceso realizado.

Artículo 99: Deben establecer procedimientos para la realización de pruebas al hardware o software instalado. Estos procedimientos deben incluir como mínimo las siguientes pruebas:

a. Unitarias e integrales.

b. De interfaz.

c. De capacidad.

d. De aceptación del usuario.

Artículo 100: Se deben realizar en forma semestral estudios de capacidad y desempeño del hardware y las líneas de comunicaciones que permitan determinar las necesidades de expansión de capacidades o actualizaciones de equipos en forma oportuna.

Artículo 101: Se deben establecer políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base, a fin de asegurar que proporcionen la plataforma tecnológica apropiada para soportar las aplicaciones relacionadas con las redes y comunicaciones y minimicen la frecuencia e impacto de las fallas de desempeño de las mismas.

CAPITULO II
ADMINISTRACIÓN Y CONTROLES DE LAS REDES

Artículo 102: Los administradores de redes en conjunto con el área de unidad de seguridad de los activos de información deben implementar controles para garantizar la protección de los servicios conectados contra el acceso no autorizado, en este sentido se debe considerar lo siguiente:

a. La responsabilidad operativa de las redes debe estar separada de aquellas asociadas a las operaciones del computador central.

b. Se deben establecer los procedimientos y responsabilidades para la administración de equipos remotos, incluyendo aquellos ubicados en las áreas usuarias y bajo custodia y/o administración de terceros o proveedores.

c. Definir y documentar los controles tendentes a salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, así como, mantener la disponibilidad de los servicios de red y computadoras conectadas.

Artículo 103: Establecer procedimientos de protección de los datos que se transmiten por la red de telecomunicaciones, mediante técnicas adecuadas de encriptación a través de equipos o aplicaciones definidas para tal fin.

Artículo 104: Se debe contar con un sistema o aplicación que permita establecer una adecuada seguridad

para los accesos a las redes, los cambios a su sistema operativo y el monitoreo de las actividades que se desarrollan en ellas.

Artículo 105: Administrar adecuadamente las redes y las líneas de comunicaciones. En este sentido, se deben establecer los procedimientos que aseguren que las redes instaladas de voz y/o datos cumplan con los requerimientos mínimos vigentes del cableado estructurado.

CAPITULO III
REGISTRO DE USUARIOS Y POLÍTICA DE UTILIZACIÓN DE LOS SERVICIOS DE RED.

Artículo 106: Asegurar la existencia de un procedimiento formal de registro y eliminación de usuarios para otorgar accesos a todos los sistemas y servicios de información multi-usuario existentes, el cual debe incluir los siguientes aspectos:

a. Utilizar identificaciones de usuario únicos de forma tal que se sea posible vincularlos y hacer responsables a estos por sus acciones.

b. Verificar que el usuario tenga la autorización del propietario del sistema para su uso.

c. Asegurar que el nivel de acceso otorgado es adecuado para el propósito del negocio, es coherente con la política de seguridad de la organización y consistente con las funciones asociadas al cargo que desempeña.

d. Entregar a los usuarios un detalle escrito de sus derechos de acceso.

e. Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso.

f. Garantizar que a los proveedores de servicios no se otorgan accesos a aplicaciones, sistemas o equipos críticos hasta que se hayan completado los procedimientos de autorización definidos para tal fin.

g. Mantener un registro formal de todas las personas autorizadas para utilizar el servicio.

h. Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización.

i. Verificar periódicamente y cancelar las cuentas de usuarios redundantes o egresados de la Institución.

Artículo 107: Limitar y controlar la asignación y uso de privilegios especiales o cualquier servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones. Para ello, se estima necesario considerar los siguientes aspectos:

a. Deben identificarse los privilegios asociados a cada producto del sistema y las categorías o nivel de cargo del personal a los cuales deben asignarse los productos.

b. Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso.

c. Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización definido para tal fin.

d. Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

e. Los privilegios deben asignarse a una identidad de usuario diferente de aquellas utilizadas en las actividades comerciales normales.

Artículo 108: Los usuarios sólo deben contar con acceso directo a los servicios para los cuales han sido expresamente autorizados, para ello deberá formularse una política concerniente al uso de redes y servicios de red. Esta debe comprender como mínimo:

a. Las redes y servicios de red a los cuales se permite el acceso.

b. Procedimientos de autorización para determinar las personas, las redes y los servicios de red a los cuales tienen permitido el acceso.

c. Controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

CAPITULO IV
PROTECCIÓN DE LOS PUERTOS DE DIAGNOSTICO REMOTO

Artículo 109: El acceso a los puertos de diagnóstico debe ser controlado de manera segura por un mecanismo de seguridad apropiado y un procedimiento que garantice que sólo son accesibles mediante un acuerdo formal y documentado que justifique el ingreso por parte del personal de soporte de hardware y software.

Artículo 110: Los especialistas de redes en conjunto con el área de unidad de seguridad de los activos de información, deben establecer las políticas de control de acceso para redes compartidas, especialmente aquellas que se extiendan más allá de los límites de la Institución. Dichos controles deben implementarse mediante equipos o software de red que filtren el tráfico por medio de reglas o tablas previamente definidas. Las restricciones aplicadas deben basarse en la política y los requerimientos de acceso de las aplicaciones del Ente supervisado y deben mantenerse y actualizarse de conformidad a lo expresamente establecido en la norma definida para tal fin. En este sentido, deben considerarse restricciones para:

a. Correo electrónico.

b. Transferencia unidireccional de archivos.

c. Transferencia de archivos en ambas direcciones.

d. Acceso interactivo.

e. Acceso de red vinculado a hora o fecha.

TITULO IX
INFRAESTRUCTURA DE LAS TELECOMUNICACIONES

Artículo 111: La administración del sistema de cableado de telecomunicaciones incluye la documentación, terminación de los cables y certificación, paneles de patcheo, armarios de telecomunicaciones y otros espacios ocupados por el sistema.

Artículo 112: Conforme a lo establecido por la norma ANSI/EIA/TIA-606, se considera necesario marcar

con el código de color que a continuación se detalla, los cables de telecomunicaciones empleados para su debida identificación:

a. Color Naranja: Terminación central de oficina.

b. Color Verde: Conexión de red / circuito auxiliar.

c. Color púrpura: Conexión mayor / equipo de datos.

d. Color Blanco: Terminación de cable MC (conector de cruzado principal) a IC (conector de cruzado intermedio).

e. Color Gris: Terminación de cable IC (conector de cruzado intermedio) a MC (conector de cruzado principal).

f. Color Azul: Terminación de cable horizontal.

g. Color Marrón: Terminación del cable del campo.

h. Color Amarillo: Mantenimiento auxiliar, alarmas y seguridad.

i. Color Rojo: sistema telefónico.

Artículo 113: El área o cuarto de telecomunicaciones debe ser empleado únicamente para ubicar el equipo asociado con el sistema de cableado, destacando que no debe ser compartido con instalaciones eléctricas distintas al equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado, destacando que esta zona debe mantenerse libre de contactos e instalaciones en mal estado. Pueden incorporarse otros sistemas de información del edificio como alarmas, seguridad audio y de telecomunicaciones.

Artículo 114: En los cuartos de telecomunicaciones será necesario el uso de paneles de patcheo para terminar el cableado telefónico y el horizontal, implementando las cruzadas de patcheo (también llamadas patch cords).

Artículo 115: Se debe evitar el polvo y la electricidad estática, utilizando piso de concreto, terrazo, loza o similar en los cuartos de telecomunicaciones. La temperatura y la humedad relativa deben ser las recomendadas para este tipo de instalaciones. Por otra parte, debe evitarse el uso de cielos falsos estar libres de amenazas de inundación.

Artículo 116: Los equipos activos de la red como switches, concentradores, multiplexores, puentes, enrrutadores, conmutadores y componentes del cableado estructurado deberán instalarse sobre los muebles (rack) de comunicaciones.

Artículo 117: La documentación técnica asociada a la infraestructura de telecomunicaciones deberá contemplar como mínimo los siguientes aspectos:

a. Diagrama lógico de la red.

b. Descripción de los elementos de cableado.

c. Planos de trayectoria del cableado y ubicación de puntos de salida.

d. Diagrama del sistema de parcheo, distribución de regletas y salidas.

e. Informe de certificación del cableado estructurado, con su respectivo diagrama de conectividad, apegado a lo establecido en las normas TIA/EIA/568B.

Artículo 118: En el sistema de cableado estructurado se deberá considerar el uso de cables y conectores que ofrezcan prestaciones iguales o superiores a las especificadas para la categoría 5. Por otra parte, el cableado debe estar debidamente protegido por canaletas, así como, identificado o etiquetado y separado de los cables de electricidad.

Artículo 119: La estructura del cableado estructurado debe permitir un crecimiento continuo sin alterar los niveles de servicio ofrecidos, es decir, que las salidas del sistema de cableado se deben incrementar sin interrupciones en el servicio.

Artículo 120: Los componentes de tubería deberán ser galvanizados, con un diámetro que garantice el cuarenta por ciento (40%) de espacio libre en el interior del tubo para instalaciones futuras. Dicha tubería debe quedar aterrizada eléctricamente.

Artículo 121: Todo el sistema de tubería deberá quedar acoplado, utilizando los componentes requeridos para ello (curvas, conectores, cajas de paso, entre otros).

Artículo 122: Se deberán emplear como mínimo las herramientas que a continuación se detallan para monitorear la red de telecomunicaciones:

a. Reportes de Tiempo Improductivo (downtime): los cuales tienen como objetivo rastrear la disponibilidad de líneas y circuitos de comunicación. En este reporte se deberán identificar las interrupciones debidas a falta de energía, carga excesiva del tráfico, error del operador o posible intercepción de transmisiones.

b. Monitores en Línea: son comúnmente empleados para medir las transmisiones de telecomunicaciones y determinan si esta se encuentran correctas y completas.

c. Analizadores de protocolo: permiten diagnosticar la actividad de la red que monitorean y registran la información de administración de la red a partir de los paquetes que viajan en el enlace al cual esta conectado el analizador.

TITULO X
BANCA VIRTUAL

CAPITULO I
ADMINISTRACIÓN Y CONTROL DEL SERVICIO DE BANCA VIRTUAL

Artículo 123: El Ente supervisado, previa notificación a la Superintendencia de Bancos, podrá brindar, a través de la banca virtual, los siguientes servicios:

a. Preguntas y consultas de cuentas, balances y tarifas bancarias.

b. Historial de transacciones.

c. Enviar o recibir mensajes del Banco.

d. Acceso a información personal del cliente, de tal manera que pueda ser modificada y actualizada.

e. Consulta de las transacciones efectuadas en los diversos productos mantenidos por la Institución.

f. Pagos a cuentas de préstamos, cuentas de tarjetas de crédito y servicios públicos.

g. Realizar pagos a ciertas entidades privadas que sean designadas por la Institución, previa solicitud del cliente.

h. Traspaso de fondos entre cuentas de la propia Institución y de otros bancos o instituciones financieras.

i. Reportar pérdida de tarjetas de crédito o débito emitidas por la Institución.

j. Solicitudes de aprobación de Préstamos.

k. El ente supervisado podrá, previa autorización de la SUDEBAN, incorporar otros servicios adicionales.

Artículo 124: La Junta Directiva debe asegurarse de integrar al manual de operaciones del Ente supervisado, los procedimientos, políticas y controles internos que garantice el mantenimiento de una estructura administrativa y operativa adecuada para ofrecer el servicio de banca virtual, considerando los siguientes aspectos:

a. Naturaleza de las transacciones u operaciones bancarias ofrecidas.

b. Sistema de registro de las transacciones u operaciones.

c. Mecanismos definidos para la supervisión de los riesgos asociados con las actividades de la banca virtual y el establecimiento de políticas y controles para administrar los riesgos asociados.

d. Procedimientos, equipos, sistemas, aplicaciones y dispositivos de seguridad implementados para asegurar la protección interna y externa, aplicables en caso de amenazas potenciales.

e. Acciones de monitoreo y vigilancia de las relaciones externas (incluyendo terceros y proveedores) que brinden servicios al sistema de banca virtual.

Artículo 125: La unidad de administración integral de riesgos existente en la Institución, deberá tener entre sus funciones la identificación, medición, monitoreo y control de los riesgos asociados al servicio de banca virtual, considerando como mínimo los siguientes aspectos:

a. La integración de los planes de desarrollo de banca virtual dentro de los objetivos estratégicos de la Institución.

b. La exposición manifiesta de los riesgos clásicos relacionados con el ambiente de tecnología de la información.

c. Procesos de planeación e implementación para el uso de la tecnología asociada al servicio.

d. Identificar y establecer los riesgos existentes, así como, controlar su evolución a medida que se incorporen a la Institución aspectos tecnológicos.

Artículo 126: La unidad de auditoria de sistemas del Ente supervisado, deberá efectuar revisiones periódicas para la evaluación y seguimiento permanente de la función y operación de los servicios de banca virtual, razón por la cual deberá contar con personal con suficiente experticia técnica para evaluar las amenazas de seguridad y controles asociados al ambiente, así como, programas actualizados para la ejecución de sus funciones.

El Ente supervisado, podrá contratar los servicios de empresas para realizar evaluaciones técnicas o auditorias de las operaciones de la banca virtual manteniendo la adecuada independencia entre los servicios de ésta y la Institución.

Artículo 127: El Ente supervisado deberá informar al cliente de la banca virtual sobre las características, condiciones, costo y cualquier otra estipulación determinante que conlleve el uso del servicio. Asimismo, el Ente deberá remitir la confirmación de la ejecución de las operaciones efectuadas por el cliente a través del servicio de banca.

En este sentido, se debe incluir en su sitio de Internet en el que opera la Banca Virtual, así como en el contrato, por lo menos lo siguientes aspectos:

a. Identidad y dirección del Ente supervisado.

b. La descripción de las principales características del servicio.

c. Las características especiales de cada producto.

d. Modalidades de ejecución de las transacciones, plazo de validez de la oferta.

e. Forma de pago.

f. Costo de la prestación de servicio a través del medio electrónico.

g. Costo de la prestación de servicio a través del medio electrónico.

h. Políticas de seguridad, privacidad y responsabilidad del cliente en su uso (esto incluye acuerdos de seguridad).

i. Constancia de la aceptación del contrato de banca virtual, sin que esto conlleve la firma convencional. Es imprescindible se incorpore un enlace destacado o “link” a las condiciones generales para que su existencia resulte manifiesta y sean fácilmente accesibles en la pantalla y puedan ser reproducidas a través de cualquier mecanismo de impresión disponible por el cliente.

CAPITULO II
MECANISMOS DE CONTABILIZACIÓN Y REGISTRO DE TRANSACCIONES

Artículo 128: La Institución que ofrezca el servicio de banca virtual mantendrá una bitácora de acceso y de uso del sistema que permita registrar las transacciones bancarias y autenticaciones que realiza el cliente, la cual estará a disposición de este Organismo y conservará, por cualquier medio autorizado por Ley, por un período de tiempo no inferior a cinco (5) años, contados a partir de la fecha de la transacción.

De igual manera, la Institución debe contar con mecanismos que garanticen la custodia de dichos datos y la recuperación de la actividad procesada por la aplicación manteniendo una asociación entre la transacción de banca virtual y la persona que la ejecutó.

CAPITULO III
SEGURIDAD DEL SERVICIO DE BANCA VIRTUAL

Artículo 129: La unidad de seguridad de los activos de información del Ente supervisado, deberá establecer mecanismos de control que permitan alertar las fallas y minimizar las vulnerabilidades que la plataforma tecnológica que soporta los servicios de banca virtual pueda presentar, considerando como mínimo:

a. Definición de controles de acceso lógicos a datos, sistemas, aplicaciones, software, utilitarios, líneas de comunicaciones, librerías, entre otros.

b. Existencia de mecanismos cortafuegos (firewalls) para mediar entre la red pública, Internet y la red privada del Ente supervisado, a fin de garantizar la no intromisión cuando estas se evidencien.

c. Protección contra virus y monitoreo y acciones correctivas sobre cualquier actividad asociada a delitos informáticos en el ambiente de banca virtual y sus redes privadas de soporte (denegación del servicio, plagio, usurpación o adulteración de identidad, captura de información personal, financiera y privada del cliente, entre otros aspectos).

d. Inhabilitación de servicios innecesarios en el servidor de aplicación de la banca virtual, tales como: Protocolo de Transferencia de Archivo (FTP - File Transfer Protocol), Telnet.

e. Utilización de tecnologías de seguridad para implementar el servicio de la banca virtual, tales como: Infraestructura de Claves Públicas (PKI – Public Key Infraestructura), Protocolos SSL (Secure Sockets Layer), TLS (Transport Layer Security), IPSec, SET.

f. Uso de herramientas que permitan el monitoreo de los sistemas y las redes para detectar intrusos o prevenir ataques.

g. Manejo de precauciones para emplear los enlaces de telecomunicación a través de redes privadas virtuales y técnicas de encriptación relacionadas.

h. Revisión periódica de la infraestructura y políticas de seguridad de la Institución con el fin de optimizar las mismas basadas en la propia experiencia de la Institución y sus cambios tecnológicos.

i. Reforzamiento de los controles de acceso físico.

j. Infraestructura apropiada para la ejecución de respaldos de la data, la cual debe ser probada periódicamente.

k. Mecanismos que garanticen la disponibilidad del servicio.

l. Planes apropiados de respuesta a incidentes que incluyan estrategias de comunicación que aseguren la continuidad del servicio y responsabilidad limitada asociada con interrupciones del servicio de banca virtual incluyendo aquellos originados desde sistemas externos.

m. Definición e implantación de procedimientos y controles que brinden una adecuada seguridad en las aplicaciones de banca virtual: control de cambios y/o modificaciones, separación de ambientes de prueba.

Artículo 130: Se debe garantizar la autenticidad, la integridad, la confidencialidad y el no repudio o rechazo de las transacciones; así como, asegurar una adecuada segregación de responsabilidades y controles de autorización. En este sentido, se deben considerar como mínimo los siguientes aspectos:

a. Métodos para la verificación de la identidad y autorización de los nuevos clientes o aquellos ya existentes que deseen iniciar transacciones a través de los servicios de banca virtual.

b. Establecimiento de medidas para preservar la confidencialidad y seguridad de la información relevante de la Institución, las cuales deben estar acordes con la sensibilidad de la información transmitida y/o guardada en sus bases de datos.

c. Técnicas que ayuden a establecer el no repudio o rechazo de la transacción.

d. Segregación adecuada de responsabilidades y medidas de control interno que puedan reducir el riesgo de fraude en procesos y sistemas operacionales y asegurar que las transacciones estén autorizadas, registradas y salvaguardadas apropiadamente.

e. Establecimiento de medidas que aseguren la exactitud, culminación y confianza de las transacciones, registros de información asociados a banca virtual que puedan ser transmitidas a través de Internet, ya sea en bases de datos internas de la Institución o guardadas por proveedores externos al servicio del Banco.

f. Uso de técnicas de control apropiadas, tales como criptografía, protocolos específicos u otros que permitan garantizar la privacidad y confidencialidad de la información del cliente

Artículo 131: El Ente supervisado debe tomar las medidas apropiadas para informar a los clientes del servicio de banca virtual sobre el manejo de la seguridad y privacidad de la información. Para tal propósito se deben aplicar, al menos, las siguientes medidas:

a. Informar a los clientes, en forma clara, las políticas de seguridad empleadas por la Institución en su servicio de banca virtual.

b. Instruir a los clientes sobre la necesidad de proteger su clave secreta, número de identificación personal y cualquier información bancaria y personal.

TITULO XI

DISPOSICIONES FINALES

CAPITULO I

SUMINISTRO DE INFORMACIÓN ASOCIADA AL USO DE LA TECNOLOGÍA DE INFORMACIÓN

Articulo 132: El Ente supervisado deberá, conforme a lo establecido en el articulo 251 del Decreto con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras, suministrar en la forma y plazo que este Organismo lo establezca, la información requerida y relacionada con las aplicaciones, sistemas de información, infraestructura de telecomunicaciones, seguridad, programas y equipos empleados por las Instituciones sometidas a su control, fiscalización y regulación.

CAPITULO II

FORMACIÓN DE TALENTO HUMANO, ACTIVIDADES DE INVESTIGACIÓN Y DESARROLLO ASOCIADAS A LA TECNOLOGÍA DE INFORMACIÓN

Articulo 133: El Ente supervisado deberá definir mecanismos que aseguren el cumplimiento de lo establecido en el artículo 28 de la Ley Orgánica de Ciencia, Tecnología e Innovación, destacando que este Organismo definirá los procedimientos que estime necesarios para garantizar la formación de talento humano, actividades de investigación y desarrollo a ser realizadas en el país, en áreas relacionadas con el objeto de su actividad, considerando para ello el porcentaje establecido en la mencionada ley.

CAPITULO III
USO DE SISTEMAS DE REGISTRO, CONTROL Y MONITOREO DE RECLAMOS EFECTUADOS POR CLIENTES POR EL INADECUADO FUNCIONAMIENTO, DELITOS, FALLAS O DESPERFECTOS EN LOS CANALES ELECTRÓNICOS

Articulo 134: El Ente supervisado deberá mantener sistemas de información que faculten el registro, control y seguimiento electrónico de cada una de las instancias manejadas por la Institución para procesar efectivamente los reclamos realizados por los usuarios del Sistema Bancario Nacional por el inadecuado funcionamiento, delitos, fallas o desperfectos presentados en el funcionamiento u operatividad de los servicios, sistemas o equipos que constituyen los canales electrónicos.

En este sentido, deberán asegurar el cumplimiento de lo establecido en el artículo 43 del Decreto con Fuerza de Ley de Reforma de Ley General de Bancos y Otras Instituciones Financieras.