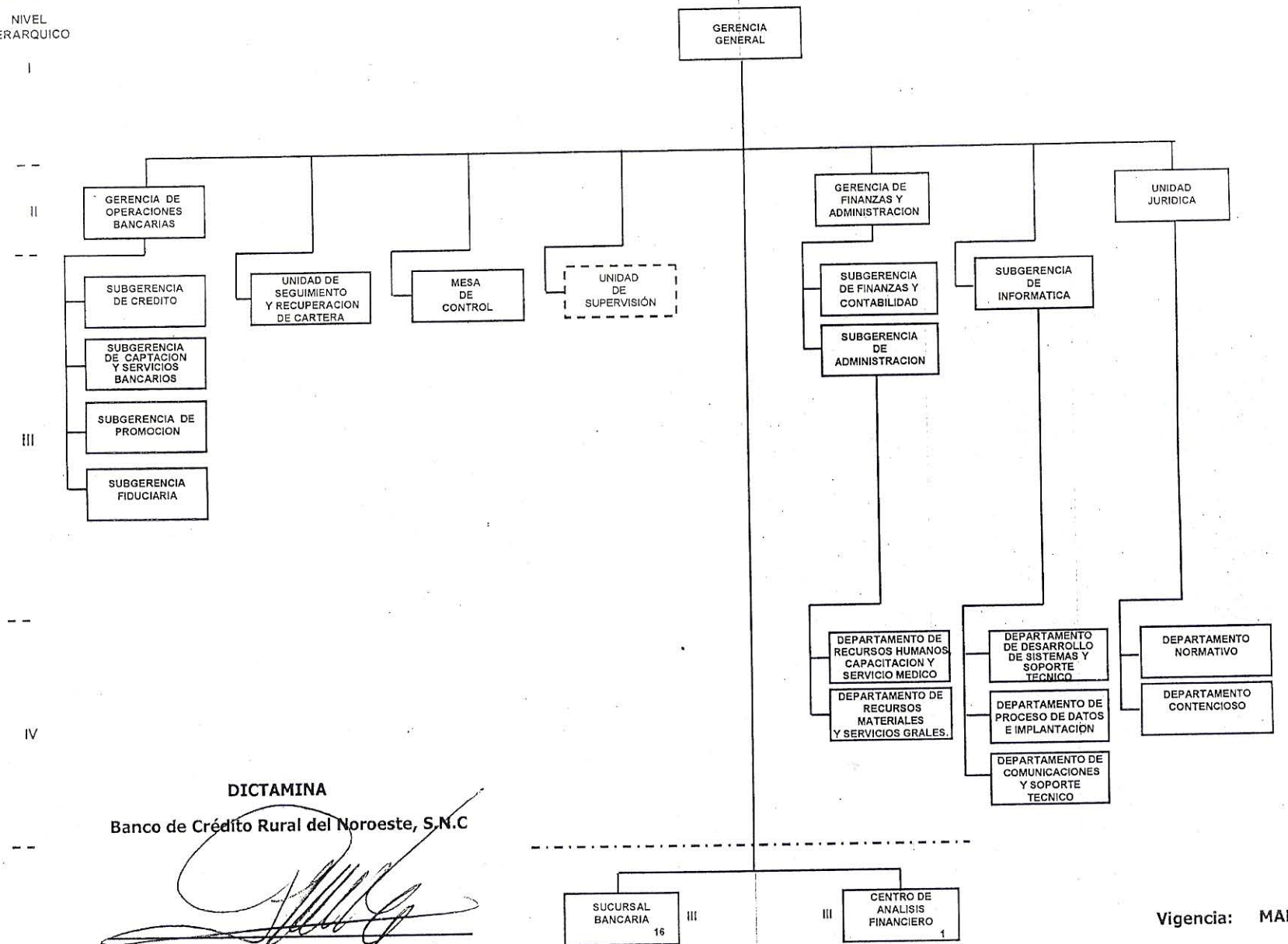
BANCO DE CRÉDITO RURAL DEL NOROESTE, S.N.C



DICTAMINA

Banco de Crédito Rural del Noroeste, S.N.C

Gerente General
Dr. Gonzalo de la Fuente Escobar

NOTA: NO SE CONSIDERA LA ESTRUCTURA DEL OIC

Vigencia: MARZO DE 2003

Políticas en Informática del Sistema BANRURAL

Dirección Adjunta de Planeación Estratégica

Dirección de Informática

Marzo 2002

CONTENIDO

I.- INTRODUCCIÓN

Los bienes informáticos en nuestra Institución son una herramienta de la mas alta importancia para alcanzar y mantener una óptima competitividad bancaria, por lo que es necesario instrumentar las políticas que permitan fomentar el orden, compatibilidad y estandarización de sistemas y equipos, ante los constantes y rápidos cambios tecnológicos que surgen día con día, así como racionalizar la asignación, operación y uso de bienes y productos de esta naturaleza.

Así mismo se pretende que los usuarios de los bienes y productos informáticos y el personal en general, conozcan los lineamientos Institucionales emitidos en esta materia, que orientan su trabajo cotidiano en las mejores condiciones y que les permitan administrar, controlar, operar y aprovechar los recursos más eficientemente.

Estas políticas serán actualizadas periódicamente como apoyo a la eficiente solución de los problemas de carácter informático del Sistema BANRURAL, por lo que se requiere que las observaciones y/o sugerencias sobre este tema sean enviadas a la Dirección de Informática, con el fin de mantener vigente este documento.

El incumplimiento del contenido del presente documento será sancionado en base a lo estipulado en la Ley Federal de Responsabilidades de los Servidores Públicos en razón de la gravedad de la falta.

II.- OBJETIVO

Orientar y conducir las actividades en materia de informática y telecomunicaciones, mediante el establecimiento e implantación de políticas que permitan consolidar la integralidad de los sistemas, estandarizar los equipos y el software, asegurar la legalidad en el uso de estas herramientas, salvaguardar los equipos, programas y productos, aplicar las medidas de seguridad y garantizar la confidencialidad de los procesos de información.

III.- POLÍTICAS GENERALES

a) En Materia de Informática para el Sistema BANRURAL.

Planes y Programas.

La Dirección de Informática propondrá a las autoridades institucionales; a través de la Dirección Adjunta de Planeación Estratégica, los Planes y el Programa de Desarrollo Informático y verificará en forma coordinada con sus áreas homologas, su cumplimiento en las instancias que conforman el Sistema BANRURAL.

El Programa de adquisición de bienes informáticos para los Regionales, deberá elaborarse en coordinación y acorde con los planes presentados por la Dirección de Informática, a fin de homologar y mantener sistemas y equipos homogéneos en el Sistema BANRURAL.

Los proyectos específicos que surjan en los Regionales, también deberán incorporarse al plan general para darles seguimiento, evaluar su desempeño y en su caso implantarlos en los Bancos del sistema.

La información, sistemas, equipos y software deberán estar en conocimiento y disposición de las áreas del Sistema BANRURAL que lo requieran, sujetándose a las condiciones de seguridad y confidencialidad establecidas para cada caso.

El control de los bienes institucionales corresponderá al área de Recursos Materiales y Servicios Generales.

Presupuestación.

La Subdirección Corporativa de Programación y Presupuesto y la Dirección de Informática, enviarán a los Regionales los lineamientos a seguir, para que los presupuestos en materia de informática del Sistema BANRURAL sean congruentes con los planes y el Programa de Desarrollo Informático.

Los Bancos del Sistema BANRURAL deberán integrar su programa de adquisiciones de bienes informáticos y gasto corriente para cada año calendario, mismo que será elaborado en coordinación con la Dirección de Informática.

De igual forma deberán efectuar provisiones presupuestales para la adquisición de bienes y servicios de informática de acuerdo a las fechas y características que se establezcan para el proceso general de programación presupuestación. Dichas provisiones deberán acompañarse de una justificación que explique las funciones específicas a las que se destinarán los bienes y servicios, así como el nivel de uso y explotación del equipo; respondiendo a las necesidades específicas de cada área de acuerdo a las funciones que se deban desempeñar para cumplir con los objetivos que como Institución tiene el Sistema BANRURAL.

La Dirección Adjunta de Planeación Estratégica a través de la Dirección de Informática, dictaminará los bienes que se pretendan adquirir, su número y montos presupuestados, en razón de las prioridades establecidas en los planes y programas de desarrollo informático de la Institución.

Recursos Humanos.

Es responsabilidad de la Subdirecciones Corporativas de Recursos Humanos y Servicio Medico y de la Dirección de Informática y de sus áreas homólogas en los Regionales, la selección y contratación del personal competente para cumplir con la labor informática, así como proporcionar los cursos de capacitación para mantenerlos actualizados.

Estructura Organizacional.

Será responsabilidad de la Dirección Adjunta de Planeación Estratégica, en conjunto con la Dirección de Informática y la Subgerencia de Informática, revisar su estructura de puestos y los perfiles de estos periódicamente, proponiendo los ajustes necesarios para el mejor desarrollo de las funciones encomendadas.

En el caso de las Subgerencias de Informática de los Regionales, las propuestas serán enviadas a la Dirección de Informática, para su evaluación.

b) Para la Administración de los Bienes Informáticos.

Control y Evaluación.

El control de los equipos informáticos así como el desarrollo y explotación de los sistemas aplicativos y de los procesos que se efectúan para su utilización, se regirán conforme a los lineamientos específicos que establezca y dé a conocer la Dirección de Informática en conjunto con la Subdirección de Recursos Materiales y Servicios Generales.

Actualización Tecnológica.

Queda bajo la responsabilidad de la Dirección de Informática y de las Subgerencias de Informática en Regionales en conjuntos con las Áreas de Recursos Humanos, Capacitación y Servicio Medico, establecer los mecanismos que garanticen la formación y actualización tecnológica del personal, en materia de informática, procurando contar con recursos capacitados para resolver las situaciones que se presentan.

Divulgación Técnica.

La Dirección de Informática en colaboración con la Dirección de Comunicación Social, divulgará boletines y notas técnicas que permitan aprovechar ampliamente los recursos informáticos, quedando dicho material a disposición de los usuarios.

Las Políticas en Informática del Sistema BANRURAL, deberán implementarse y acatarse por toda la Institución.

IV.- POLÍTICAS ESPECÍFICAS

IV.1.- Administración de la Configuración

Identificación de la Configuración Inicial

Las siguientes son responsabilidades de la Dirección de Informática:

- La identificación de la configuración inicial deberá contener toda aquella información mínima indispensable para que los equipos estén en posibilidades de reiniciar operaciones en caso de falla o siniestro.

- La identificación de los componentes originales deberá formar parte de esta configuración inicial. Esta deberá existir antes de que se efectúe cualquier modificación posterior a la misma.

- Esta identificación deberá contener un descriptivo de los componentes y su función dentro de la configuración, de manera que se tenga un marco de referencia para conocer su evolución en cada uno de sus componentes a lo largo de su ciclo de vida.

- Las Memorias Técnicas deberán ser la base para identificar e integrar la configuración inicial.

- Deberá recabar e integrar la documentación que soporte la identificación de la configuración inicial y cualquier modificación que se genere. La elaboración de estos documentos deberá seguir los lineamientos internos de la Institución, además de los que se indiquen en específico para cada uno.

- Desde la configuración inicial se deberá tener conocimiento de las dependencias y funcionamiento de los componentes de la configuración, para estar en posibilidades de proporcionar soporte a los productos durante la fase operacional de los mismos.

Administración y Control de la Configuración

Análisis y Planeación

- Para llevar a cabo una adecuada Administración y Control de la Configuración, la Dirección de Informática deberá procurar que la documentación soporte contenga como mínimo lo siguiente:

a) Diseño de la solución

Deberá describir los principales detalles de la solución, tales como, el tipo de plataforma con que se cuenta, sistema operativo bajo el cual trabaja, etc.

b) Descripción de los equipos

Deberá enunciar las características físicas de los componentes de los equipos, tales como: tipo de equipo, modelo, serie, capacidad de almacenamiento, memoria, velocidad de proceso, velocidad de transmisión, tipo de componente, conectividad, software instalado, etc.

c) Descripción de los sistemas

Deberá contener las características y facilidades de los sistemas operativos, las versiones y modificaciones, las consideraciones de funcionamiento, herramientas propias, características de seguridad, dependencias y características funcionales de cada uno de ellos.

d) Configuraciones de hardware

Deberá contener la descripción física, diagramas de las instalaciones de alimentación de energía eléctrica, diagramas de los arreglos de los equipos en las diferentes localidades, conexiones entre ellos, tendido de cableado eléctrico, localización física de los equipos.

e) Configuraciones de software

Deberá contener una descripción de cada uno de los sistemas aplicativos que se encuentran instalados y operando, sistemas que conforman la Red de comunicaciones, versiones, necesidad de recursos para operar, dependencias operativas con otros sistemas y requerimientos de funcionamiento.

f) Diagramas de instalaciones

Deberá describir gráfica y detalladamente las diferentes configuraciones de hardware, software y sistemas de comunicación que conforman la plataforma informática del Sistema BANRURAL. Estos diagramas deberán contemplar cada Sucursal, Nodo Regional, Central y Espejo.

g) Documentación de pruebas

Se deberá proporcionar a los responsables de las diferentes Subgerencias de Informática de los Regionales, un documento que contenga los protocolos de aceptación, plan de pruebas y de procedimientos que muestren cómo deberán verificarse los mecanismos de funcionalidad, recuperación y seguridad de los sistemas para los diferentes escenarios de problemas o fallas en ellos.

h) Instalación

Deberá contar con la información acerca del estado y características finales de la instalación para ser integrada en esta documentación.

i) Memorias técnicas

Se deberá recabar la información que forma parte de las memorias técnicas, integrarla y mantenerla disponible para cualquier aclaración.

j) Actualización

Se deberá mantener toda la documentación aquí descrita actualizada y disponible para el personal involucrado en el Análisis y Planeación de la Configuración.

Administración de la Configuración

Es responsabilidad de la Dirección de Informática, llevar a cabo lo siguiente:

- Deberá mantener resguardada la documentación soporte de la configuración inicial y actualizaciones de los equipos respectivos.

- Deberá llevar un histórico de todos y cada uno de los elementos que componen la configuración, permitiendo conocer el estado que guarda y la relación con todos los componentes a lo largo de su ciclo de vida.

- Cada uno de los componentes de la configuración (registro, archivo, programa, cable, pantalla, módem, etc.) deberá tener asignado un identificador (número de inventario) con la finalidad de llevar un control. Esta responsabilidad, así como la de identificar claramente todos y cada uno de los componentes, será en conjunto con la Subdirección Corporativa de Recursos Materiales y Servicios Generales.

Control y/o Modificación de la Configuración

Será responsabilidad de la Dirección de Informática:

- Actualizar la configuración inicial de los equipos cada vez que se ejecute un cambio en algún componente. Deberán además llevar un estricto control de cambios.

- Aprobar todas aquellas modificaciones que se pretendan efectuar a la configuración de los equipos, así como informar a las áreas afectadas.

- En caso de existir alguna modificación a la configuración de los equipos de la Institución, ya sea por parte de terceros o por su propio personal, solicitar las memorias técnicas o la información técnica sobre los cambios efectuados, esto con la finalidad de actualizar la documentación de dicha configuración.

- Deberá coordinar auditorias funcionales y físicas por lo menos trimestralmente, a la configuración y sus componentes, de acuerdo a las características de los mismos, con requerimientos detallados, procesos específicos, tareas y responsabilidades de manera que los documentos de la misma reflejen la realidad.

- Deberá ser la instancia responsable de tomar las acciones derivadas de las recomendaciones surgidas de los resultados de las auditorias.

- Deberá documentar cualquier modificación que se realice a la configuración de tal forma que se mantenga actualizada dicha documentación.

Sistemas Aplicativos

Es responsabilidad de la Dirección de Informática:

- Asegurar que la Administración de la Configuración se aplica a todos los proyectos de los sistemas aplicativos. Coordinará la integración de los diversos elementos que conforman la configuración durante el ciclo de vida del proyecto.

- Deberá de establecer los mecanismos necesarios para que las tareas de configuración se hagan al nivel de detalle requerido.

- Deberá conformar la administración de pruebas de integración y codificación, diseñar la administración de la generación de archivos, crear la especificación de la Administración de la Configuración de los componentes de software y de los de hardware.

- Deberá participar en el desarrollo de los códigos respectivos que contendrá la documentación del proyecto.

- Realizar la identificación de la configuración y evaluar los nuevos productos que se generen, así como, el proceso utilizado para el desarrollo de estos, asegurando la calidad de los mismos.

IV.2.- Administración de Impresoras

- Todos los usuarios de impresoras deberán revisar los documentos en la pantalla de la computadora y corregir cualquier error que se encuentre, antes de que el documento sea enviado a imprimir.

- En caso de que la información impresa tenga como clasificación “Confidencial” o superior, deberá resguardarse inmediatamente por el usuario que la imprime o bien destruirse si no será utilizada.

- Es responsabilidad del usuario que ejecuta la impresión de su información, el uso indebido que se dé a esta.

- Es responsabilidad de cada usuario o propietario de la información asegurarse que se proporcione la “Clasificación de Información” adecuada a los reportes o impresiones que genere.

- Es responsabilidad de cada usuario o propietario de la información asegurarse que los procedimientos de manejo de material impreso están de acuerdo a su “clasificación” (confidencial, uso interno, confidencial/restringida y público).

- Las impresoras de la Institución deben utilizarse solo para fines exclusivos de trabajo de la Institución. Por lo tanto, no deberán efectuarse impresiones de carácter “personal”.

Impresoras Compartidas

Impresoras ubicadas dentro del Centro de Cómputo

- El personal que trabaja dentro del Centro de Cómputo, es responsable solo de las impresiones que ellos mismos generen.

- El personal del Centro de Cómputo deberá balancear las impresiones de manera que las de alto volumen se canalicen a una impresora dedicada, mientras que las demás a otra diferente, de tal forma que no se generen retrasos por falta de disponibilidad de impresoras.

- El personal del Centro de Cómputo deberá desarrollar un plan de ejecución de tareas de impresión y distribuirlas de acuerdo a los grupos de usuarios y/o al tipo de impresión.

- El personal del Centro de Cómputo administrará, verificará y depurará periódicamente la cola de impresión.

- La entrega de listados por ventanilla solo deberá hacerse cuando el volumen de la misma así lo implique y se efectuará previa identificación del usuario de la misma.

- La Dirección de Informática en conjunto con la Subdirección Corporativa de Recursos Materiales y Servicios Generales, deberán mantener un inventario de las impresoras instaladas en el Sistema BANRURAL indicando su localización física.

- El personal que labora en Centro de Cómputo es responsable de la instalación y reubicación de las impresoras dentro del mismo. Las Subgerencias de Informática supervisarán la instalación y reubicación de impresoras en su área de influencia, debiendo informar al Centro Nacional de Cómputo de cualquier modificación y de esta forma mantener actualizado el inventario.

- El área del Centro de Cómputo deberá asegurarse que las incidencias son reportadas, revisadas y aclaradas.

- Todas las tareas o referencias contenidas dentro de las bibliotecas deberán ser eliminadas y reemplazadas en cada nueva generación de producción de las bibliotecas.

- En caso de que el usuario no este en posibilidades de cancelar alguna impresión generada por el mismo, deberá solicitarse al Centro de Cómputo, dicha cancelación.

Tareas Extraordinarias

- Para obtener el servicio de impresión de una tarea extraordinaria o de producción, se deberá presentar la solicitud de impresión en el formato establecido para este fin, debidamente requisitado y autorizado al Centro Nacional de Cómputo.

- El Centro de Cómputo, deberá llevar un control de las solicitudes de impresiones extraordinarias y/o de producción solicitadas en ventanilla.

- El personal de Servicios de Producción se reserva los derechos para aceptar o rechazar un flujo de tareas dentro del tiempo de producción, si el tiempo de corrida es tal, que no puede ser terminado en el ciclo del procesamiento normal.

Impresoras en Red

- La Dirección de Informática deberá verificar y depurar periódicamente la cola de impresión de las impresoras conectadas a la Red.

- La Dirección de Informática deberá habilitar varias impresoras en puntos estratégicos de los edificios del Banco, de acuerdo a las necesidades específicas de cada área.

- Debido a que las impresoras de la Red son compartidas, pueden ser utilizadas por todo el personal del Sistema BANRURAL, de acuerdo al área o grupo de trabajo donde se encuentren registrados.

- Es responsabilidad de los usuarios de las impresoras conectadas a la Red el uso que se les dé a las que tengan asignadas a su área o grupo de trabajo.

- Los usuarios tienen la opción de reciclar y reutilizar en la impresora, el papel en buen estado que cuente con una cara libre.

- El usuario de la Red solo podrá cancelar los trabajos de impresión de su propiedad cuando así lo requiera. En caso de necesitar ayuda deberá consultar directamente con las áreas de la Dirección de Informática.

Impresoras esclavas

- Los usuarios directos son responsables de la administración y uso que se dé a las impresoras que proporcionan únicamente servicio a su computadora personal, denominadas impresoras esclavas.

- Los usuarios de dichas impresoras son los responsables de la depuración de la cola de impresión y de las cancelaciones de trabajos.

- Los usuarios directos de estas impresoras deberán supervisar que se les proporcione el mantenimiento preventivo y correctivo requerido.

IV.3.- Administración de Medios Magnéticos

Almacenamiento y Cuidados Específicos para los Medios Magnéticos

Los usuarios de medios magnéticos tienen las siguientes responsabilidades:

- Todos los medios magnéticos utilizados en equipos de cómputo, deberán mantenerse alejados de la luz solar directa, de temperaturas extremas, agua, humedad, aparatos que generen radiación o campos magnéticos (TV., equipo electrónico, cafetera, etc.).

- Todos los medios magnéticos utilizados en equipos de cómputo, deberán almacenarse en lugares seguros, limpios, libres de polvo o de cualquier contaminante que pudiera deteriorarlos. Deberán mantenerse en los lugares propios para dicho almacenamiento.

- Los medios magnéticos que de acuerdo a su confidencialidad, características especificas ó nivel de clasificación de información, deberán mantenerse en lugares de acceso restringido y solo podrán ser utilizados por el personal que trabaja directamente con dicha información, que cuente con la autorización por escrito de su jefe inmediato y en su caso de la Dirección de Informática y en los Regionales por conducto de las Subgerencias de Informática.

Medios Magnéticos utilizados en Equipos de Cómputo Personal

Los usuarios de medios magnéticos tienen las siguientes responsabilidades:

- El responsable de almacenar su información, en un lugar seguro y bajo llave, si así lo amerita y mantener en buenas condiciones los medios magnéticos utilizados en equipos de cómputo personales es el usuario directo de los mismos.

- Este usuario directo ó custodio es responsable de la información contenida y utilización que se dé a estos medios magnéticos, por terceras personas, estén estas autorizadas o no.

- De acuerdo al nivel de clasificación de información (Uso Interno, Confidencial, Confidencial/Restringido ó Público), asignado a los medios magnéticos, estos deberán ser resguardados por su propietario o custodio con mayor o menor seguridad y protección.

- En caso de que el nivel de clasificación del medio magnético sea “Confidencial” o “Confidencial/Restringido”, este deberá resguardarse invariablemente bajo llave y de acuerdo a los cuidados específicos aquí mencionados.

- Específicamente, los diskettes no deberán doblarse, sujetarse con clips o cualquier tipo de sujetapapeles. En caso de requerir adjuntarse a algún documento, deberán depositarse en su caja de fábrica o en un sobre.

- Los cartuchos de cinta de 4 mm. deberán seguir los mismos cuidados que se mencionan para los diskettes, con la diferencia de que deberán guardarse en su contenedor individual para su manejo y almacenaje.

Equipos SP2, G40 y NT

El personal del centro de cómputo, tiene las siguientes responsabilidades:

- Los medios magnéticos del equipo SP2 y G40 respectivamente (Unidad de disco RAID-5 (7135-210), y Unidad de cintas 3750-B11) deberán ubicarse dentro del área que ocupa el centro de cómputo

- Los medios magnéticos deberán mantener y seguir las condiciones ambientales definidas para el centro de cómputo.

- Los permisos de acceso a los discos deberán ser vigilados por la Dirección de Informática, de acuerdo al nivel de clasificación de información que contengan dichos dispositivos y a la autorización por escrito que presente el personal que desee accesarlos.

- Deberán proporcionarle cuidado especial a la unidad de cintas Magstar 3570-B11, ya que por sus características específicas requiere de manipulación de cartuchos y del carrusel que los contiene de acuerdo a su capacidad.

- Deberán proporcionarles periódicamente limpieza y asegurarse de que se realiza el mantenimiento preventivo a los equipos de cómputo, con la finalidad de evitar que los medios magnéticos tengan problemas futuros.

- Deberán montar los cartuchos de acuerdo al orden y los procedimientos indicados por el usuario para la ejecución de los diferentes procesos.

- Deberán proporcionar la limpieza de la trayectoria de la cinta mediante el cartucho de limpieza y el procedimiento indicado en el manual de operación de la unidad 3570 (GA32-0345-01), cuando la unidad así solicite.

- Es responsabilidad de Dirección de Informática, la administración, manejo y control de las unidades de disco de los equipos NT y de los medios magnéticos utilizados en estos equipos.

Control y Verificación

Los usuarios de medios magnéticos y personal del Centro de Cómputo tienen las siguientes responsabilidades:

- Deberán verificarse periódicamente (por lo menos 1 vez al mes), todos los medios magnéticos con el fin de comprobar daños, contaminación, saturación o posibilidad de depuración. De esta forma se mantendrán en óptimas condiciones de uso.

- Antes y después de utilizar un diskette debe verificarse que no contenga algún tipo de “virus” o daño irreparable.

- No deberán almacenar, trabajar, utilizar o transportar medios magnéticos que no se encuentren debidamente identificados y clasificados de acuerdo a las “Políticas de Clasificación de Información”.

- En los equipos de computo personales, el usuario directo o propietario de la información deberá efectuar revisiones periódicas (por lo menos 1 vez al mes) a sus medios magnéticos, para determinar la validez y utilidad de la información de tal forma que dichos medios tengan la posibilidad de reutilizarse.

- En los equipos SP2 y G40, se deberá llevar un control de los errores temporales que presenten los medios magnéticos y un listado de los volúmenes más utilizados, con su respectivo conteo de errores. En el caso de que algún medio magnético cuente con un apreciable incremento de errores temporales en un volumen, o bien se presenten consistentemente errores permanentes este deberá reemplazarse.

- Mediante el listado de los volúmenes más utilizados (número de errores por número de montajes), deberá calcularse el periodo de vida para estos volúmenes.

- Cualquier medio magnético que haya sido maltratado por el equipo de cómputo, se encuentre deteriorado, contaminado permanentemente y/o desgastado por su uso constante deberá ser reemplazado.

Transportación de los Medios Magnéticos

Los usuarios de medios magnéticos tienen las siguientes responsabilidades:

- Antes de efectuar la transportación de cualquier medio magnético fuera de las instalaciones originales, se deberá obtener autorización por escrito del Jefe inmediato que funja como propietario de la información para su transporte y salida de las instalaciones, con la relación de los dispositivos, contenido, responsable y lugar a donde serán trasladados y almacenados.

- Cuando deban ser transportados los medios magnéticos, la temperatura no deberá exceder de 43° C (110° F).

- Para su transporte, los medios magnéticos deberán ser colocados en la misma posición y orden en el que se almacenan normalmente. Deberán ir contenidos en cajas contenedoras o estantes adecuados para el transporte, y no deberán transportarse de manera aislada.

- El personal designado para efectuar la transportación de los medios magnéticos, será responsable de los mismos y deberá hacer frente a cualquier eventualidad que se presente.

Reutilización de Medios Magnéticos

Los usuarios de medios magnéticos y personal del centro de cómputo, tienen las siguientes responsabilidades:

- Cuando sea necesario reutilizar algún tipo de medio magnético, este deberá ser revisado, de manera que no presente problemas futuros. La reutilización deberá hacerse de acuerdo al programa y/o calendarización de respaldos.

- Aquellos medios magnéticos que no puedan reutilizarse, deberán ser desechados y/o destruidos, con el fin de evitar la posibilidad de que por error sean utilizados y causar algún problema en el futuro.

- La reutilización de medios magnéticos para efectuar respaldos, dependerá de las recomendaciones de los fabricantes de los mismos y de la experiencia que se obtenga con su uso.

- La Dirección de Informática, es responsable de llevar a cabo el programa de reutilización de los medios magnéticos de acuerdo a las necesidades específicas de información y almacenamiento de cada uno y al programa de respaldos.

Depuración de Información

- El usuario directo o propietario de la información deberá depurar periódicamente los medios magnéticos utilizados por equipos de cómputo personales.

- Es responsabilidad de la Dirección de Informática, la depuración de la información contenida en el arreglo de discos y medios magnéticos que utilice para efectuar su trabajo.

- El personal del centro de cómputo tiene la responsabilidad de conservar la información mensual en los medios magnéticos y la información contable por lo menos durante 10 años.

IV.4.- Administración de Procesos Batch.

Responsabilidades

- La Dirección de Informática, deberá proporcionar los elementos y el ambiente necesarios para estar en posibilidades de que las áreas usuarias ejecuten sus procesos Batch.

- La Dirección de Informática, deberá mantener disponibles los ambientes y sistemas para la ejecución de los procesos Batch.

- Los cambios en los ambientes, sistemas o nuevos requerimientos para procesos Batch, deberán ser solicitados formalmente y por escrito a la Dirección de Informática.

- La Dirección de Informática, deberá evaluar las solicitudes de requerimientos de los procesos Batch en cuanto a validar si ha existido un requerimiento similar, identificar si es temporal o permanente, las áreas beneficiadas y a que aplicación o sistemas afecta.

- La Dirección de Informática y las áreas responsables de los procesos Batch, deberán considerar cualquier cambio en programas, equipos, mecanismos de control, configuraciones, instalaciones, diseño de bases de datos, aplicaciones y/o ambiente operativo que modifique las funciones de dichos procesos.

- La Dirección de Informática, deberá desarrollar, probar y ejecutar los procesos Batch que le correspondan.

- El área usuaria es responsable directo de los procesos Batch que genere.

- Es responsabilidad de cada usuario responsable de los procesos Batch, verificar la calidad de los resultados de los mismos, luego de su ejecución.

- Es responsabilidad de la Dirección de Informática, monitorear los procesos Batch que generen las áreas usuarias, notificarles cualquier problema que se presente y en su caso proporcionar soporte técnico necesario.

Administración

- Todos los cambios que afecten a los procesos Batch deberán ser aprobados, validados y documentados por las áreas solicitantes y/o responsables de dichos procesos.

- Las áreas responsables de los procesos Batch y la Dirección de Informática, deberán documentar todos los cambios que se efectúen a los recursos de los sistemas así como contar con un procedimiento que permita restablecer el ambiente original en caso de alguna eventualidad y de un plan de capacitación para el personal de operación de sistemas cuando así se requiera.

- En el caso de requerirse un reproceso por causas imputables a la operación de los equipos y sistemas de cómputo, la Dirección de Informática deberá informar al área responsable del proceso, de la situación, así como anotar la incidencia en la bitácora correspondiente.

  La documentación técnica como los manuales de operación, manuales de usuario, documentación de referencia y diagramas de cada aplicación deberán ser actualizados por la Dirección de Informática, para ello, el área responsable de los procesos Batch, deberá documentar y consultar a dicha área cada vez que se pretenda implantar un cambio, y en caso de que ambas áreas lo consideren procedente implantarlo y actualizarlo dentro de la documentación técnica.

- Las áreas responsables de los procesos Batch deberán hacer una revisión de la calidad de los trabajos en lo que respecta a la confiabilidad e integridad de los datos, legibilidad de los reportes (si se generan), revisión de las salidas a medios magnéticos.

- La Dirección de Informática, deberá efectuar el proceso de eliminación de archivos de acuerdo a lo especificado en cada aplicativo que forme parte de los procesos Batch.

Control y Verificación

- La Dirección de Informática, deberá efectuar el mantenimiento periódico a las bases de datos y vigilar la capacidad disponible en los equipos.

- La Dirección de Informática, deberán documentar las actividades y cambios en dependencias, calendarios e incidencias diarias, para obtener gráficos por horario y por aplicación, para llevar a cabo el estadístico de comportamiento.

- La Dirección de Informática, deberá llevar un control o programa centralizado de los cambios instalados y por instalarse en cuanto al ambiente de operación, así como reportes estadísticos que permitan distinguir, analizar y corregir desviaciones.

- La Dirección de Informática, generará mediciones y estadísticas de las actividades para reportar al área responsable del proceso cuando se presenten comportamientos anormales, utilizando las herramientas de monitoreo propias o del sistema operativo.

- La Dirección de Informática, verificarán que se corrijan las desviaciones encontradas en los procesos Batch, efectuando los ajustes necesarios

- Las áreas responsables de los procesos Batch deberán colaborar con la Dirección de Informática, para definir, probar y validar el procedimiento de recuperación de sus procesos Batch, que permita restablecer el ambiente original en caso de alguna eventualidad.

- Es responsabilidad de la Dirección de Informática, identificar, establecer y mantener los procedimientos de recuperación de los procesos, de acuerdo a los procedimientos definidos en conjunto con las áreas responsables de los procesos Batch, con la finalidad de garantizar la continuidad de estos.

IV.5.- Administración de Procesos en Línea

Requerimientos de Operación

- Los procesos en línea que corran en los sistemas de la Institución deberán estar debidamente autorizados y probados por las áreas usuarias de los mismos.

- Las solicitudes para cualquier cambio en los ambientes operativos o en los sistemas de los procesos en línea, se deberán efectuar por escrito a la Dirección de Informática.

Responsabilidades

- Es responsabilidad de la Dirección de Informática, levantar y mantener funcionales, los sistemas necesarios para que los procesos en línea puedan ejecutarse.

- Es responsabilidad directa del usuario y/o área usuaria, la ejecución de sus procesos en línea.

- Las áreas responsables de los procesos en línea, deberán trabajar en conjunto con la Dirección de Informática, la definición, prueba y validación del procedimiento de ejecución y recuperación de su proceso en línea, que permita restablecer el ambiente original en caso de alguna eventualidad.

- La Dirección de Informática, deberá documentar los procesos en línea que tenga bajo su responsabilidad.

- Es responsabilidad de la Dirección de Informática, resguardar los procedimientos de recuperación de los procesos en línea, con la finalidad de garantizar la continuidad de estos.

- Es responsabilidad de la Dirección de Informática, monitorear la ejecución y comportamiento de los procesos en línea.

- En caso de detectarse alguna anomalía durante la ejecución de algún proceso en línea, la Dirección de Informática, deberá documentarla y reportarla al responsable directo del proceso.

- Es responsabilidad de la Dirección de Informática, proporcionar soporte técnico a las áreas responsables de los procesos en línea, cuando estas así lo requieran.

Primer Nivel de Determinación de Problemas

- La Dirección de Informática, deberá definir la ventana de disponibilidad de los procesos y documentar las funciones de iniciar, detener, configurar y monitorear la operación de las aplicaciones en línea ó interactivas.

- En caso de que el área usuaria detecte alguna anomalía o retraso en su proceso en línea, deberá informarlo a la Dirección de Informática. Esta verificará el problema y determinará las posibles causas y soluciones.

- Es responsabilidad de la Dirección de Informática, proporcionar el primer nivel de determinación de problemas que se presenten en la Red, también deberá registrar, documentar y dar seguimiento a cada problema hasta la solución del mismo.

- Es responsabilidad del personal del Centro de Cómputo, proporcionar el primer nivel de determinación de problemas que se presenten en los sistemas en línea, también deberá registrar y documentar cada problema que se presente en los sistemas en línea hasta la solución del mismo.

- Es responsabilidad de la Dirección de Informática contactar a los proveedores de servicio de mantenimiento correctivo que dé solución a los problemas, así como también deberán informar a la coordinación correspondiente cuando se presente un problema que afecte la operación y/o prestación de servicios.

Planeación de Procesos

- El área usuaria deberá programar y/o calendarizar sus procesos en línea.

- El Centro de Cómputo debe manejar prioridades para la ejecución de los procesos en línea, evitando así la saturación de su equipo.

- Todos los cambios que se hagan a los procesos en línea, deberán contar con un procedimiento que permita restablecer el ambiente original en caso de presentarse alguna falla provocada por el cambio.

- La implantación de nuevos sistemas para proporcionar un mejor servicio a los usuarios, deberá ser requerida a la Dirección de Informática de manera formal.

IV.6.- Administración de la Operación

Responsabilidades en la Operación

- La información que se presente en la recepción de los diferentes Nodos, independientemente del medio en que se encuentre contenida para ser procesada en los sistemas y equipos de cómputo, deberá estar identificada con el nombre del propietario o custodio, nivel de clasificación de seguridad (en caso de que lo requiera), e identificación de la misma de acuerdo a las Políticas referentes a la Clasificación de la Información.

- La Dirección de Informática es responsable tanto de la información que genera, como de aquella que está bajo su custodia.

- El responsable de cada Nodo deberá planear las cargas de trabajo para el personal de operación, considerando situaciones imprevistas de personal ausente, vacaciones y/o enfermedad.

- El personal usuario que deba operar un equipo o sistema de cómputo deberá contar y aplicar el “Manual de Usuario”.

- La Dirección de Informática deberá resguardar los originales de la documentación técnica de equipos y sistemas y vigilar la actualización de estos manuales cuando así sea necesario.

- La Dirección de Informática deberá vigilar el uso adecuado de los recursos compartidos (impresoras y estaciones de trabajo).

- La Dirección de Informática deberá vigilar que se tenga un sistema de energía ininterrumpible (no-break) que permita concluir apropiadamente las actividades en caso de corte de energía en los diferentes Nodos integrantes del Sistema BANRURAL.

- Los usuarios de microcomputadoras deberán mantenerlas conectadas al no-break respectivo.

- En caso de interrupción de energía eléctrica deberá procederse a concluir la sesión de trabajo, apagar el equipo y el No-Break, a fin de no agotar las baterías de este último.

- En el caso de los equipos microcomputadores, los usuarios de los mismos, al concluir sus labores o retirarse de la oficina por tiempo prolongado, el usuario deberá apagar el equipo y el No-Break.

- No deberán conectarse al No-Break aparatos electrónicos tales como radios, cafeteras, ventiladores, etc., así como impresoras láser, ya que existen limitaciones en su capacidad de suministro.

- Se deberán evitar conexiones provisionales (cables de corriente eléctrica sueltos), contactos en mal estado o sin tierra física. En caso de observar alguna anomalía o falla deberá reportarla al Área de Mantenimiento, dependiente de la Subdirección Corporativa de Recursos Materiales y Servicios Generales.

Nodo Central

- El personal del Nodo Central es responsable de mantener en operación adecuada los equipos, sistemas de cómputo, servicios de telecomunicaciones y Redes.

La Dirección de Informática es responsable de:

En la Operación de equipos de cómputo y sistemas:

- Operar y monitorear los dispositivos de I/O (entrada / salida), de los sistemas de cómputo RS/6000 SP2 y G40.

- Controlar, monitorear, ejecutar las tareas y operar los sistemas de cómputo RS/6000 SP2 y G40.

- En caso de una falla en los equipos, anotar en la bitácora de fallas, informar a la Gerencia y dar seguimiento a los problemas o fallas en los equipos y sistemas de cómputo.

- Supervisar el correcto llenado de la carpeta de IBM “Account Management” por parte de los Representantes de Servicio de este proveedor.

- Utilizar adecuadamente las herramientas del sistema para monitoreo.

- Anotar las incidencias, problemas pendientes de solución y servicios pendientes de finalización en la bitácora de cambio de turno.

- Ejecutar procedimientos de respaldo y recuperación de información proporcionados por los administradores de sistemas y de bases de datos.

- Seguir los procedimientos de seguridad física y lógica en el Centro de Cómputo.

- Mantener operacionales y en buen estado los equipos y sistemas de cómputo.

- Documentar los procedimientos operativos.
- Clasificar la información que ellos mismos generen.

La Dirección de Informática es responsable de:

En la Administración de sistemas y bases de datos:

- Administrar, controlar y configurar los Sistemas RS/6000 SP2.
- Instalación, soporte y mantenimiento de Software.
- Mantenimiento preventivo y correctivo a las Bases de Datos.
- Definir estándares de instalación y operación.
- Implantar esquemas de seguridad lógica.
- Definir elementos de medición para mejorar el rendimiento de los sistemas.
- Supervisar el correcto llenado del Account Management por parte de los representantes de servicio de IBM.
- Utilizar las herramientas para el monitoreo de los sistemas.
- Reportar al proveedor del servicio las incidencias de fallas de los equipos.
- Supervisar que se cumplan los acuerdos de niveles de servicio.
- Elaborar y documentar procedimientos de operación de equipos y sistemas de cómputo.
- Preparar y acordar con el prestador de servicios de mantenimiento de los equipos y sistemas de cómputo un calendario para estos servicios.
- Supervisar que se proporcionen en tiempo y forma los diferentes servicios de mantenimiento a los equipos y sistemas de cómputo.
- Identificar problemas de Hardware y Software de los equipos RS/6000 SP2 y G40.
- Dar asesoría a los usuarios en los problemas de primer nivel.
- Identificar y canalizar los problemas de segundo nivel a otras áreas.
- Optimizar recursos.
- Solucionar problemas de los usuarios relacionados con el equipo a su cargo.
- Asegurar la actualización del Nodo Espejo.

- Definir procedimientos y programas de respaldo y restauración.
- Instalar, soportar y mantener actualizado el software.
- Elaborar procedimientos y documentación de los sistemas instalados.
- Definir elementos de medición para mejorar el rendimiento de los sistemas.

La Dirección de Informática es responsable de:

En Telecomunicaciones y Administración de la Red:

- Administrar, controlar y configurar la Red Local del Nodo Central (Red), la Red Satelital y la Red de RDI (Telecomunicaciones).
- Operar y monitorear los sistemas y servicios de telecomunicaciones y Redes.
- Reportar al proveedor, anotar en la bitácora de fallas, dar seguimiento a los problemas o fallas en los equipos de telecomunicaciones y la Red.
- Anotar las incidencias, problemas pendientes de solución y estado de los sistemas de telecomunicaciones y Redes en la bitácora de cambio de turno.
- Cumplir con los acuerdos de servicio de telecomunicaciones y Redes pactados con los usuarios.
- Seguir los procedimientos de seguridad y/o contingencia de los equipos de telecomunicaciones y Redes.
- Mantener operacionales y en buen estado los equipos de telecomunicaciones y Redes.
- Elaborar procedimientos de operación de los equipos de telecomunicaciones y Redes.
- Preparar y acordar con el prestador de servicios de mantenimiento a los equipos de telecomunicaciones y Redes.
- Informar sobre la utilización y rendimiento de las telecomunicaciones y la Red.

En Soporte Técnico de Comunicaciones:

- Monitorear, detectar y reportar fallas en el equipo satelital a quien corresponda según el caso.
- Controlar y configurar la Red de RDI.
- Monitorear, detectar y reportar fallas en el equipo de RDI a quien corresponda según el caso.
- Activar y controlar el equipo satelital para casos de contingencia tanto en el Nodo Central como el Espejo.
- Generar y controlar estadísticas para diseño y planeación.
- Informar sobre la utilización y rendimiento de la Red satelital.
- Administrar inventarios de equipos y dispositivos de comunicación.

En Soporte Técnico a equipos NT:

- Identificar de problemas de Hardware y Software.
- Proporcionar asesoría a los usuarios en los problemas de primer nivel.
- Identificar y canalizar los problemas de segundo nivel a otras áreas.
- Optimizar recursos.
- Solucionar problemas de los usuarios relacionados con el equipo a su cargo.
- Definir procedimientos y programas de respaldo y restauración.
- Instalar, soportar y mantener actualizado el Software Básico.
- Definir elementos de medición para mejorar del rendimiento de los sistemas.
- Controlar el inventario de Software instalado.

En Soporte Técnico de Sucursales y Comunicaciones:

- Identificar problemas de hardware y software relacionados con los equipos instalados en sucursales operativas.
- Dar asesoría a los usuarios en los problemas de primer nivel.
- Identificar y canalizar los problemas de segundo nivel a otras áreas.
- Monitorear, detectar, corregir y reportar en su caso fallas en el equipo satelital a quien corresponda según el caso.
- Instalar, soportar y mantener actualizado el software básico.

En cuanto a desarrollo de sistemas aplicativos:

- Proveer asesoría en la operación de las aplicaciones.
- Diagnosticar y dirigir la corrección de problemas en la operación de los sistemas aplicativos.
- Modificar la funcionalidad de las aplicaciones vía parametrización.
- Crear y/o modificar los reportes del sistema.

Nodo Espejo

- El personal del Nodo Espejo deberá mantenerlo operacional y activo, de manera que si se presenta una eventualidad en los sistemas de proceso de datos del Nodo Central, éste se haga cargo de la operación.
- Es responsabilidad del personal Nodo Espejo, coordinarse y asesorarse del personal del Nodo Central.
- Es responsabilidad del personal del Nodo Espejo mantener una imagen actualizada de los sistemas, aplicaciones, bases de datos e información contenidos en el Nodo Central.

La Subgerencia de Informática del Banco de Crédito Rural de Occidente

En Administración de sistemas y bases de datos es responsable de:

- Administrar, controlar y configurar los Sistemas RS/6000 SP2.
- Instalación, soporte y mantenimiento de Software.
- Definir estándares de instalación y operación.
- Implantar esquemas de seguridad lógica.

- Definir elementos de medición para mejorar el rendimiento de los sistemas.
- Supervisar el correcto llenado del Account Management por parte de los representantes de servicio de IBM.
- Utilizar las herramientas para el monitoreo de los sistemas.
- Reportar al proveedor del servicio las incidencias de fallas de los equipos.
- Supervisar que se cumplan los acuerdos de niveles de servicio.
- Elaborar y documentar procedimientos de operación de equipos y sistemas de cómputo.
- Preparar y acordar con el prestador de servicios de mantenimiento de los equipos y sistemas de cómputo un calendario para estos servicios.
- Supervisar que se proporcionen en tiempo y forma los diferentes servicios de mantenimiento a los equipos y sistemas de cómputo.

En Telecomunicaciones y Administración de la Red es responsable de:

- Operar y monitorear los sistemas de telecomunicaciones y Redes.
- Reportar al proveedor, anotar en la bitácora de fallas, informar al responsable del Nodo y dar seguimiento a los problemas o fallas en los equipos de telecomunicaciones y en la Red.
- Anotar las incidencias, problemas pendientes de solución y estado de los sistemas de telecomunicaciones y Redes en la bitácora de cambio de turno.
- Seguir los procedimientos de seguridad de los equipos de telecomunicaciones y Redes.
- Mantener operacionales y en buen estado los equipos de telecomunicaciones y Redes.

Nodos Regionales

- Es responsabilidad de las Subgerencias de Informática en los Nodos Regionales mantener en operación los equipos y sistemas de cómputo y los servicios de telecomunicaciones y Redes.

- Es responsabilidad de las Subgerencias de Informática en los Nodos Regionales proporcionar servicios de soporte de operación, telecomunicaciones, soporte técnico y soporte de sistemas de Información a los Nodos Sucursales por medio del personal técnico creado para este fin.

Las Subgerencias de Informática de los Regionales

En operación de los equipos de cómputo son responsables de:

- Utilizar las herramientas para el monitoreo de los sistemas.

- Operar y monitorear los dispositivos de I/O (entrada / salida), de los sistemas de cómputo G40.

- Programar, controlar, monitorear la ejecución de las tareas y operar los sistemas de cómputo G40.

- Canalizar al Nodo Central aquellos problemas que no se encontró solución en el Regional.

- Anotar las incidencias, problemas pendientes de solución y servicios pendientes de finalización en la bitácora de cambio de turno.

- Cumplir con los acuerdos de niveles de servicio acordados con los usuarios.

- Seguir los procedimientos de seguridad física y lógica en el Centro de Cómputo.

- Mantener operacionales y en buen estado los equipos y sistemas de cómputo.

- Clasificar la información que ellos mismos generen.

En Administración de sistemas:

- Administrar y controlar los equipos G40.

- Definir elementos de medición para mejorar el rendimiento de los sistemas.

- Utilizar las herramientas para el monitoreo de los sistemas.

- Reportar al Nodo Central las incidencias de fallas de los equipos.
- Supervisar que se cumplan los acuerdos de niveles de servicio.

- Elaborar y documentar procedimientos de operación de equipos y sistemas de cómputo

- Preparar y acordar con el prestador de servicios de mantenimiento de los equipos y sistemas de cómputo un calendario para estos servicios.

- Supervisar que se proporcionen en tiempo y forma los diferentes servicios de mantenimiento a los equipos y sistemas de cómputo.

- Identificar problemas de Hardware y Software de los equipos G40.

- Dar asesoría a los usuarios en los problemas de primer nivel.

- Identificar y canalizar los problemas de segundo nivel al Nodo Central o a otras áreas, en su caso.

- Optimizar recursos.

- Solucionar problemas de los usuarios relacionados con el equipo a su cargo.

- Asegurar la actualización del Nodo Espejo.

- Definir procedimientos y programas de respaldo y restauración.

- Instalar, soportar y mantener actualizado el software.

En Administración de la Red:

- Administrar, controlar y configurar la Red Local (Red).

- Operar y monitorear los sistemas y servicios de la Red.

- Reportar al Nodo Central, anotar en la bitácora de fallas, dar seguimiento a los problemas o fallas en los equipos de la Red.

- Cumplir con los acuerdos de servicio de la Red, pactados con los usuarios.

- Seguir los procedimientos de seguridad y/o contingencia de los equipos de la Red.

- Mantener operacionales y en buen estado los equipos de la Red.

- Preparar y acordar con el prestador de servicios de mantenimiento a los equipos de la Red.

En Soporte Técnico de Comunicaciones:

- Monitorear, detectar y reportar fallas en el equipo satelital a quien corresponda según el caso.
- Controlar y configurar la Red de RDI.
- Monitorear, detectar y reportar fallas en el equipo de RDI a quien corresponda según el caso.
- Activar y controlar el equipo satelital para casos de contingencia.
- Generar y controlar estadísticas para diseño y planeación.
- Administrar inventarios de equipos y dispositivos de comunicación.

En Soporte Técnico de Sucursales y Comunicaciones:

- Identificar problemas de hardware y software relacionados con los equipos instalados en sucursales operativas.
- Brindar soporte técnico a los Nodos Sucursales.
- Dar asesoría a los usuarios en los problemas de primer nivel.
- Identificar y canalizar los problemas de segundo nivel al Nodo Central ó a otras áreas, en su caso.
- Monitorear, detectar, corregir y reportar en su caso fallas en el equipo satelital a quien corresponda según el caso.
- Instalar, soportar y mantener actualizado el software básico.

Servicios de Mantenimiento

- Los sistemas, equipos de cómputo y de telecomunicaciones del Sistema BANRURAL deberán recibir de manera periódica mantenimiento preventivo, predictivo y actualizaciones, independientemente del periodo de garantía de los mismos. La Dirección de Informática, es responsable de esta actividad.

- Es responsabilidad de la Dirección de Informática, conocer los periodos y condiciones que cubren las garantías de los sistemas, equipos de cómputo y de telecomunicaciones, así como solicitarlos en caso necesario.

- Queda estrictamente prohibido abrir los equipos de cómputo por personal no autorizado y/o capacitado para tratar de proporcionarles mantenimiento. En caso de infringir este punto será bajo la responsabilidad absoluta de la persona que tenga el resguardo de dicho equipo ó responsable del mismo.

- La Dirección de Informática, deberá encargarse de solicitar al área correspondiente, la renovación de los contratos de mantenimiento de los equipos cuando así aplique, así como de la supervisión del servicio recibido.

- Cuando ocurra una falla en los sistemas y equipos de cómputo o en los de telecomunicaciones, el personal de la Dirección de Informática responsable de los mismos deberá solicitar al proveedor de servicios dicho mantenimiento correctivo.

- La Dirección de Informática, deberá considerar en los programas de mantenimiento a todos los equipos de cómputo, telecomunicaciones, periféricos y auxiliares del Centro de Cómputo; a continuación se relacionan algunos en forma enunciativa y no limitativa.

  - Equipos de cómputo y auxiliares
  - Aire acondicionado
  - Instalaciones eléctricas y de soporte
  - Señalización de emergencia
  - Pasillos y puertas de emergencia
  - Piso Falso
  - Equipos de control de acceso
  - Mobiliario
  - Equipos de extinción

Acuerdos de Servicio

- La Dirección de Informática, deberá llevar un calendario de programas de mantenimiento preventivo para las instalaciones, equipos de cómputo y auxiliares.

- La Dirección de Informática, deberá verificar que el mantenimiento correctivo mantenga un acuerdo de tiempo de respuesta que no exceda a las 2 (dos) horas en zona metropolitana y 24 (veinticuatro) horas en zonas rurales.

- La Dirección de Informática, deberá llevar una bitácora de los servicios de mantenimiento preventivo y correctivo que se hayan proporcionado a las instalaciones, equipos de cómputo y equipos auxiliares para controlar el cumplimiento del mantenimiento. Esta deberá resguardarse por lo menos un año, para efectos de Auditoría.

Escalamiento de Fallas y Soporte Técnico

Nodo Central	← **Nodo Espejo**
↑	↑
Nodos Regionales	**Nodos Regionales**
↑	↑
Nodos Sucursales	**Nodos Sucursales**

Nodo Central

- La Dirección de Informática es responsable de proporcionar los servicios de soporte de operación, telecomunicaciones, soporte técnico y sistemas de Información a los Nodos Regionales, solo cuando el personal de soporte local no este en posibilidades de resolver alguna problemática.

Nodo Espejo

- La Subgerencia de Informática en el Nodo Espejo es responsable de proporcionar los servicios de soporte de operación, telecomunicaciones, soporte técnico y sistemas de Información, asimismo y a los Nodos Regionales cuando así lo requieran. Solo en el caso de que el personal de soporte de este Nodo no este en posibilidades de resolver alguna problemática o requiera de alguna consulta específica, deberá acudir al Nodo Central.

- En caso de alguna eventualidad o falla en el Nodo Espejo, este deberá comunicárselo de inmediato al Nodo Central.

Nodos Regionales y Sucursales

- Es responsabilidad de la Subgerencia de Informática en los Nodos Regionales proporcionar servicios de soporte de operación, telecomunicaciones, soporte técnico y soporte de sistemas de Información asimismo y a los Nodos Sucursales, por medio del personal técnico creado para este fin.

- Es responsabilidad de los Nodos Sucursales proporcionar a sus usuarios el soporte de proceso de datos para los servicios bancarios que se entregan a clientes.

Evaluación de la Operación

- Los Servicios proporcionados por los centros de cómputo de los diferentes Nodos de la Institución deberán ser evaluados periódicamente por la Dirección de Informática, mediante la encuesta anual de satisfacción de usuarios y la encuesta de disponibilidad.

- La encuesta anual de satisfacción de usuarios deberá conformarse por un cuestionario que contemple los principales puntos de relación entre los usuarios y el servicio prestado, como lo son tiempo de respuesta de los sistemas, facilidad de acceso (sin descuidar la seguridad), integridad de la información, facilidad de uso de los sistemas (ventanas y/o pantallas), etc.

- Los resultados de esta encuesta deberán resultar en acciones concretas por parte de la Dirección de Informática para mejorar el servicio proporcionado.

- Será responsabilidad de la Dirección de Informática, coordinar la elaboración y desarrollo de las encuestas de evaluación de los servicios proporcionados por Nodo Central.

Niveles de servicio

- La Dirección de Informática, por medio de los diferentes Nodos integrantes del Sistema BANRURAL, deberán establecer acuerdos de niveles de servicio con los usuarios que reciben los servicios de cómputo y telecomunicaciones.

- Los acuerdos de niveles de servicio deberán especificar con precisión cada uno de los servicios que se proporcionan por medio de los sistemas, debiendo incluir horarios y fechas comprometidos; asimismo deberán contemplar las sanciones para el prestador de servicios por incumplimiento de los mismos; también deberán especificar las condiciones que debe cumplir el usuario para estar en posibilidades de recibir el servicio.

- Los acuerdos de niveles de servicio deberán contemplar las rutas de escalamiento en caso de problemas, la duración del acuerdo, costos, fechas de revisión del acuerdo, parámetros de comparación y resultados de las encuestas de satisfacción.

Lineamientos para el uso y administración de productos TIVOLI.

Las Subgerencias de Informática de los Bancos Regionales

En cuanto al uso y administración de los productos de administración, control y monitoreo (TIVOLI) son responsables de:

Instalación de los productos TIVOLI

- Deberá verificarse que los equipos denominados TIVOLI MANAGER REGION (equipos G40 o NT), instalados en la oficina matriz de los bancos regionales se encuentren activos.

- Deberán verificar diariamente que los equipos de cómputo denominados endpoints (terminales finales) se encuentren activos tanto en sucursales como en los bancos regionales.

- En caso de que alguno de estos equipos endpoints sufra alguna falla en sus componentes (específicamente el disco), deberá substituirse el servidor y posteriormente instalar el agente de TIVOLI correspondiente.

- Deberán realizar un respaldo diario de la configuración del TIVOLI MANAGER REGION (TMR) en medio magnético con la finalidad de salvaguardar la configuración del software de administración y monitoreo TIVOLI. E

  Este respaldo podrá se reciclado semanalmente de lunes a jueves, el respaldo del viernes deberá conservarse al menos cuatro semanas. A fin de mes deberá conservarse un respaldo mensual el cuál deberá resguardarse al menos un año.

Administración de Usuarios mediante la herramienta Tivoli User Admin

- Con la finalidad de supervisar las altas y mantenimiento de las claves de usuario de los equipos NT de sucursales y banco regional, estás deberán administrarse mediante la herramienta User Admin de TIVOLI.

Distribución de Software mediante la herramienta Tivoli software distribution

- Deberán utilizar la herramienta denominada Tivoli software distribution para la distribución del software ó actualizaciones del sistema operativo y OFI que sean necesarias, así como también distribuir la reportería correspondiente a los módulos de Servicios Bancarios y Crédito a las Sucursales del Banco Regional que les corresponda.

- Deberán verificar las bitácoras de distribución para confirmar que la información haya llegado a las Sucursales destino.

Control Remoto mediante la herramienta Tivoli Remote Control

- Deberán efectuar los mantenimientos preventivos y correctivos del software aplicativo (OFI, CS2, INFORMIX, etc.) a los equipos endpoints de las sucursales correspondientes a su banco regional, mediante Tivoli Remote Control, eliminando con esto el desplazamiento del personal del banco regional a sucursales.

Tivoli Management Framework

- Deberán verificar que este activa la herramienta denominada Tivoli Management Framework en los equipos denominados TIVOLI MANAGER REGION (equipos G40 o NT)

Tivoli Inventory

- Deberá utilizarse la herramienta Tivoli Inventory para llevar a cabo de forma periódica el inventario de Software y Hardware de los equipos endpoints, lo que permitirá tener un mayor control en las actualizaciones de OFI liberadas a las sucursales por la Dirección de Informática.

Tivoli Distributed Monitoring

- Por medio de la herramienta Tivoli Distributed Monitoring, el personal de las subgerencias de informática deberán programar los eventos que requiera monitorear en las sucursales que le corresponde, relacionados con los recursos físicos de los equipos. Este monitoreo permitirá reducir los riesgos de fallas durante la operación en línea.

La Gerencia de Soporte Técnico y Operación:

En cuanto al uso y administración de los productos TIVOLI son responsables de:

Instalación de los productos TIVOLI

- Deberá instalar y mantener operando los productos TIVOLI (Framework, User Admin, Distributed Monitoring, Remote Control, Netview, Inventory y Software Distribution) en los equipos RS/6000 denominados Sermon1, Sermon2 y Sermon3 los cuales son utilizados como consolas centrales de las herramientas TIVOLI .

- Es responsable de atender o canalizar en caso de ser necesario al proveedor, los servicios de mantenimiento así como, los reportes de fallas sobre el uso o instalación de los productos TIVOLI.

- Es responsable de la actualización de las versiones en los equipos denominados TMR y endpoints. Debe considerar la funcionalidad y las necesidades respectivas para efectuar dichos cambios.

- Deberá realizar un respaldo semanal de la configuración instalada en las consolas de monitoreo centrales en medio magnético, con la finalidad de salvaguardar la configuración del software de administración y monitoreo TIVOLI. Este respaldo podrá se reciclado mensualmente.

- Deberá promover la utilización de las herramientas TIVOLI en el sistema BANRURAL.

Administración de Usuarios mediante la herramienta Tivoli User Admin

- Deberá facilitar mensualmente a la Gerencia de Planeación y Seguridad, los archivos conteniendo la información de los usuarios de los equipos NT de sucursales y bancos regionales que estén registrados como endpoints, con la finalidad de que sean verificados contra lo registrado en la nomina del sistema BANRURAL.

Distribución de Software mediante la herramienta Tivoli software distribution

- Deberán utilizar la herramienta denominada Tivoli software distribution para la distribución del software ó actualizaciones del sistema operativo y OFI que sean necesarias, así como también distribuir la reportería correspondiente a los módulos de Servicios Bancarios y Crédito a los bancos regionales.

- Deberá verificar las bitácoras de distribución para confirmar que la información haya llegado a los bancos regionales destino.

Control Remoto mediante la herramienta Tivoli Remote Control

- En caso de ser necesario se brindará soporte técnico a las sucursales del Sistema BANRURAL por medio de está herramienta.

Tivoli Management Framework

- Deberán verificar que este activa la herramienta denominada Tivoli Management Framework en las Consolas Centrales de TIVOLI.

Tivoli Inventory

- Deberá promover el uso de la herramienta Tivoli Inventory para llevar a cabo de forma periódica el inventario de Software y Hardware de los equipos endpoints, permitiendo con ello, tener un mayor control en las actualizaciones de Software.

Tivoli Distributed monitoring

- Por medio de la herramienta Tivoli Distributed Monitoring el personal de esta Gerencia deberá programar los eventos que requiera monitorear en los equipos centrales de computo, relacionados con lo recursos físicos del equipo con el fin de reducir los riesgos de fallas durante la operación en línea.

Tivoli Netview

- Deberá monitorear mediante la herramienta denominada Tivoli Netview la red de comunicaciones del Sistema BANRURAL.

IV.7.- Administración de Procesos de Recuperación

Respaldo y Recuperación de Información

- La Dirección de Informática, así como, las áreas usuarias, tienen la responsabilidad de trabajar conjuntamente para crear los procedimientos de respaldo de información de los sistemas aplicativos de los que son responsables.

- La Dirección de Informática, es responsable de crear los procedimientos de respaldo del medio ambiente de operación, así como la frecuencia y periodicidad, para los diferentes equipos y sistemas de la Institución, mismos que deberán incluirse en los planes de recuperación.

- La Dirección de Informática, tiene la responsabilidad de proporcionar los procedimientos para recuperar la información en caso de alguna eventualidad. Estos también deberán estar contenidos en los planes de recuperación de cada Nodo.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, tienen la responsabilidad de contar con un respaldo de primer nivel del sistema operativo y de los sistemas aplicativos para lograr la recuperación de los equipos de cómputo.

- Los Nodos Sucursales deben efectuar un respaldo de contingencia, que contenga el sistema operativo, sistemas aplicativos y todo aquello que forme parte del medio ambiente del equipo. Este debe efectuarse en el momento en que dicho medio ambiente se encuentre estable y sin problemas.

- Es responsabilidad de la Dirección de Informática, efectuar el respaldo de segundo nivel, es decir, de las aplicaciones que no tienen que ver directamente con el sistema operativo.

- Es responsabilidad de la Dirección de Informática, así como de las áreas usuarias, efectuar el respaldo de la información y de los datos.

- Es responsabilidad de la Dirección de Informática y de las Subgerencias de Informática en Regionales, obtener dos copias de cada respaldo efectuado con el fin de guardar uno en la cintoteca del propio centro de cómputo y otro en una localidad diferente.

- Los respaldos obtenidos con la finalidad de apoyar la recuperación de operaciones de la Institución y que se almacenan en una localidad diferente al centro de cómputo local, deberán tener las características de seguridad que los almacenados en la cintoteca. Estas se encuentran definidas en las Políticas en Informática de Administración de la Seguridad y Políticas en Informática de Administración de Medios Magnéticos.

- La Dirección de Informática y de las Subgerencias de Informática en Regionales, deberán recuperar la información de su Nodo respectivo, de acuerdo a los procedimientos de recuperación creados para este fin y contenidos en el plan de recuperación del centro de cómputo en caso de siniestro.

- Cuando un equipo de cómputo sea preparado para viajar a otra localidad del Sistema BANRURAL, se deberá respaldar la información vital en discos flexibles o en un disco duro movible para resguardarla y protegerla.

- El personal que deba viajar con el equipo y respaldos antes mencionados es responsable de que lleguen a su destino en buenas condiciones y del uso que se dé a la información.

- La recuperación de información deberá efectuarse de acuerdo al escalamiento de fallas, descrito en este documento.

Respaldos en equipos SP

- La Dirección de Informática, deberá ejecutar los respaldos de acuerdo al calendario estipulado entre esta y los responsables de cada uno de los sistemas aplicativos.

Respaldos en equipos G40

- Las Subgerencias de Informática en los Regionales, son responsables de proporcionar las fechas y procedimientos para respaldo y recuperación de información en los equipos RS/6000 G40 de su respectivo Nodo.

- Las Subgerencias de Informática en los Regionales, en coordinación con la Dirección de Informática, deberán definir la información que se debe respaldar de acuerdo al sistema aplicativo del cual sean responsables.

Respaldos en equipos NT

- La Dirección de Informática deberá generar los procedimientos de respaldo y recuperación para la información de los equipos NT de acuerdo al calendario acordado entre estos y los responsables de los sistemas.

- Las Subgerencias de Informática en los Regionales, serán responsables de ejecutar los procedimientos para obtener los respaldos y recuperación de la información de los equipos NT.

Respaldos en equipos PC

- El usuario del equipo de micro computación es responsable de la información contenida en los discos duros y por tanto de respaldarla periódicamente y recuperarla en caso de alguna eventualidad.

- Los usuarios de los equipos PC, son responsables de resguardar sus respaldos en lugares seguros donde no estén expuestos al sol o a la humedad, así como del posible uso que se dé a dicha información por terceros.

Plan de Pruebas

- Un plan de pruebas de recuperación de archivos y sistemas deberá ser implementado por la Dirección de Informática, para asegurar que luego de la toma de respaldos, estos mismos puedan ser utilizados de manera confiable en caso de alguna eventualidad.

- Este plan de pruebas deberá estar calendarizado para efectuar las mencionadas pruebas, contemplando diferentes escenarios de falla de manera que se disminuyan los riesgos en caso de alguna eventualidad que afecte los activos de información de la Institución.

- La Dirección de Informática y las Subgerencias de Informática en Regionales, deberán ser responsables de verificar que los respaldos ejecutados contengan la información correcta (por medio de los códigos de condición y pruebas) y no presenten algún problema para accesarlos nuevamente eligiendo al azar un respaldo y bajándolo a disco con un proceso de verificación por comparación de datos. Esta verificación deberá efectuarse sobre todo a los respaldos de información vital.

Plan de Recuperación de los Centros de Cómputo

- Cada uno de los Nodos que constituyen el Sistema BANRURAL, deberá contar con un plan de recuperación del centro de cómputo en caso de siniestro.

- El plan de recuperación deberá identificar sus escenarios y características propias de cada localidad con la finalidad de Regionalizarlo y satisfacer necesidades particulares de posibles eventualidades.

- El plan de recuperación deberá contar con un grupo denominado “grupo de recuperación en caso de contingencia”, el cual deberá estar formado por personal del área de informática, del área usuaria y del área de servicios generales o equivalente en Regional.

- El Nodo Central deberá proporcionar el “Plan de Recuperación del Centro Nacional de Cómputo” a los Nodos Regionales para tomarlo como ejemplo y elaborar el propio con las características antes mencionadas.

- Cada Nodo, al concluir la elaboración de dicho plan de recuperación Regionalizado, deberá evaluarlo periódicamente para verificar su efectividad y mantenerlo actualizado.

- Cada plan de recuperación como mínimo deberá contar con los siguientes procedimientos:

1) Recuperación de Información vital, a través de medios magnéticos.
2) Recuperación de Información.
3) Recuperación de Comunicaciones.
4) Recuperación de Líneas telefónicas.
5) Recuperación por Problemas en la Red.
6) Recuperación de Sistemas operativos.
7) Recuperación de Bases de datos.
8) Recuperación de Sistemas aplicativos.
9) Recuperación de Archivos.
10) Recuperación de Información de usuario.

IV.8.- Administración de la Red

Administración

La Dirección de Informática y la Subgerencia de Informática en los Regionales, deberán observar el cumplimiento de lo siguiente:

- En cada equipo servidor, organizar, coordinar, instalar, configurar, dar mantenimiento, respaldar, proteger y llevar un seguimiento de la conexión entre las computadoras.

- Serán responsables de la formalización de protocolos de TCP/IP, su configuración y documentación.

- Deberán configurar, equipar e integrar los equipos de Red local bajo su área de responsabilidad.

- Deberán documentar y controlar estadísticas para diseño y planeación de la Red, así como definir elementos de medición para mejorar el rendimiento de la Red de datos.

- Tienen la responsabilidad de optimizar la utilización de las herramientas para el monitoreo y control de los sistemas de comunicación.

- La Dirección de Informática, deberá instrumentar el uso obligatorio de claves confidenciales para servicios de larga distancia. Mediante el sistema de control del servicio telefónico, se identificarán aquellas de carácter personal, mismas que serán cargadas al responsable del aparato telefónico.

- Deben mantener el registro de llamadas que entran y salen a puntos remotos, para efectos de control y administración de la Red de Telecomunicaciones.

- La Dirección de Informática es responsable del diseño, puesta en marcha y optimización de la Red Nacional de Telecomunicación de voz y datos del Sistema BANRURAL.

- Todos los cambios, adiciones de servicios, así como las modificaciones a los servicios existentes o nuevos requerimientos deberán ser solicitados formalmente a la Dirección de Informática.

Operación

La Dirección de Informática y la Subgerencia de Informática en los Regionales, deberán observar el cumplimiento de lo siguiente:

- Tienen la responsabilidad de operar la Red, establecer privilegios, dar de alta y proporcionar mantenimiento a usuarios.

- Deberán proporcionar una clave de acceso al personal usuario de la Red. Esta será única, personal e intransferible por lo que el uso que se dé de ella es responsabilidad del usuario directo de la misma.

- El personal usuario de la Red deberá conocer y acatar los lineamientos existentes para la operación de la misma.

- Deberán configurar los dispositivos periféricos de comunicaciones, desarrollar utilerías para el manejo del equipo, así como solucionar problemas de los usuarios relacionados con el equipo a su cargo.

- Deberán notificar los cambios que se hagan al entorno de la Red, así como llevar un registro por cada usuario que reporte alguna falla por las modificaciones efectuadas.

- Deberán respaldar aquellos archivos o dispositivos críticos para la operación de la Red. Debido a la sensibilidad de las operaciones, estos respaldos se deberán tomar diariamente en dos copias, de las cuales una la guardará en un lugar seguro bajo llave dentro de las instalaciones del edificio y la otra en una localidad alterna.

- Deberán colocar todos los dispositivos de interconexión (hubs, bridges, routers, paneles de parcheo, etc.) y ubicarlos en una zona de acceso restringida a personal ajeno a la administración de la Red.

- La utilización de los equipos instalados solo se dará dentro de los horarios establecidos, cualquier utilización de éstos fuera del horario establecido requiere de autorización por escrito la Dirección de Informática o de la Subgerencia de Informática en Regionales.

- En el caso de solicitud de servicios no planeados como es el caso de la extensión de algún “servicio de Red” existente, deberán ser solicitados y canalizados a la Dirección de Informática o a las Subgerencias de Informática en los Regionales y Sucursal. Su ejecución estará basada en la disponibilidad de los recursos y a la carga de trabajo existente.

- Las autorizaciones respectivas de los diferentes servicios deberán hacerse siempre por escrito, y deberán ser firmadas para su autorización por el jefe inmediato superior del solicitante y por la Dirección de Informática ó de las Subgerencias de Informática en los Regionales y sucursales. Los equipos de cómputo personal conectados a la Red deberán sujetarse a los lineamientos de seguridad y utilización aquí plasmados.

- Las Subgerencias de Informática de los Nodos Regionales deberán realizar la operación de la Red del Regional y de la Red de Sucursales en su zona.

- Las llamadas de larga distancia que se requieren como parte del trabajo cotidiano del personal en las diferentes instancias del Sistema BANRURAL, deberán efectuarse invariablemente a través de la Red de Telecomunicaciones.

- La transmisión de documentos vía fax entre las áreas del Sistema BANRURAL, deberán realizarse a través de equipos conectados a extensiones del conmutador que cuenten con marcación de tonos.

- El personal encargado del equipo de telecomunicaciones deberá verificar la buena calidad del servicio de transmisión y recepción de la señal de voz y datos.

- Los equipos de telecomunicaciones deberán permanecer encendidos las 24 horas. del día, ya que proveen la comunicación de voz y datos a todo el Sistema BANRURAL.

- En los Nodos Regionales, la operación de conmutadores híbrido-digitales, multiplexores, módems, etc., estará a cargo exclusivamente del personal capacitado, adscrito a las Subgerencias de Informática, quienes serán los únicos autorizados para abrir los gabinetes y remover sus componentes.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán mantener funcional y en operación el equipo y sistemas que se encuentra bajo su responsabilidad.

Contratación y Uso de Líneas

- La Dirección de Informática estudiará y dictaminará la procedencia de contrataciones de líneas terrestres y satelitales para ampliar y modernizar la Red de telecomunicaciones y conjuntamente con la Subdirección Corporativa de Recursos Materiales y Servicios Generales, se encargarán de gestionar los permisos que se requieran para su instalación y puesta en operación.

Instalaciones

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán vigilar que el acondicionamiento de los locales que albergan este equipo cuente con las características requeridas para su adecuado funcionamiento. (procurar que estén a una temperatura no mayor de 23 grados centígrados).

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán verificar que el nivel y características de alimentación eléctrica sean confiables.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán asegurarse de que en los lugares remotos exista una protección física adecuada, especialmente para las terminales, concentradores, multiplexores y procesadores frontales.

- No deberán colocarse objetos en los anaqueles ni sobre el mobiliario que contiene el equipo de telecomunicaciones, ya que esto podría generar mal funcionamiento y/o accidentes.

- Los registros telefónicos deberán mantenerse bajo llave, quedando prohibido realizar conexiones paralelas a extensiones de los conmutadores o líneas directas.

- Con el propósito de asegurar la permanencia del servicio, es responsabilidad de la Dirección de Informática asignar y distribuir fuentes de poder ininterrumpibles a los equipos multiplexor y módem, situadas en lugares remotos, con el propósito de evitar la caída en los enlaces de voz/datos.

- La Dirección de Informática deberá instalar o diseñar controles de Seguridad física para los equipos de Comunicaciones, estos pueden ser cerraduras, guardias, insignias, sensores térmicos, alarmas, aterrizaje de tierra eléctrica o medidas administrativas para proteger los servicios con el equipo relacionado.

- El cableado estructurado de la Red deberá cumplir con las normas ANSI/TIA/EIA.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán establecer una adecuada administración del cableado de la Red local.

Soporte del Sistema

- Cada usuario es responsable de su información y por tanto de la seguridad de la misma y del respaldo de sus propios datos.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán establecer una metodología que se observe estrictamente para efectuar los respaldos, de tal forma que estos permitan restablecer la información en caso de falla o siniestro.

- La Dirección de Informática efectuará la distribución de licencias a cada una de las Gerencias del Banco Nacional de Crédito Rural, además de las distribuidas a nivel Sistema BANRURAL, cubriendo de esta forma todos y cada uno de los equipos de cómputo independientemente de que se encuentren conectados a la Red.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán instalar programas protectores contra virus en el equipo servidor, además de dejar este software disponible en la Red para los usuarios.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán monitorear, detectar, reportar y dar seguimiento a las fallas que se presenten. En caso de detectarse alguna eventualidad deberán iniciar los procedimientos de recuperación respectivos.

- La Dirección de Informática deberá hacer un análisis de propuestas para la implantación de nuevos hardware y software de comunicaciones.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán registrar todas las actividades de las terminales o estaciones de trabajo y serán responsables de la seguridad de cada Subred que se genere.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán proporcionar soporte y apoyo técnico al personal bajo su esfera de influencia, en cada localidad de acuerdo al escalamiento de fallas de este documento.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, serán responsables de mantener actualizada la configuración de la Red de la cual son responsables, documentando cualquier cambio que se haga a la misma.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, serán responsables de la custodia de la documentación de todos los componentes físicos y lógicos, así como de mantener actualizada esta documentación.

Mantenimiento

- Por ningún motivo, personal no autorizado deberá abrir equipos de telecomunicaciones para revisión o reparación de estos.

- El mantenimiento tanto preventivo como correctivo de los equipos e instalaciones de la Red Nacional de Telecomunicaciones ubicados en el Sistema BANRURAL, queda bajo la responsabilidad de la Dirección de Informática.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán verificar que se efectué mantenimiento preventivo periódicamente al equipo bajo su responsabilidad.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán proporcionar un mantenimiento preventivo y constante a la Red.

- No debe realizarse el mantenimiento a la Red en horas de laborables de trabajo, solo en casos de extrema necesidad o por mal funcionamiento.

Administración y Uso del Correo Electrónico

- Es responsabilidad de la Dirección de Informática la administración y control del correo electrónico.

- Los usuarios que requieran una clave de acceso al correo electrónico, deberán solicitarla mediante escrito suscrito por el funcionario del área a la Dirección de Informática.

- El uso del correo electrónico es específicamente para envío y recepción de mensajes relacionados estrictamente con las actividades y funciones institucionales.

- Deberá evitarse el envío de mensajes en forma masiva a los usuarios del correo electrónico tanto internos como externos, salvo que el asunto lo amerite.

- Los usuarios del correo electrónico, no deberán estar inscritos en servicios externos que generen correos automáticos a las cuentas de la Institución.

- El correo electrónico interno del Sistema BANRURAL, solo podrá ser utilizado por personal del Banco, el cual cuente con una clave de acceso autorizada.

- Es conveniente que aquellos archivos de gran longitud que requieran ser enviados por este medio sean compactados, logrando reducir el tiempo de envío.
- Los usuarios del correo electrónico, deberán abstenerse de abrir mensajes de dudosa procedencia.

Administración y Uso de Internet

- La Dirección de Informática es responsable de definir y aplicar los esquemas de seguridad necesarios para proteger los sistemas internos de cualquier acceso por personal ajeno al Sistema BANRURAL.

- El usuario que requiera acceso a Internet deberá solicitarlo por escrito a la Dirección de Informática, justificando la utilización del servicio y mediante oficio suscrito por el funcionario del área que se trate.

- El servicio de Internet deberá ser utilizado específicamente para desarrollar actividades relacionadas estrictamente con las funciones institucionales.

- Las claves de acceso asignadas a los usuarios para la utilización del servicio de Internet son únicas, personales e intransferibles, por lo que es responsabilidad del usuario el uso que se dé a las mismas.

- Queda estrictamente prohibido efectuar accesos telefónicos a Internet.

- No deberán efectuarse accesos a Internet utilizando cuentas proporcionadas por proveedores de estos servicios.

- Cualquier anomalía detectada por los usuarios de estos servicios, deberá notificarse a la Dirección de Informática.

- Las áreas usuarias deberán notificar por escrito a la Dirección de Informática, de cualquier movimiento de personal que tenga que ver con el acceso a Internet y de cualquier resignación o cambio de ubicación del equipo computo, debido a que éste está en estrechamente relacionado con la clave de acceso para la utilización del servicio.

- Se prohíbe el uso de cuentas que proporcione cualquier proveedor de acceso a Internet o tercero que ofrezca este tipo de servicios.

IV.9.- Administración de la Seguridad

Los siguientes puntos son responsabilidad de la Dirección de Informática y de las Subgerencias de Informática de los Regionales:

Seguridad Física

La seguridad física deberá cubrir los siguientes puntos:

- Ubicación física.
- Consideraciones en la construcción y edificio.
- Áreas de acceso restringido.
- Instalaciones eléctricas.
- Sistema de alarma y detección.
- Señalizaciones.
- Documentación.
- Auditoría.

Ubicación física de los centros de Cómputo

Respecto a la ubicación del centro de cómputo dentro del edificio:

- Deberá efectuarse un estudio para seleccionar el lugar mas seguro dentro del edificio para instalar el Centro de Cómputo.
- Deberá contar con alimentaciones eléctricas, acometidas telefónicas, servicios públicos y de emergencia, adecuados e independientes.

Consideraciones en la construcción y edificio

Respecto al edificio

- Deben existir espacios disponibles para la instalación de equipos de soporte y auxiliares.
- Deberá contar con acceso para la entrada y salida del equipo sin que este sufra ningún daño.
- Deberá tener capacidad eléctrica adecuada e independiente.
- Contar con pararrayos.

- La zona en que se ubica el edificio que alberga el centro de cómputo, deberá contar con facilidades de comunicación (telefonía, transporte, vías de comunicación accesibles).

Respecto al centro de cómputo en general

- El material de techos, paredes y pisos deberá ser de material incombustible e impermeable.

- Debe tener un mínimo de ventanas exteriores a fin de evitar interferencias y reducir la posibilidad de accesos no autorizados.

En cuanto a Soporte Ambiental, el Centro de Cómputo deberá:

- Contar con un sistema de aire acondicionado para el Centro de Cómputo independiente del requerido por el edificio o inmueble.

- Contar con instrumentos que midan la temperatura de operación de los equipos, la cual debe oscilar entre 18 y 22 grados centígrados, así como la humedad relativa, la cual debe ser de 50% con desviación de hasta 5%.

- Instalar un control de potencia independiente del aire acondicionado del edificio para el Centro de Cómputo.

- Contar con equipo de filtrado de aire fresco antes de llevarlo al área de operación del Centro de Cómputo.

- Verificar que se proporcione mantenimiento al sistema de aire acondicionado, **de acuerdo a las especificaciones del proveedor al respecto**.

- Generar un medio ambiente de temperatura y humedad controladas en el área. Mantener diagramas de humedad por medio de un registrador continuo.

Respecto a la cintoteca

- Construirla con un rango de resistencia al fuego de por lo menos 4 horas.

- Utilizar la cintoteca únicamente para este fin.

Áreas de Acceso Restringido

- Los centros de cómputo deberán contar con las características de seguridad física mencionadas.

- Los centros de cómputo ó áreas que alberguen equipos de cómputo, deberán ser áreas de acceso restringido.

- Considerar el Centro de Cómputo como área restringida a personal no autorizado, además que de acuerdo a los recursos disponibles deberá contar con un mecanismo de control de acceso adecuado: mecánico, eléctrico o electrónico.

- Solo personal autorizado tendrá acceso a estas áreas restringidas. Específicamente para el Centro de Cómputo se deberá controlar la entrada del personal autorizado (personal de la Institución o ajeno a esta) con gafete o algún otro medio de identificación.

- El personal que trabaja dentro del área de acceso restringido deberá registrarse en una lista de asistencia.

- Determinar al personal facultado para autorizar los accesos al Centro de Cómputo y salida de suministros.

- Se deberá contar con mecanismos para controlar la entrada y salida de suministros, dispositivos magnéticos, equipo e información procesada.

- Se deberá contar con una sola entrada de acceso al Centro de Cómputo, misma que si es posible, deberá ser controlada las 24 horas durante los 365 días del año, el resto de las puertas deberán ser utilizadas como salidas de emergencia.

- Cualquier acceso al interior de un área restringida por personal ajeno a esta, deberá autorizarse y registrarse en la bitácora de accesos, además se le deberá proporcionar un gafete que lo identifique como visitante, el cual deberá portar en un lugar visible durante su permanencia en las instalaciones.

- Se prohíbe el uso de teléfonos celulares dentro del centro de cómputo.

- De ser posible instalar circuito cerrado de televisión.
- Deberá indicarse al personal las prohibiciones y restricciones dentro del Centro de Cómputo y áreas restringidas, tales como: evitar comer, fumar o beber en el área donde se encuentre instalado el equipo de cómputo, así como en las áreas destinadas al resguardo de cintas o discos.

- Los visitantes deberán portar un gafete que los identifique como tales al interior de las áreas de acceso restringido, mismo que se les proporcionará a su ingreso a cambio de una identificación personal vigente, y que les será cambiado al momento de su salida.

- Todos los objetos como bolsas de mano y maletas deberán ser revisados por el personal de seguridad al ingresar a las instalaciones del Banco y áreas de acceso restringido, con esto se evita la introducción de elementos que pudieran poner en peligro la integridad de personas y activos de información, de igual manera, se deberán revisar a la salida de las instalaciones para evitar la extracción no autorizada de equipo de cómputo o de material de valor para el Banco.

Instalaciones eléctricas

- Las instalaciones eléctricas de los equipos de cómputo deberán cubrir las especificaciones del fabricante del equipo, asegurando con esto la prevención de daño físico.

- Deberá contarse con dos sistemas de alimentación de energía independientes, donde cada uno de ellos tenga su propia tierra física, uno se utilizará exclusivamente para los equipos y sistemas de cómputo, telecomunicaciones y Redes y el otro para los servicios del área.

- El centro de carga o acometida (tableros) y distribución de energía para el Centro de Cómputo deberá quedar dentro del área donde se encuentren instalados los equipos, mismo que deberá tener los señalamientos de identificación para cada pastilla o circuito de protección.

- No deberán existir cables de energía sueltos, contactos en mal estado o sin tierra física. En caso de observar alguna anomalía o falla deberá reportarla al Área de mantenimiento, dependiente de la Subdirección Corporativa de Recursos Materiales y Servicios Generales ó su equivalente en Regional.

- Para salvaguardar la integridad de los equipos se deberá contar con un sistema de protección de energía, denominado “Sistema ininterrumpible de energía” (No-Break) ó bien contar con reguladores de voltaje para los equipos microcomputadores.

- Se deberá contar con plantas de emergencia en los centros de cómputo Nacional, Espejo, Nodos Regionales y Sucursales en caso de interrupción de energía eléctrica.
- Proteger las conexiones eléctricas y las cajas de los circuitos que alimenten a los Sistemas de Aire Acondicionado.

Sistemas de Alarma y Detección

Respecto a la Protección para Prevenir Daños Provocados por Fuego

- El área del Centro de Cómputo deberá contar con un sistema de alarma y detección de incendio, mismo que proporcionará un mayor nivel de seguridad para empleados, equipos e información contenidos en el área.

- El sistema de alarma deberá contar con detectores de humo capaces de identificar los distintos tipos de gases que desprendan los cuerpos en combustión, indicando la presencia de fuego en su etapa incipiente y proporcionar una alarma que señale el punto de origen a fin de extinguirlo. Será necesario colocar detectores de humo y calor abajo del piso y en los conductos de aire acondicionado.

- Este sistema deberá contar con los elementos necesarios (detectores de humo, luz y bocinas), programados por zonas, de manera que cuando se activen dos sensores en diferentes zonas se active el sistema de alarma (luz y bocinas), que alerten al personal de una situación de fuego en el área.

- Deberá contar con liberación automática y/o manual de Bióxido de Carbono para eliminación del fuego sin daño a las personas y equipo electrónico.

- Se deberá contar con extintores portátiles y distribuirlos estratégicamente dentro del Centro de Cómputo.

- Se deberá contar con el inventario mínimo indispensable de material combustible en el Centro de Cómputo. (Papel, cajas de cartón, etc.).

- El sistema de detección no deberá interrumpir la corriente de energía eléctrica del equipo de cómputo, a menos que el daño sea producido en dicho sistema.

Respecto a la Protección para Prevenir Daños Provocados por Agua

- Se deberá contar con ductos y equipos de bombeo adecuados.

- Se deberán tener cubiertas apropiadas para el equipo, muebles y armarios los cuales se usarán en casos de emergencia.

- Se deberán realizar revisiones periódicas para sellar orificios en paredes, techos y ventanas con el fin de prevenir filtrados de agua.

- Las tuberías de agua deberán estar aisladas de manera que no tengan escurrimientos cerca o sobre el equipo de cómputo o de los materiales relacionados con el equipo de cómputo.

- Deberá verificarse que todo el cableado instalado en los equipos de cómputo se encuentre en buenas condiciones para evitar cortos circuitos en caso de filtraciones de agua inesperadas.

Señalización

- Deberá existir señalización que indique claramente las rutas de evacuación, prohibiciones y zonas de seguridad en áreas comunes, para las áreas de acceso restringido se deberá seguir la misma norma.

- El responsable del Centro de Cómputo deberá verificar el estado operativo y funcional de los sistemas de seguridad y de los elementos de extinción de fuego (hidrantes, boquillas y extintores), mismos que deberán estar claramente identificados, al igual que las salidas de emergencia.

- Los elementos de extinción de fuego deberán cumplir con las normas establecidas por el Departamento de Bomberos de la localidad donde se encuentre ubicado el Centro de Cómputo.

Documentación de Seguridad

- Los documentos que contengan los procedimientos específicos de seguridad de los activos de información deberán cumplir con la Guía para la Elaboración de Documentos y/o procedimientos.

- Las bitácoras de entrada / salida de personas, objetos y equipos de cómputo deberán almacenarse y mantenerse con fines de Auditoría por lo menos un año, cada una de ellas deberá contener anexas las autorizaciones respectivas, de manera que un evento relevante de seguridad pueda ser identificado en tiempo y persona.

Auditoría

- Será facultad de la Contraloría Interna efectuar las revisiones que considere pertinentes a las áreas de Informática por parte del Sistema BANRURAL.

- La Dirección de Informática deberá verificar que los procedimientos y eventos relevantes de seguridad contemplen la posibilidad de proporcionar información, datos y/o pistas auditables.

- Los responsables de los Centros de Cómputo de los diferentes Nodos deberán verificar periódicamente la seguridad física y lógica del mismo, con la finalidad de que cuando se presente una Auditoría se cumplan con los mecanismos de seguridad requeridos.

Seguridad Lógica

- La Dirección de Informática, es responsable de implantar la seguridad lógica mediante esquemas de seguridad a los diferentes usuarios de los sistemas aplicativos.

- Toda aquella documentación que funja como soporte a la seguridad lógica (esquemas de seguridad, oficios de solicitud de modificaciones, listas de modificación de accesos, información de los sistemas y su funcionamiento, pruebas, etc.) deberá ser resguardada por la Dirección de Informática.

- La documentación de pruebas deberá ser un descriptivo para los mecanismos de seguridad, incluyendo los resultados esperados de las mismas y los procedimientos a seguir en caso de que estos no se obtengan.

Accesos.

- Solo los empleados del Sistema BANRURAL deben tener acceso a las estaciones de trabajo.

- Cada usuario deberá contar con una clave de acceso personalizada. Para obtenerla deberá requerirla por escrito a la Dirección de Informática mediante la Solicitud de Alta de Usuario y contar con las firmas de autorización de los funcionarios de su área.

- Las Áreas Usuarias deberán sujetarse con todo apego a los lineamientos de operación, explotación, seguridad y control de acceso a los sistemas que operen, informando a la superioridad de cualquier anomalía que se detecte, a fin de reforzar o cambiar las claves de acceso para efectuar diferentes tipos de operación y con ello garantizar la integridad de la información.

- Es responsabilidad de la Dirección de Informática, proporcionar el login y password inicial a los usuarios conectados a los sistemas centrales, previa solicitud por escrito del área que la requiera.

- La Dirección de Informática, proporcionará las claves de acceso tanto a los equipos como a la conexión a las Bases de Datos de acuerdo al perfil y funciones a desempeñar por el usuario.

- Es responsabilidad de los nodos regionales supervisar que los usuarios tanto del nodo Regional como del nodo sucursal, modifiquen periódicamente (cada 30 días naturales) las claves de acceso al sistema OFI.

- Es responsabilidad de la Dirección de Informática supervisar que en todo el Sistema BANRURAL, no existan usuarios repetidos con la misma clave de acceso.

- En caso de detectar que algunas claves de usuarios están repetidas en sucursales diferentes dentro de un mismo Regional, estas ocurrencias deberán depurarse. De ser estrictamente necesario y mediante previa justificación, que un empleado coexista en más de una sucursal, no deberá estar registrado con la misma clave de usuario, habrá de considerar la opción definida para el caso de requerir múltiples claves de usuario determinada por la Dirección de Informática .

- Es responsabilidad de los usuarios, confirmar que las claves de acceso asignadas operen correctamente, debido a que quedaran inutilizadas y serán eliminadas de no acceder a ellas en los días posteriores a su alta.

- La Dirección de Informática, deberá asignar la contraseña ***inicial*** a los usuarios. Los usuarios son responsables de modificar dicha clave tan pronto se firmen en el sistema, de no ser así, se les revocará el acceso.

- Es responsabilidad de cada usuario el uso y modificación de su contraseña. Esta deberá modificarse por lo menos cada 30 días naturales y su conformación no deberá asociarse con nombres, fechas, lugares, etc., que sean familiares para el usuario.

- La clave de acceso deberá constituirse de la siguiente manera:
  La longitud deberá ser de ocho caracteres.
  Al menos dos caracteres numéricos (0-9) y seis alfabéticos (letras mayúsculas o minúsculas). No deberán incluirse ningún otro carácter diferente a los anteriores, ejemplo: $, #, &, etc.
  Como máximo repetir un solo carácter 3 veces (**EEE**99HGU, **E**AR**EE**Y94, etc.)
  Hasta después de 6 modificaciones no se permitirá utilizar una misma clave o password.
  Después de cierto número de intentos no exitosos para introducir la clave correcta o password, la cuenta se bloqueará automáticamente.

- La clave de acceso proporcionada a un usuario es personal e intransferible y por tanto es su responsabilidad el uso que se le dé.

- La Dirección de Informática, deberá asignar controles de acceso a programas, sistemas operativos y aplicativos, debiendo contener la definición de los usuarios por nombre asignado (identificación de usuario), así como de los objetos de información (archivos y programas), contenidos en ellos.

- La Dirección de Informática, es responsable de las altas, bajas y cambios de privilegios de los usuarios en los sistemas bajo su responsabilidad o administración, previa solicitud por escrito del área usuaria, de acuerdo a los perfiles y funciones de cada usuario. Dicha solicitud deberá ser conservada en un lugar seguro, ya que constituye el soporte de la modificación a la seguridad lógica.

- La Dirección de Informática deberá ser notificada por las áreas usuarias de los Sistemas Centrales en un periodo no mayor a una semana, de las bajas de usuarios que se presenten así como de cualquier cambio en los privilegios de acceso de los mismos.

- Las sucursales que realicen algún movimiento de alta o baja de usuarios, deberán reportarlo a la brevedad al nodo central a la Subgerencia de Captación y Servicios Bancarios, que será la responsable de las altas o bajas en la tabla de ejecutivos de la base de datos del equipo central. En caso contrario dichos usuarios no podrán efectuar operaciones en línea con el Sistema.

- Cualquier clave de usuario con acceso a los Sistemas de Aplicativos Centrales, que permanezca inactiva por 30 (treinta) días naturales deberá darse de baja. En caso de que el usuario no la utilice más, o deje de utilizarla por cierto periodo, deberá informar por escrito a la Dirección de Informática, quien se encargará de bloquear los accesos para dicha clave hasta nueva notificación de su parte.

- La Dirección de Informática, es responsable de instrumentar los mecanismos de protección a las claves de acceso a los sistemas.

- Los permisos de acceso provisional para aquellos usuarios que no tengan este privilegio, deberán ser solicitados por escrito, por el responsable del área usuaria que lo requiera, especificando equipo de cómputo y sistema a accesar, nombres de los usuarios, periodo y horario en que se desea utilizar. De ser autorizada dicha solicitud, el área usuaria será notificada por la Dirección de Informática.

Administración de la Red

- Solicitar clave de acceso a la Dirección de Informática mediante oficio suscrito por el funcionario del área que se trate. Esta clave es personal e intransferible.

- El uso de la clave de acceso será responsabilidad del usuario, por lo que cualquier violación a los sistemas podrá ser motivo de sanciones administrativas y/o penales.

- La Dirección de Informática comunicará por escrito al usuario solicitante: la clave, el grupo de seguridad (en su caso) y el password temporal, este último deberá ser modificado por el propio usuario al momento de accesar por primera vez al sistema con la clave asignada e invariablemente se mantendrá en forma confidencial.

- Cada usuario es responsable de su información y por tanto de la seguridad de la misma y del respaldo de sus propios datos.

- La clave de acceso de los equipos microcomputadores que cuenten con este elemento de seguridad, debe hacerse del conocimiento del jefe inmediato superior, para que en caso necesario pueda disponerse del equipo y la información.

- Los servidores NT, no deberán estar protegidos con la contraseña del protector de pantalla.

- Los usuarios de los servidores NT deberán contar con una clave de acceso personalizada y tienen la responsabilidad de suprimir la utilización del usuario “ANONYMUS” en todos los servidores NT de los Nodos Sucursales y laboratorios.

- Los usuarios dados de alta en los equipos NT de sucursales no deberán tener acceso a los equipos centrales de Cómputo vía telnet.

- Es responsabilidad de la Subgerencia de Informática de los Regionales, modificar periódicamente (cada 30 días) las claves de acceso del administrador NT de las sucursales y laboratorios de su respectivo Regional.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán controlar el acceso a la Red terrestre evitando y dando seguimiento a los accesos no autorizados.

- La Dirección de Informática deberá apoyar la operación y solución de problemas de la Red en conjunto con el personal de la Subgerencia de Informática del Nodo Espejo en caso de que se presente alguna eventualidad.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, serán responsables de clasificar las áreas de influencia para cada usuario o grupo de usuarios, ya sean estas comunes o específicas de acuerdo a las restricciones y limitaciones de cada usuario o grupo de usuarios.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán diseñar un entorno operativo funcional y seguro, basado en los requisitos individuales de cada usuario y grupo de trabajo.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán controlar los accesos al procesador por medio de la Red, su arranque y desactivación de estos accesos al inicio y término de la jornada laboral, además de vigilar que los equipos, Redes y sistemas cuenten con protección antivirus.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán supervisar que se realicen cambios periódicos de las claves de acceso, mediante el programa de conexión a una fecha de expiración.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, serán responsables de asignar los permisos de acceso a la Red de Internet cuando estos sean autorizados, limitándolos solo para las Web que se requieran accesar por motivos de trabajo. Identificarán a todos y cada uno de los usuarios con estos permisos.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, serán responsables de la seguridad de los sistemas a nivel de cuentas, nivel de claves o contraseñas de acceso a los sistemas, directorios y archivos, así como de la seguridad e integridad de la información durante los enlaces entre las Redes existentes.

Administración de Sistemas / Administración de Base de Datos

- En los equipos RS6000, SP2 y G40, la Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán efectuar por lo menos una vez a la semana el cambio de password a la clave de acceso del administrador root.

- Cuando el responsable del Centro de Cómputo proporcione a los usuarios su clave de acceso o modificación de privilegios, deberá acompañarla de un documento que plasme los lineamientos de seguridad, privilegios y funciones de acuerdo a su perfil, el cual deberá ser firmado por el usuario responsabilizándose a cumplir con el contenido de dicho documento.

Respaldos

- La Dirección de Informática o la Subgerencia de Informática en el caso de Regionales, tienen la responsabilidad de mantener en un lugar distinto al edificio donde se encuentra el centro de cómputo, una copia actualizada de la documentación soporte de la seguridad lógica para prevenir alguna eventualidad.
- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán obtener y mantener copias de seguridad del software instalado así como mantener la custodia de los respaldos de los registros históricos y de la información que se considere valiosa.

- La Dirección de Informática y las Subgerencias de Informática en los Regionales, deberán mantener una copia de seguridad en medio magnético de la información de los equipos bajo su responsabilidad, en un lugar distinto al edificio en donde se ubica el centro de cómputo.

- Es responsabilidad de la Subgerencia de Informática, supervisar que se efectúen los respaldos de seguridad y bases de datos, contemplados en el Plan de Recuperación en caso de contingencia para Sucursales del Sistema BANRURAL.

Equipo de cómputo (hardware)

- La utilización de los equipos de cómputo y telecomunicaciones, instalados en el Centro de Cómputo deberá efectuarse en los días y horarios de trabajo, salvo las excepciones establecidas en congruencia con las actividades de la Institución y previa autorización por escrito.

- Cada usuario será responsable del buen uso y cuidado del equipo de cómputo y periféricos que le asigne la Institución y deberá conservar en sus archivos los registros de mantenimiento preventivo y correctivo, manuales y llaves del mismo, así como observar los lineamientos emitidos para este fin.

- En caso de daños o extravío del equipo de cómputo, el usuario deberá dar aviso al área de Seguridad y proceder a levantar el acta administrativa correspondiente.

  Se deberá enviar copia del acta administrativa a la Dirección de Informática y a la Subdirección Corporativa de Recursos Materiales y Servicios Generales en un plazo no mayor de 2 (dos) días.

- En aquellas localidades donde se ubiquen los laboratorios, se deberán seguir los lineamientos descritos para las áreas de acceso restringido.

- Cualquier modificación a los equipos de cómputo (instalación de componentes, movimiento, etc.), deberá canalizarse por medio de la Dirección de Informática.

- Los equipos de cómputo deberán estar invariablemente conectados al No-break o regulador de voltaje; en caso de no contar con este equipo, deberá solicitarlo a la Dirección de Informática.

- Queda estrictamente prohibido destapar los equipos de cómputo o intentar la reparación de cualquiera de sus componentes internos.

- Los mantenimientos y corrección de fallas deberán solicitarse a la Dirección de Informática por medio del centro de soporte (help desk) a la extensión 1294, donde levantarán un reporte para su atención.

- Cualquier modificación a los equipos de cómputo (instalación o desinstalación de componentes), deberá canalizarse por medio de la Dirección de Informática.

- Cualquier equipo o componente que requiera ser retirado temporalmente de las instalaciones, deberá contar con autorización por escrito debidamente firmada por el responsable del área

- Cualquier reubicación de los equipos de cómputo, deberá notificarse a la Dirección de Informática y a la Subdirección Corporativa de Recursos Materiales y Servicios Generales, en un término no mayor a 10 días hábiles.

Software y Sistemas

- Es responsabilidad de la Dirección de Informática evaluar y autorizar el software y los sistemas que deban ser utilizados por el personal del Sistema BANRURAL.

- A la recepción del equipo de cómputo, el usuario deberá recibir por parte de la Dirección de Informática una relación del software instalado. En caso de no contar con dicha relación deberá notificarlo a esta área en un plazo no mayor de 10 días hábiles.
  Los productos contenidos en la citada relación constituyen el único software autorizado que debe residir en el equipo asignado al usuario.

- El usuario sólo deberá utilizar el software autorizado de acuerdo a dicha relación, o en su caso de aquel que se le instale posteriormente de acuerdo a solicitudes y autorizaciones correspondientes.

- Cualquier violación a la Ley Federal del Derecho de Autor es responsabilidad del usuario.

- De acuerdo a la fracción tercera del artículo 47 de la Ley Federal de Responsabilidades de los Servidores Públicos, todos los servidores públicos deberán utilizar los recursos que tengan asignados para el desempeño de su empleo, cargo o comisión, las facultades que les sean atribuidas o la información reservada a que tenga acceso por su función, exclusivamente para los fines a que están afectos.

Conforme a lo anterior, no deberá instalarse software de entretenimiento (juegos) sin excepción, aunque estos cuenten con licencia de uso. En caso de detectarse alguna violación o inobservancia a esta disposición, se notificará a la Contraloría Interna para que en el ámbito de su competencia provea lo conducente.

- En caso de que el empleado sea propietario del equipo de cómputo, únicamente podrá instalar el software que cuente con la licencia de uso correspondiente y le sea autorizado mediante escrito que emita la Dirección de Informática.

- Es responsabilidad de la Dirección de Informática y del Jefe Inmediato del empleado que cuente con un equipo de su propiedad, desinstalar el software licenciado para el Sistema BANRURAL, una vez que dicho equipo cumpla su ciclo de servicio y/o utilización dentro de la Institución.

- El usuario del equipo de cómputo deberá correr cuando menos quincenalmente, los programas antivirus disponibles en la red local conforme al procedimiento que emita la Dirección de Informática.

- No esta permitido el uso de shareware (productos para prueba por un período determinado que genera un costo posterior).

- En caso de que la Dirección de Informática instale o haya instalado software denominado freeware (productos de libre uso), este será considerado como software autorizado y podrá ser utilizado libremente.

- El freeware que se requiera instalar deberá ser autorizado por escrito por la Dirección de Informática.

Diseño y Desarrollo

- Cada usuario será responsable de mantener los sistemas instalados en sus computadoras en buen estado, quedando prohibido el hacer cualquier tipo de modificación a los mismos.

- Cualquier requerimiento ó adición de software deberá estar debidamente justificada y ser solicitada por escrito a la Dirección de Informática.

- Los desarrollos originales de software que sean creados utilizando los equipos e instalaciones del Banco ya sea este, desarrollado por personal de BANRURAL o personal contratado de manera externa, será propiedad de la Institución, quién gozará de los derechos legales sobre este software.

- Cualquier desarrollo original deberá ser evaluado y autorizado por la Dirección de Informática previo a su implantación y/o utilización.

- Las adecuaciones o actualizaciones a los programas deberán contar con su módulo de seguridad para ser liberados dentro de los sistemas de la Institución, además de su documentación técnica y de usuario respectivamente para la propia operación y/o aplicación de los mismos.

- Los sistemas aplicativos deberán contar con la posibilidad de ser auditados.

Control de Versiones

- La actualización y distribución de nuevo software deberá hacerse desde el Nodo Central.

- El Nodo Central deberá llevar el control de versiones.

- Las actualizaciones de programas de software antivirus deberán solicitarse a la Dirección de Informática, quien las pondrá a disposición de cada Gerencia del Banco Nacional, del personal de enlace, a nivel Sistema BANRURAL y en la Red.

- La Dirección de Informática y las Subgerencias de Informática de los Nodos Regionales, son responsables de mantener un inventario de su propio equipo y software instalado en ellos, así como de las respectivas licencias de uso.

Recursos Humanos

- Los empleados del Banco deberán portar su gafete de identificación en lugar visible mientras se encuentren en las áreas de acceso restringido.

- La Dirección de Informática en conjunto con las Áreas de Comunicación Social y Recursos Humanos y Servicio Médico, deberán establecer programas permanentes de información acerca de tópicos de seguridad al interior de la Institución.

- Los usuarios son responsables de los equipos que tengan resguardados, así como de su propia clave de acceso y del uso que se les dé a los mismos.

- El personal de la Dirección de Informática, de Recursos Materiales, y de las áreas usuarias deberá participar en la creación y aplicación de los Planes de Recuperación en caso de siniestro del Nodo correspondiente a su respectiva localidad.

IV.10.- Clasificación de la Información

Identificación de la Información

- Es responsabilidad del área generadora / usuaria de la información identificar y clasificar su información de acuerdo al grado de sensibilidad, importancia y nivel de seguridad que requiera.

- La Dirección de Informática, deberá identificar tanto sus sistemas aplicativos como la documentación técnica y de usuario que generan, de acuerdo a la normatividad aquí expuesta.

- La Dirección de Informática, deberá identificar y clasificar la información que generen los sistemas a su cargo, es responsable de su custodia y del uso que se dé a la misma.

- La Dirección de Informática y las Subgerencias de Informática, deberán identificar y clasificar la información y respaldos que generen.

- Únicamente se manejará, procesará y utilizará la información que se encuentre debidamente identificada y clasificada de acuerdo a los lineamientos de "Clasificación de Información" aquí expuestos.

Clasificación de la Información

- Los lineamientos aquí expuestos deben aplicar para toda la información que maneja el Sistema BANRURAL sobre cualquier medio o dispositivo.

- Los usuarios que tengan permiso de acceso a la información clasificada, automáticamente se convierten en custodios y responsables del uso que se dé a esta.

- La toma de decisiones sobre la información que se maneja en la Institución deberá hacerla solo el personal autorizado para este fin, por lo que los usuarios deberán comunicarle a sus superiores de dicho acontecimiento.

- La clasificación de la información deberá hacerse de acuerdo a la siguiente tabla que presenta los datos que deben incluirse:

Número o Color de Etiqueta	Tipo de Uso	Secuencia	Vigencia
1.- Rojo = Confidencial Restringido	A = Respaldo	Del 1 a n ó 1 de n	De: **dd-mm-aa** A: **dd-mm-aa**
2.- Naranja = Confidencial	B = Producción		
3.- Amarillo = Uso Interno	C = Pruebas		
4.- Verde = Público			

Número o Color de Etiqueta: Se debe seleccionar aquel que identifique claramente el nivel de seguridad, confidencialidad y valor de la información para la Institución.

Tipo de uso: Se debe utilizar la letra que describa la utilización que se le dará a la información.

- **Secuencia**: Debe indicarse si se trata de un solo dispositivo que contiene dicha información o si forma parte de un grupo.

- **Vigencia**: Deberá indicarse el periodo de vida útil y de última actualización de la información de tal forma que sea posible identificarla y en caso de vencer su vigencia, depurar dichos dispositivos.

- El personal que trabaje con información "vital" para la Institución, deberá etiquetarla como "confidencial restringido"

- El área generadora / usuaria deberá clasificarla mediante el número ó color de etiqueta, tipo de uso, secuencia y vigencia.

Controles Internos de la Información

- El área generadora / usuaria es quien conoce mejor su propia información, por lo tanto deberá establecer los controles internos para la misma.

- El área generadora / usuaria es responsable de asignar el acceso a la información, así como verificar que las modificaciones que se hagan a la misma sean debidamente aprobadas y autorizadas por escrito por dicha área.

Cambio de Clasificación

- El área generadora y/o usuaria es quien deberá autorizar un cambio en la clasificación de su información.

- La Dirección de Informática, es responsable de cambiar la clasificación de los sistemas aplicativos o bien de autorizar por escrito que se efectúe dicha modificación.

- Al cambiar la clasificación de la información dentro de un sistema o ambiente de cómputo, este debe acompañarse siempre de la documentación soporte que apoye dicha modificación.

- Los responsables de cada área deberán informar a la Dirección de Informática cualquier movimiento o cambio en las responsabilidades o clasificación de su información.

- Los operadores de los equipos de cómputo de los diferentes centros de cómputo de la Institución no podrán modificar la clasificación de la información a menos que se reciba una instrucción por escrito del propietario de la misma y del jefe inmediato superior de éste, debidamente firmada por ambos.
- El personal de los centros de cómputo no proporcionarán la rotulación externa de la clasificación a los dispositivos que contienen información clasificada, el área generadora / usuaria de la información es responsable de efectuar esta rotulación indicando la modificación en su clasificación.

Responsabilidades y Custodia de la Información

- Es responsabilidad de la Dirección de Informática y de las Subgerencias de Informática en los Regionales la seguridad y protección de la información clasificada que se maneja en sus respectivos nodos, así como también el encargarse de que se cumplan las políticas de Clasificación de la Información.

- Los responsables de cada área deberán asegurarse de la devolución de toda la información clasificada cuando alguna de las personas bajo su cargo o responsabilidad cese su relación laboral con la Institución o sea transferido a otras responsabilidades dentro del Banco.

- Las áreas generadoras ó usuarias de la información son las responsables de custodiarla adecuadamente de acuerdo a sus propias necesidades de seguridad.

- Es responsabilidad del área generadora y/o usuaria de la información participar en el desarrollo del plan de recuperación en caso de contingencia del Centro de Cómputo de su localidad, en lo relacionado con el apartado de clasificación de información.

- Cada área usuaria / generadora de información debe llevar un control escrito sobre el personal que designe como responsable y/o custodio de la información.

- El área generadora y/o usuaria es responsable de su información y por lo tanto es quien podrá autorizar la custodia de la misma a otra área o personal.

- Todo el personal involucrado que trabaje con información clasificada, será responsable del uso y seguridad que se dé a la misma.

- El personal del centro de cómputo tiene la responsabilidad de seguir las políticas de manejo de información clasificada, y de anotar y reportar cualquier incidente en referencia a esta información que se suscite durante su estancia en el área del centro de cómputo, de manera que siempre quede un registro de estas incidencias, para efectos de Auditoría.

- La información que es proporcionada a la Institución por parte de sus clientes, proveedores y empleados deberá manejarse confidencialmente.

Monitoreo

- La Dirección de Informática, deberá supervisar que se cubran los requerimientos de seguridad para los procesos que modifiquen información.

- El área generadora y/o usuaria y la Dirección de Informática, son responsables de los procesos involucrados con su información, serán quienes periódicamente deberán hacer revisiones y se asegurarán de que se lleven a cabo Auditorias internas de tal forma que se mantenga actualizada la clasificación de la información.

- La Dirección de Informática, deberá efectuar una revisión anual como mínimo a los controles de seguridad.

- La Dirección de Informática y las Subgerencias de Informática en Regionales, deberán difundir las políticas de “clasificación de información” a las áreas generadoras / usuarias, de tal forma que se salvaguarden y administren adecuadamente.

Control y Actualización

- El área generadora / usuaria deberá llevar un estricto control sobre la clasificación de su información y las actualizaciones que generen, de tal forma que el personal trabaje siempre con la última versión.

- En los casos que sea necesario, debido a la confidencialidad de la información, el personal deberá firmar un convenio de no divulgación donde se estipulen claramente las consecuencias y sanciones en caso de no cumplirse.

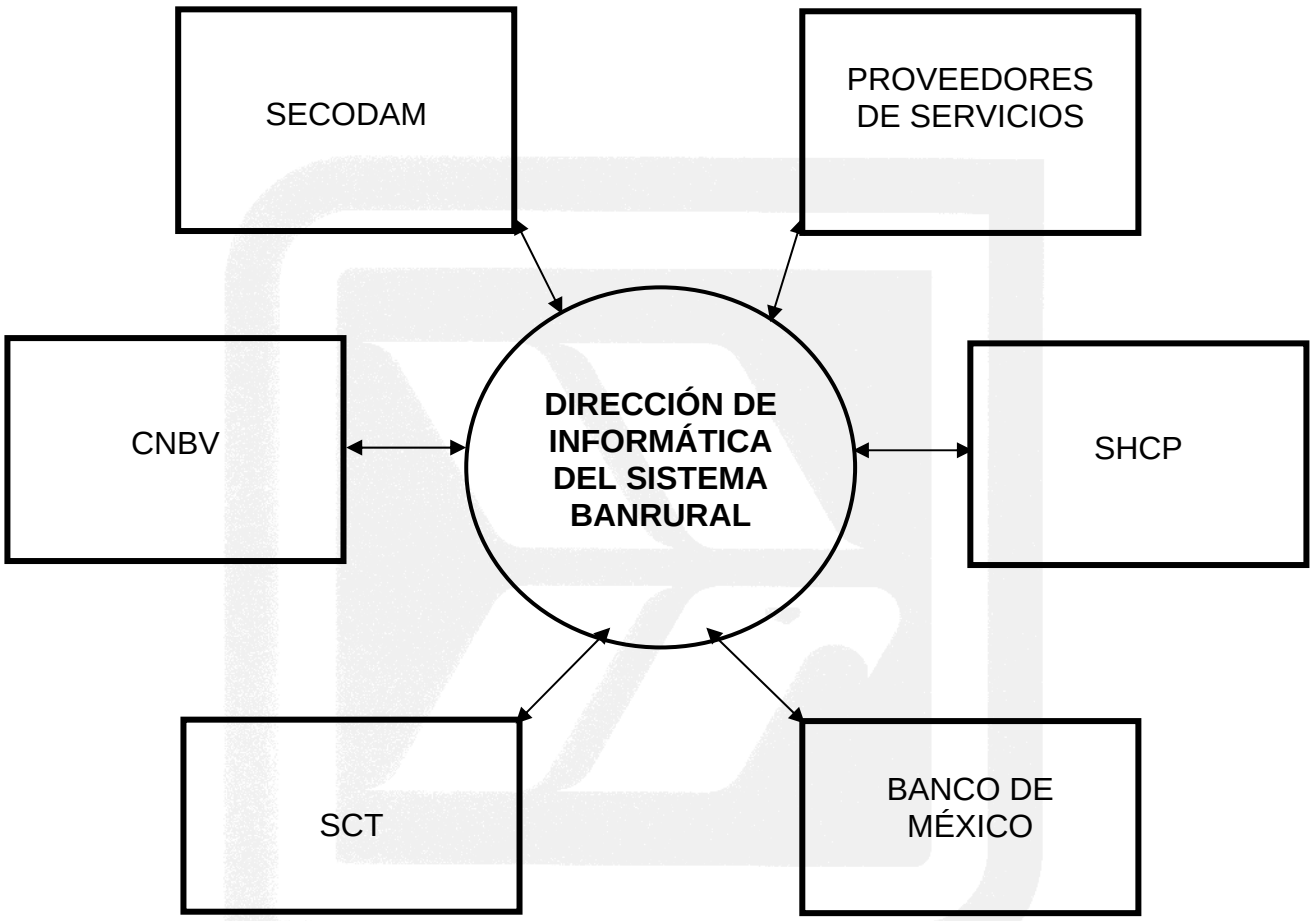
- La Dirección de Informática, deberá llevar un estricto control sobre las versiones de aplicativos que libera, verificando que se actualice la información de acuerdo a la última versión.

- La Dirección de Informática, deberá establecer los procesos de riesgo para las aplicaciones así como las respectivas modificaciones.

V.- DIAGRAMA DE ENTIDAD – RELACIÓN

INTERNA

EXTERNA


SECODAM
PROVEEDORES DE SERVICIOS
CNBV
DIRECCIÓN DE INFORMÁTICA DEL SISTEMA BANRURAL
SHCP
SCT
BANCO DE MÉXICO