

BANCO CENTRAL DE LA REPÚBLICA ARGENTINA



COMUNICACIÓN “B” 9042	24/07/2007
-----------------------	------------

A LAS ENTIDADES FINANCIERAS,
A LAS CÁMARAS ELECTRÓNICAS DE COMPENSACIÓN:

Ref.: Comunicaciones “A” 4690 y “C” 48583. Actualización de texto ordenado.

Nos dirigimos a Uds. con el objeto de hacerles llegar las hojas que corresponde reemplazar en el texto ordenado de las normas sobre “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con Tecnología Informática y Sistemas de Información y recursos asociados para las entidades financieras” cuya actualización fuera divulgada mediante las Comunicaciones “A” 4690 y “C” 48583.

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Marcelo D. Fernández
Gerente de
Auditoría Externa de Sistemas

Pablo L. Carbajo
Subgerente General de Análisis
y Auditoría

ANEXO



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 2. Organización funcional y gestión de tecnología informática y sistemas.

2.5.4. Actividades y segregación de funciones. Incompatibilidades.

	Análisis funcional / Programación	Control de calidad	Operaciones	Administración de resguardos	Implementaciones	Data Entry	Administración de bases de datos	Administración de redes	Administración de telecomunicaciones	Administración del sistema operativo	Mesa de ayuda	Usuario final	Asignación de perfiles	Definición e implementación de políticas, perfiles y accesos	Control y monitoreo de seguridad informática
Análisis funcional / Programación		X	NO	NO	NO		NO	X	X	NO		NO	NO	NO	NO
Control de calidad	X		NO	NO	X	X	NO	X	X	NO	NO		NO	NO	NO
Operaciones	NO	NO			X	NO	X	X	X	X		NO	NO	NO	NO
Administración de resguardos	NO	NO			X	NO	NO			X	NO	X	NO	NO	NO
Implementaciones	NO	X	X	X		NO	NO			X	X	NO	NO	NO	NO
Data Entry		X	NO	NO	NO		NO	X	X	X	X		NO	NO	NO
Administración de bases de datos	NO	NO	X	NO	NO	NO				X	X	NO	NO	NO	NO
Administración de redes	X	X	X			X						NO	NO	NO	NO
Administrador de comunicaciones	X	X	X			X						NO	NO	NO	NO
Administración de sistemas operativos	NO	NO	X	X	X	X	X					NO	NO	NO	NO
Mesa de ayuda		NO		NO	X	X	X					NO	NO	NO	NO
Usuario final	NO		NO	X	NO		NO	NO	NO	NO	NO			NO	NO
Asignación de perfiles	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO				
Definición e implementación de políticas, perfiles y accesos	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			
Control y monitoreo de seguridad informática	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO			

Versión: 1a.	COMUNICACIÓN "A" 4609	Vigencia: 27/12/2006	Página 4
--------------	-----------------------	-------------------------	----------



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 2. Organización funcional y gestión de tecnología informática y sistemas.

2.5.5. Glosario de funciones descritas en el cuadro del punto 2.5.4.:

Análisis de sistemas / programación: diseño y desarrollo de los sistemas aplicativos, de acuerdo con las necesidades del negocio y del usuario.

Control de calidad: prueba y homologación de software de aplicación para la puesta en producción.

Operaciones: gestión operativa del procesamiento de información y el equipamiento afectado.

Administración de resguardos: custodia, guarda y mantenimiento de los archivos de datos y programas almacenados en distintos medios.

Implementaciones: puesta en producción de sistemas aplicativos.

Data entry: recepción y carga a los sistemas de lotes de información para su posterior procesamiento.

Administración de bases de datos: definición y mantenimiento de la estructura de los datos de las aplicaciones que utilizan este tipo de software.

Administración de redes: administración y control técnico de la red local.

Administración de telecomunicaciones: administración y control técnico de la red WAN.

Administración de sistemas operativos (system programming): mantenimiento del software de sistemas operativos.

Mesa de ayuda: canalización de respuestas a inquietudes técnicas de los usuarios.

Usuario final: aquel que hace uso de los sistemas aplicativos.

Asignación de perfiles: vinculación de los usuarios finales con los perfiles de las funciones que aquellos pueden realizar.

Definición e implementación de políticas, perfiles y accesos: diseño y puesta operativa de las políticas y los procedimientos de seguridad, de la creación y mantenimiento de los perfiles de usuario y de la asignación de los permisos a los activos de información.

Control y monitoreo de seguridad informática: seguimiento de las actividades relacionadas con el empleo de los activos de información.

Versión: 1a.	COMUNICACIÓN "A" 4609	Vigencia: 27/12/2006	Página 5
--------------	-----------------------	-------------------------	----------

B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 3. Protección de activos de información.

Se deberá proteger la integridad de la información registrada en dichos reportes, la que deberá ser resguardada adecuadamente, manteniéndose en archivo por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dichos registros de seguridad o pistas de auditoría, podrá ser inferior a 6 (seis) años. Para ello, se utilizarán soportes de almacenamiento no modificables o soportes reutilizables, siempre que se proteja la integridad de la información con medidas de control que permitan evidenciar la no alteración posterior a su generación. En caso de ser CD (Compact Disc), deberá registrarse oportunamente el número de serie del mismo al momento de generación y/o firmas digitales.

3.1.4.5. Alertas de seguridad y software de análisis.

Las entidades financieras deben implementar funciones de alertas de seguridad y sistemas de detección y reporte de accesos sospechosos a los activos de información, y contar con monitoreo constante de los accesos a recursos y eventos críticos, que reporten a los administradores sobre un probable incidente o anomalía en los sistemas de información.

Asimismo, se considera una sana práctica de seguridad la detección en tiempo real de los eventos o intrusiones, así como la utilización de herramientas automatizadas para el análisis de la información contenida en los registros operativos, de seguridad y de auditoría. De esta manera, se reducirá el volumen de los datos contenidos en los reportes, minimizando los costos relacionados con su almacenamiento y tareas de revisión.

3.1.4.6. Software malicioso.

Las entidades financieras deben implementar adecuados mecanismos de protección contra programas maliciosos, tales como: virus informáticos, “gusanos” de red, “spyware”, “troyanos”, y otros que en el futuro puedan surgir, con el objeto de prevenir daños sobre los datos y la pérdida de información. Deben desarrollar procedimientos de difusión a los usuarios de los sistemas de información y a los recursos humanos de las áreas técnicas, sobre sanas prácticas en materia de prevención.

Deben implementarse herramientas para la prevención, detección y eliminación de este tipo de software en los distintos ambientes de procesamiento, evitando su propagación y replicación a través de las redes informáticas, archivos y soportes de información. Estas herramientas deben actualizarse rutinariamente contra nuevas amenazas.

Deberán definirse controles de seguridad para prevenir la presencia de código malicioso en archivos adjuntos a correos electrónicos y en los accesos a Internet; asimismo, se deberá impedir la instalación y utilización de software no autorizado.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 3. Protección de activos de información.

3.1.5. Responsabilidades del área.

El área será responsable de observar la existencia y correcta aplicación de los controles considerados como práctica recomendada y de uso frecuente en la implementación de la protección de los activos de información. Los mismos comprenden:

- § la existencia de una política de protección de los activos de información, correctamente redactada, formalizada, actualizada y comunicada a toda la entidad;
- § la asignación de responsabilidades operativas en materia de administración de la protección de los activos de información;
- § la comunicación oportuna de incidentes relativos a la seguridad, a los responsables propietarios de los datos;
- § la existencia de procedimientos de control y monitoreo, y su aplicación, sobre el empleo continuo de los estándares fijados de seguridad;
- § la instrucción y el entrenamiento en materia de seguridad de la información.

Adicionalmente, los controles efectuados por el área deben establecerse formalmente a través de reportes operativos, que permitan la supervisión continua y directa de las tareas y el análisis del logro de las metas definidas. Estos reportes deben mantenerse en archivo por un término no menor a 2 (dos) años, utilizando para ello soportes de almacenamiento no reutilizables y preferentemente sometidos a algoritmos de función irreversible o como normalmente se denomina “funciones hash”.

De acuerdo con el marco definido en la política de seguridad informática, las entidades financieras deben desarrollar e implementar controles precisos, oportunos y eficaces sobre las funciones de acceso a los datos y a los recursos de información.

3.1.5.1. Control y monitoreo.

El área de protección de activos de información es la responsable primaria de efectuar las actividades regulares de monitoreo y controles de verificación. La frecuencia de revisión dependerá del valor de la información administrada y del riesgo asociado a la aplicación o servicio tecnológico.

Se deben evaluar los accesos a las funciones de administración y procesamiento de los programas de aplicación y sus registros de datos resultantes. Asimismo, se deben controlar especialmente los usuarios con niveles de accesos privilegiados, su utilización y su asignación.

Los incidentes y debilidades en materia de seguridad deben registrarse y comunicarse inmediatamente a través de adecuados canales de información, con el objeto de analizar sus causas e implementar mejoras en los controles informáticos a fin de evitar su futura ocurrencia.

Versión: 2a.	COMUNICACIÓN “B” 9042	Vigencia: 19/07/2007	Página 7
--------------	-----------------------	-------------------------	----------



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 3. Protección de activos de información.

3.2. Implementación de los controles de seguridad física aplicados a los activos de información.

Los recursos humanos, los equipos, los programas, los archivos y los datos que involucran a las operaciones y procesos de la tecnología de la información representan uno de los activos críticos de las entidades financieras. El Directorio, o autoridad equivalente, es el responsable primario por la existencia de distintos niveles de seguridad física en correspondencia con el valor, confidencialidad y criticidad de los recursos a proteger y los riesgos identificados.

Los datos y equipos considerados críticos deben ser instalados en ambientes conforme a estándares y normas nacionales e internacionales pertinentes, que protejan a los mismos contra fuego, calor, humedad, gases corrosivos, acceso indebido, desmagnetización y todo otro tipo de evento que pueda afectarlos.

El Directorio, o autoridad equivalente, debe considerar el uso de sistemas de monitoreo centralizado en todas las facilidades, con el objetivo de lograr un control preventivo y correctivo de fallas en la seguridad. Además, se valorará la inclusión de dispositivos de video y grabación de eventos en aquellas áreas con mayor concentración de activos de información.

3.2.1. Construcción y localización de las instalaciones.

Será ponderado como una buena práctica en la administración del riesgo que la localización del centro de procesamiento de datos esté en un área que resulte de difícil identificación pública.

No deben admitirse ambientes compartidos que permitan la exposición de las operaciones críticas y de carácter confidencial de la entidad financiera, a personas, materiales u otro tipo agentes externos. Esas operaciones deben realizarse en ambientes seguros, con un nivel de protección probadamente eficaz contra las amenazas de su entorno, con el propósito de preservar la integridad de los datos y dispositivos de hardware.

Las instalaciones del centro de procesamiento de datos, además de los niveles de protección físico-ambiental adecuados, deben tener en cuenta, entre otras, las siguientes consideraciones, relevantes para los controles de seguridad física:

- § instalaciones para equipamientos de apoyo, tales como: equipos de aire acondicionado, grupos generadores, llaves de transferencia automática, UPS, baterías, tableros de distribución de energía y de telecomunicaciones y estabilizadores;
- § instalaciones de montaje apropiadas para los sistemas de telecomunicaciones;
- § instalaciones de montaje apropiadas para los sistemas de suministro eléctrico, tanto primario como secundario;
- § iluminación de emergencia;
- § sistemas de monitoreo y control de las utilidades críticas del centro de procesamiento de datos; y,



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 3. Protección de activos de información.

§ se valorizará toda otra medida adoptada para minimizar los riesgos que afecten a los recursos de tecnología.

3.2.2. Acceso físico a las instalaciones del centro de procesamiento de datos.

Las instalaciones deben tener apropiados controles de acceso, por medio de los cuales se permita sólo el ingreso al área de procesamiento de datos a personal autorizado.

Se valorizará la existencia de varios niveles de acceso para los distintos recintos del centro de procesamiento de datos, basados en las definiciones de necesidad de acceder, en relación con la función o actividad primaria del personal interno o externo a la entidad financiera que solicite el ingreso.

Todos los accesos, de rutina o de excepción, deben ser registrados por mecanismos que permitan la posterior revisión de los siguientes datos como mínimo: nombre completo, relación (interno o externo), en caso de ser externo deberá constar quién ha autorizado el acceso, motivo, hora de ingreso y hora de egreso.

3.2.3. Mecanismos de protección ambiental.

Los sistemas de prevención contra incendios en los ambientes de procesamiento de datos deben posibilitar alarmas preventivas, que tengan la capacidad de ser disparadas ante la presencia de partículas características en el recalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

Los materiales combustibles deben ser minimizados dentro del área del centro de procesamiento de datos. La mampostería, muebles y útiles deben ser constructivamente no inflamables, y preferentemente ignífugos.

Se considerarán como ventajosas la aplicación de sanas prácticas de control para minimizar el riesgo de amenazas potenciales, la implementación de detectores ante: robo, presencia de agua (o falta de suministro), polvo, vibraciones, sustancias químicas, interferencia en el suministro de energía eléctrica, radiación electromagnética; y otras medidas similares.

3.2.4. Destrucción de residuos y de medios de almacenamiento de información

Todos los documentos en papel que contengan informaciones clasificadas como críticas deben ser triturados o destruidos, a efectos de imposibilitar su lectura, antes de ser desechados.

Todos los dispositivos electrónicos que ya no se utilicen, y que hayan sido funcionales para el almacenamiento de información crítica deben ser físicamente destruidos antes de su desecho.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

6.2. Operatoria y control de las transacciones cursadas por cajeros automáticos (ATM's).

El área o sector en el cual se haya delegado la responsabilidad sobre esta operatoria, debe evidenciar la existencia y cumplimiento de las medidas de seguridad y la aplicación de controles específicos sobre los cajeros automáticos y las transacciones que con ellos se realizan. Entre otros que la entidad financiera estime aplicar, los siguientes son los de cumplimiento obligatorio:

- § Los cajeros automáticos (ATM) que conformen una red administrada por una entidad y/o por terceros, deben funcionar en un esquema de proceso en tiempo real y conexión en línea directa (on-line), con el computador que administra la red y la base de datos que opera.
- § En caso de interrupción del vínculo entre un cajero automático y el computador que lo opera, el cajero deberá quedar fuera de servicio para todo tipo de transacciones monetarias hasta la normalización del proceso, no debiendo operar en ningún caso en modalidad fuera de línea.
- § Cuando, por razones contingentes, los cajeros automáticos sólo estén operando en línea con el computador de la entidad, y no con la red que los administra, será responsabilidad de la entidad el mantenimiento y registro de todos los datos y eventos que surjan durante la operación, de igual forma que se registrarían en el computador de la red que los administra.
- § La apertura de los cajeros automáticos debe ser realizada por dos personas, dejando constancia escrita en un acta de su participación y del resultado de la conciliación, balanceo de billetes, conformidad de depósitos, tarjetas retenidas, totales, diferencias si las hubiera, etc. En los casos de dispositivos neutrales, la documentación de respaldo (planillas o formularios de balanceo, de reposición, de tarjetas retenidas, de conciliación y otras) deberá ser firmada, posteriormente, por un funcionario de la entidad financiera, que será la figura responsable para cualquier intervención posterior ante requerimientos de este Banco Central.
- § En las transacciones cursadas por medio de cajeros automáticos que impliquen movimientos de fondos, se deberá emitir el comprobante correspondiente o, como mínimo, se deberá dar al usuario la opción de su impresión. En caso de que el cajero automático haya agotado el papel para la impresión de los comprobantes, el mismo deberá quedar fuera de servicio para ese tipo de transacciones.
- § Los cajeros automáticos, en todos los casos, deben imprimir en tiempo real una cinta de auditoría, donde quede reflejada toda su actividad (consultas, transacciones, mensajes del software y estado de los sensores, etc.) con detalle de fecha, hora e identificación del cajero automático. Preferentemente, la misma deberá estar alojada en el interior del cuerpo del cajero.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

Estas cintas de auditoría deben reunir todas condiciones de seguridad e integridad en relación con la no alteración del estado registrado originalmente, con el fin de garantizar su confiabilidad y mantenerse en guarda por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dichas cintas de auditoría podrá ser inferior a 6 (seis) años, debiendo estar disponible en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias lo requiera para su control.

En el caso de utilizarse papel de transferencia térmica, la entidad deberá garantizar su lectura sin pérdida de legibilidad, durante todo el período de guarda. Dicha característica deberá ser evidenciable en todo momento, bajo su entera responsabilidad.

Se podrá optar, como medio alternativo a la cinta de auditoría, por la grabación de todos los eventos a través de medios electrónicos y/u ópticos de escritura de única vez, como ejemplo: *compact discs* no reutilizables (CD). En este caso los sistemas de los cajeros automáticos deben registrar, al momento de recambio del CD, el número de serie del mismo, mediante el uso de algoritmos de función irreversibles (denominados de “*hashing*”). El valor obtenido deberá incluirse como un dato más en el ticket provisto al cliente, y dentro de cada movimiento o mensaje emitido por el cajero automático.

- § Se deben registrar, en tiempo real, todas las transacciones y mensajes del sistema que administra a los cajeros automáticos, para uso de los responsables del control y de la auditoría. Este registro debe reunir todas las condiciones de seguridad e integridad en relación con la no alteración del estado registrado originalmente, con el fin de garantizar su confiabilidad y conservación por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dicho registro podrá ser inferior a 6 (seis) años. Además, deberá estar disponible en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias lo requiera para su control.

- § La operación de los cajeros automáticos por parte de los usuarios deberá basarse en un sistema de identificación de dos factores, en la actualidad tarjeta y clave de identificación (PIN).

Se deben fijar medidas para establecer apropiadamente la clave de identificación del cliente, con una longitud no inferior a la estandarizada internacionalmente para el uso en cajeros automáticos.

- § Las claves de identificación deben gestionarse y administrarse manteniendo su confidencialidad en todas las instancias. Deberán estar encriptadas en todos los lugares en que se alojen o transmitan, y se restringirá su acceso con apropiados y justificados niveles de seguridad.
- § Los programas, los archivos y los medios magnéticos que contengan fórmulas, algoritmos y datos utilizados en la generación de la clave de identificación para ser utilizada en los cajeros automáticos deben estar sujetos a medidas de seguridad que garanticen la confidencialidad y no divulgación de los mismos.

Versión: 2a.	COMUNICACIÓN “B” 9042	Vigencia: 19/07/2007	Página 3
--------------	-----------------------	-------------------------	----------



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

- § Los procedimientos utilizados para el embozado de tarjetas y la generación de las claves de identificación personal deben contemplar una adecuada separación de funciones, a fin de no concentrar en un mismo sector o funcionario ambas actividades. Además, debe evitarse que permanezcan en un mismo sitio, o en poder de un mismo responsable, ambas partes.
- § En aquellos casos que por cualquier causa una tarjeta sea retenida por un ATM, la entidad responsable de este último deberá regularizar la situación planteada ante la entidad emisora de la tarjeta, en el lapso de 48 horas. Una vez producido esto, el cliente dispondrá de 20 días hábiles para retirar la misma. Transcurrido dicho lapso, la tarjeta deberá ser destruida y se confeccionarán los registros pertinentes que evidencien la correcta destrucción de la misma. Esto último es aplicable también para aquellas situaciones en que la entidad haya emitido una tarjeta de débito y el cliente no la haya retirado dentro del mencionado plazo, el cual se computará a partir de su puesta a disposición.
- § Los procesos de generación e impresión de las claves de identificación personal deben asegurar que las mismas no aparezcan impresas, ni puedan ser visualizadas y/o asociadas al número de cliente, cuenta y tarjeta, a fin de garantizar su estricta confidencialidad.
- § Las claves de identificación personal y las tarjetas no deben ser entregadas en forma conjunta, deben formar parte de procedimientos separados. En caso de que la entidad financiera utilice terceras partes para la distribución de las mismas, será la responsable de controlar que éstas no queden en depósito del proveedor de los servicios de entrega en forma conjunta.
- § Los sistemas de seguridad, aplicativos y operativos que operen con los cajeros automáticos y requieran el ingreso de la clave de identificación personal, deben restringir el acceso del cliente después de tres intentos de acceso fallido. Sólo deben reactivarlo por solicitud del titular de la cuenta asociada a la clave de identificación personal, comprobando fehacientemente su identidad en forma previa. La reactivación deberá basarse en la asignación de una nueva clave de identificación personal, con la obligatoriedad de que el usuario del sistema la cambie una vez ingresada. La asignación de la nueva clave deberá seguir los procedimientos de seguridad, y no podrá ser comunicada verbalmente al usuario.
- § Cada operación realizada por los cajeros automáticos debe tener asociada un número de transacción, el cual deberá ser informado en el comprobante que recibe el usuario.

Toda práctica aplicada a efectos de mejorar la seguridad y la confianza de los sistemas de cajeros automáticos, y la identificación y autenticación de los usuarios, como el uso de tarjetas inteligentes, identificación biométrica u otra tecnología relacionada, será valorizada a sus efectos.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

6.3. Operatoria y control de las transacciones cursadas por medio de puntos de venta (POS) utilizando débito directo en cuentas con tarjetas de débito.

La operatoria realizada por medio de puntos de venta (POS) con el uso de las tarjetas de débito en cuenta, conllevan un importante nivel de riesgo operacional. Para minimizar la exposición al mismo, las medidas de seguridad aplicables, obligatorias o sugeridas, según corresponda, serán:

- § Las entidades deben requerir a los comercios asociados a la red de puntos de venta que soliciten al cliente la presentación de su documento de identidad, a efectos de verificar la correspondencia con el titular de la tarjeta de débito.
- § Se sugiere que la tarjeta de débito, habilitada para realizar compras a través de puntos de venta, permita la asociación de una clave de identificación personal distinta a la utilizada para el resto de los canales electrónicos (cajeros automáticos, banca por Internet, otros).

Se sugiere que las transacciones de compra requieran el ingreso de la clave de identificación personal. Para las operaciones superiores a \$ 20.-, será obligatoria la emisión de un comprobante que deberá ser firmado por el titular de la tarjeta, quedando una copia en poder del mismo.

- § Cuando las entidades financieras decidan utilizar claves de identificación personal en las transacciones de tarjetas de débito en cuenta, los sistemas de seguridad, aplicativos y operativos que operen con los sistemas de punto de venta, deben restringir el acceso para la realización de transacciones después de tres intentos de acceso fallido. Sólo deben reactivarlo por solicitud del titular de la cuenta asociada a la clave de identificación personal, comprobando fehacientemente su identidad en forma previa.
- § Se deben registrar, en tiempo real, todas las transacciones y mensajes del sistema que administra los puntos de venta, para uso de los responsables del control y de la auditoría. Este registro debe reunir todas condiciones de seguridad e integridad en relación con la no alteración del estado registrado originalmente, con el fin de garantizar su confiabilidad. Se conservará por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dicho registro podrá ser inferior a 6 (seis) años, y deberá estar disponible en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias lo requiera para su control.
- § En todos aquellos casos en los que la operación no esté asociada a una clave de identificación personal, ante el desconocimiento de las transacciones por parte del cliente, se deberá proceder a la inmediata devolución de los fondos al mismo. Similar situación deberá ocurrir en aquellas operaciones inferiores a \$ 20.-, en las que se hubiera optado por no emitir el comprobante.

B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

6.4. Operatoria y control de las transacciones cursadas por medio de Internet (*e-banking*).

Dada la naturaleza de la exposición de Internet, éste es uno de los canales que representa mayor nivel de riesgo. Por ello, es relevante que las entidades financieras consideren políticas y prácticas adecuadas para la gestión del mismo.

En este apartado se detalla un conjunto de medidas mínimas de seguridad y control, adicionales a las ya especificadas en esta normativa, cuya aplicación permanente la entidad deberá evidenciar. Éstas son:

- § Se aplicarán mecanismos de seguridad para delimitar la red interna de la entidad y la red externa, y controlar la no existencia de intromisiones indeseadas a los sistemas internos de las entidades financieras, mediante la utilización de barreras (firewalls), sistemas de detección de intrusos, tanto a nivel de red, de servidores, como al procesador de datos central, y sistemas de detección de virus.
- Se valorizará que todo dispositivo de control de tráfico de red y de detección cuente con capacidad de registro de actividad. Dicho registro deberá evidenciar la realización de controles por los responsables designados para tal fin.
- § Toda tecnología utilizada a efectos de ofrecer servicios Web para los usuarios externos (clientes o potenciales), deberá evidenciar las mismas medidas de seguridad física y lógica expresadas en los apartados correspondientes de la presente normativa. Será valorado que las entidades financieras apliquen medidas de seguridad y control adicionales a las requeridas por esta normativa, acordes a los análisis de riesgos realizados para la actividad desarrollada por este canal.
 - § Deben contar con diagramas detallados de la infraestructura tecnológica utilizada para los servicios de e-Banking, donde quedará claramente evidenciada la utilización de prestadores de servicios relacionados a Internet.
 - § La página Web de las entidades financieras, con la que se brindan los servicios a los usuarios externos, deberá:
 - § informar claramente cual es la política de seguridad con que la entidad opera;
 - § enunciar claramente cual será la ventana de tiempo en la cual se puede operar con los servicios y productos bancarios;
 - § cuando se utilicen enlaces a otras páginas Web, informar al usuario que está abandonando la página Web de la entidad financiera y que no se tiene responsabilidad sobre la página Web en la cual se está por ingresar.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

- § Se valorizará la utilización de entidades certificadoras a efectos de que los usuarios externos puedan certificar la validez del sitio Web de la entidad financiera.
- § Todo acceso a funciones monetarias (sean éstas de consulta o transaccionales) en la banca por Internet, debe basarse en la utilización de una identificación de usuario y una clave de identificación personal distinta a la utilizada en otros canales de banca electrónica. Sus características deben ser, como mínimo, las enunciadas en el apartado de “Estándares de acceso, de identificación y autenticación, y reglas de seguridad”.
- § Se valorizará la utilización de mecanismos de autenticación de los usuarios y de no repudio de las transacciones, tales como: certificados digitales de usuarios, tarjetas inteligentes para el acceso, dispositivos biométricos, teclados virtuales, entre otros que determine la entidad.
- § Reafirmando la naturaleza de ser la banca por Internet un entorno sin papeles, las entidades deben poseer registros lógicos de toda la actividad realizada por los usuarios externos. Estos registros deberán estar disponibles por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dicho registro podrá ser inferior a 6 (seis) años.
- § Las entidades financieras deben contar con planes de continuidad de operaciones, como los requeridos en la presente normativa, que involucren las acciones de recuperación de los servicios ofrecidos a los usuarios externos por medio de Internet. Se valorizará, adicionalmente, la implementación de una infraestructura tecnológica con replicación de sus componentes, a efectos de ofrecer un servicio a los usuarios por Internet sin paradas (Non Stop Service).
- § En el caso de que las entidades financieras hayan decidido delegar en terceros actividades de hosting, housing, o incluso la actividad total de e-Banking, serán responsables directos por exigir a los terceros la existencia de planes de continuidad de procesamiento de datos y servicios por Internet. Además, deberán asegurarse de que dichos planes sean formal e integralmente probados, con los mismos requisitos que se expresan en la Sección 4.

6.5. Operatoria y control de las transacciones cursadas por medio de dispositivos móviles, que utilicen comunicaciones de telefonía celular o de redes inalámbricas de área amplia.

En adición a los requerimientos enunciados en el punto 6.4., las entidades financieras que ofrezcan servicios por medio del canal denominado como “Banca Móvil” (*m-Banking*), deben contemplar los siguientes aspectos:

- § Asegurar la confidencialidad de los datos que se comunican por medio de las redes de comunicación inalámbrica y redes de comunicación de telefonía celular, por medio de encriptación extremo a extremo.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 6. Banca electrónica por diversos medios.

- § Con el objeto de mantener la encriptación mencionada, deberán evidenciar la aplicación de controles permanentes a efectos de asegurar que no se empleen dispositivos de conversión (gateways) que apliquen desencriptación de datos y exposición de los mismos.

6.6. Operatoria y control de las transacciones cursadas por medio de atención telefónica (*Phone Banking*).

Las operatorias y transacciones que las entidades financieras ofrezcan por medio de atención telefónica, no podrán basarse en la comunicación oral de datos críticos de los usuarios, como las claves de seguridad relacionadas con cualquiera de los sistemas de identificación, o cualquier otro dato que requiera medidas de confidencialidad. En ningún caso, la clave de identificación personal -en su totalidad o partes que la compongan- podrá ser visualizada por el operador que atiende o monitorea la llamada.

Por cada transacción realizada a través de este canal, se deberá proveer al usuario el número de transacción registrado y, en caso de atención personalizada, la identificación del operador interviniente.

Para toda transacción de índole monetaria o vinculada con la gestión de claves de seguridad, se debe registrar en tiempo real toda la información cursada por este medio, para uso de los responsables del control y de la auditoría. Este registro debe reunir todas condiciones de seguridad e integridad en relación con la no alteración del estado registrado originalmente, con el fin de garantizar su confiabilidad. Además, se conservará por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dicho registro podrá ser inferior a 6 (seis) años y deberá estar disponible en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias lo requiera para su control.

Se valorizará como conveniente el uso de sistemas de grabación en el transcurso de la gestión telefónica.

6.7. Operatoria y control de las transacciones cursadas por medio de otros mecanismos no contemplados en la presente normativa.

De surgir otro canal -no contemplado en las presentes normas- por el cual la entidad financiera decidiera ofrecer sus productos y servicios, el mismo deberá ser considerado por el Directorio, o autoridad equivalente de la entidad financiera, con el fin de tomar conocimiento de los posibles riesgos e instrumentar la aplicación de todas las medidas de seguridad y control conducentes a minimizar su exposición.

Se deberá remitir a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, con no menos de 90 días de antelación a la implementación, la información relacionada al proyecto de desarrollo del nuevo canal.

Versión: 2a.	COMUNICACIÓN "B" 9042	Vigencia: 19/07/2007	Página 8
--------------	-----------------------	-------------------------	----------



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 8. Sistemas aplicativos de información.

Todos los sistemas aplicativos deben generar registros de auditoría que contengan mínimamente las actividades de los usuarios, las tareas realizadas, las funciones monetarias y no monetarias utilizadas, y quién ingresó y autorizó cada transacción, salvo que las mismas consistan en consultas o actividades, tareas o funciones similares que no generen transacciones o modificaciones en los datos o aplicativos. Estos registros deben ser revisados regularmente por los responsables del control. Se debe proteger la integridad de la información registrada en dichos reportes, la que debe ser resguardada adecuadamente y permanecer en condiciones de ser recuperada por un término no menor al plazo de prescripción para las acciones derivadas de cada tipo de operación. En ningún caso, la guarda de dichos registros podrá ser inferior a 6 (seis) años. La información podrá ser resguardada en soportes de almacenamiento no modificables o en soportes reutilizables, siempre que se proteja la integridad de la información con medidas de control que permitan evidenciar la no alteración posterior a su generación. Dichos registros deberán estar disponibles en caso de que la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias los requieran para su control.

8.3. Administración y registro de las operaciones.

Las entidades financieras deben registrar y procesar sus operaciones en los sistemas aplicativos de información correspondientes. No deberá gestionarse ninguna operación en forma manual, en hojas de cálculo, herramientas de escritorio u otro software utilitario.

8.4. Sistemas de información que generan el régimen informativo a remitir y/o a disposición del Banco Central de la República Argentina.

Las entidades financieras deben contar con sistemas aplicativos o procesos automatizados para la generación de los regímenes informativos requeridos por el Banco Central de la República Argentina. Se deberá evitar el reingreso o intercambio no automatizado de datos entre distintos sistemas, el ingreso de datos significativos en forma manual, y no se podrán efectuar ajustes a la información generada previamente en forma automática.

En los casos en que se deba ingresar información manual por no residir ésta en los archivos o bases de datos de la entidad, se debe realizar a través de programas específicos, en archivos independientes, con un adecuado esquema de seguridad, controles de integridad y validez, y sin la posibilidad de modificar la información generada en forma automatizada.

La información generada debe ser sometida a procesos de control, que analicen la consistencia e integridad de la información a remitir y/o mantener a disposición del Banco Central de la República Argentina, y que en ningún caso permitan su modificación fuera de los sistemas aplicativos que la originaron.



B.C.R.A.	REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS
	Sección 8. Sistemas aplicativos de información.

8.5. Documentación de los sistemas de información.

8.5.1. Estándares para el proceso de ingeniería del software.

De acuerdo con la estructura y complejidad de sus funciones informáticas, las entidades financieras deben contar con estándares de metodología para el proceso de ingeniería del software, que comprendan aspectos tales como: estudio de factibilidad, análisis y especificaciones, diseño, desarrollo, pruebas, migraciones de datos preexistentes, implementación y mantenimiento de los sistemas aplicativos de información.

Los mismos deben ser tenidos en consideración, tanto para desarrollos de sistemas propios de la entidad, como para aquellos que hayan sido tercerizados a través de la contratación de personal o proveedores externos.

Asimismo, deben contar con procedimientos que definan el circuito para el tratamiento de los requerimientos de usuarios y pautas para la evaluación, selección y adquisición de sistemas aplicativos.

8.5.2. Documentación técnica y manuales de usuarios.

Las entidades financieras deben contar con documentación funcional y técnica actualizada de sus sistemas aplicativos de información, en la cual se deben considerar aspectos tales como: objetivo, alcance, diagrama del sistema y de los programas componentes de los mismos, diseño de archivos y bases de datos, registro de modificaciones, lenguaje de programación utilizado, propiedad de los programas fuentes, descripción del "hardware" y "software", su interrelación con las redes de telecomunicaciones y descripción de las funciones que permitan la modificación directa de datos de producción (cambio de parámetros, fórmulas, tasas, datos y otros).

Además, deben poseer manuales de usuarios finales de cada sistema aplicativo de información que contengan, por ejemplo: objetivo, alcance, descripción de las funciones y menús, descripción de los listados operativos y de control, e instrucciones para el caso de cancelaciones, entre otros.



B.C.R.A.	ORIGEN DE LAS DISPOSICIONES INCLUIDAS EN EL TEXTO ORDENADO DE LAS NORMAS SOBRE “REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS”
----------	---

TEXTO ORDENADO			NORMA DE ORIGEN				
Sección	Punto	Párrafo	Com.	Anexo	Punto	Párrafo	Observaciones
1.		1° a 3°	“A” 4609	único	1.	1° a 3°	
		4°	“A” 3198		1.	1°	
	1.1.		“A” 4609	único	1.1.		
	1.2.		“A” 3198		1.2.		
	1.3.		“A” 3198		1.3.		
	1.4.		“A” 3198		1.4.		
	1.5.		“A” 4609	único	1.5.		
	1.6.		“A” 3198		1.6.		
	1.7.		“A” 3198		1.7.		
		12° y 13°	“A” 3198			9° y 10°	
2.	2.1.		“A” 3198		2.5.		Según Com. “A” 4609.
	2.2.		“A” 3198		3.1. a 3.3.		Según Com. “A” 4609.
	2.3.		“A” 4609	único	2.3.		
	2.4.		“A” 3198		2.1. y 2.5.		Según Com. “A” 4609.
	2.5.1.		“A” 3198		2.3.		Según Com. “A” 4609.
	2.5.2.		“A” 3198		2.4.		
	2.5.3.		“A” 3198		2.2.		Según Com. “A” 4609.
	2.5.4.		“A” 4609	único	2.5.4.		
	2.5.5.		“A” 4609	único	2.5.5.		
3.	3.1.		“A” 4609	único	3.1.		
	3.1.1.		“A” 3198		6.1.		Según Com. “A” 4609.
	3.1.2.		“A” 4609	único	3.1.2.		
	3.1.3.		“A” 4609	único	3.1.3.		
	3.1.4.		“A” 3198		6.3. a 6.5.		Según Com. “A” 4609 y “A” 4690, pto. 1.
	3.1.5.		“A” 4609	único	3.1.5.		
	3.2.		“A” 4609	único	3.2.		
	3.2.1.		“A” 4609	único	3.2.1.		
	3.2.2.		“A” 3198		7.3.		Según Com. “A” 4609.
	3.2.3.		“A” 3198		7.3.		Según Com. “A” 4609.
	3.2.4.		“A” 4609	único	3.2.4.		
4.	4.1.		“A” 4609	único	4.1.		
	4.2.		“A” 4609	único	4.2.		
	4.3.		“A” 3198		7.2.		Según Com. “A” 4609.
	4.4.		“A” 3198		7.2.		Según Com. “A” 4609.
	4.5.		“A” 3198		7.2.		Según Com. “A” 4609.
	4.6.		“A” 3198		7.2.		Según Com. “A” 4609.
5.	5.1.		“A” 3198		4.2.3.		Según Com. “A” 4609.
	5.2.		“A” 4609	único	5.2.		
	5.3.		“A” 3198		4.1.		Según Com. “A” 4609.



REQUISITOS MÍNIMOS DE GESTIÓN, IMPLEMENTACIÓN, Y CONTROL DE LOS RIESGOS RELACIONADOS CON TECNOLOGÍA INFORMÁTICA, SISTEMAS DE INFORMACIÓN Y RECURSOS ASOCIADOS PARA LAS ENTIDADES FINANCIERAS							
TEXTO ORDENADO			NORMA DE ORIGEN				
Sección	Punto	Párrafo	Com.	Anexo	Punto	Párrafo	Observaciones
5.	5.4.		"A" 3198		7.1.		Según Com. "A" 4609.
	5.5.		"A" 4609	único	5.5.		
	5.6.		"A" 4609	único	5.6.		
	5.7.		"A" 4609	único	5.7.		
	5.8.		"A" 3198		4.2.1., 6.6. y 6.7.		Según Com. 4609.
	5.9.		"A" 4609	único	5.9.		
	5.10.		"A" 4609	único	5.10.		
	5.11.		"A" 4609	único	5.11.		
	5.12.		"A" 4609	único	5.12.		
6.		1° y 2°	"A" 4609	único	6.	1° y 2°	
	6.1.		"A" 4609	único	6.1.		
	6.2.		"A" 3198		11.1. a 11.6.		Según Com. "A" 4609 y "A" 4690, pto. 2.
	6.3.		"A" 4609	único	6.3.		Según Com. "A" 4690, pto. 3.
	6.4.		"A" 4609	único	6.4.		Según Com. "A" 4690, pto. 4.
	6.5.		"A" 4609	único	6.5.		
	6.6.		"A" 3198		11.7.		Según Com. "A" 4609 y "A" 4690, pto. 5.
	6.7.		"A" 4609	único	6.7.		
7.	7.1.		"A" 4609	único	7.1.		
	7.2.		"A" 4609	único	7.2.		
	7.3.		"A" 3198		5.1.		Según Com. "A" 4609.
	7.4.		"A" 3198		5.2. a 5.4.		Según Com. "A" 4609.
	7.5.		"A" 3198		5.5.		Según Com. "A" 4609.
	7.6.		"A" 3198		5.4.		Según Com. "A" 4609.
	7.7.		"A" 3198		5.6.		Según Com. "A" 4609.
8.	8.1.		"A" 3198		9.2.		Según Com. "A" 4609.
	8.2.		"A" 3198		4.2.2.		Según Com. "A" 4609 y "A" 4690, pto. 6.
	8.3.		"A" 4609	único	8.3.		
	8.4.		"A" 3198		9.4.		Según Com. "A" 4609.
	8.5.1.		"A" 4609	único	9.1.		
	8.5.2.		"A" 3198		9.1.		Según Com. "A" 4609.