BANCO CENTRAL DE LA REPÚBLICA ARGENTINA

COMUNICACIÓN "A" **4609**	**27/12/2006**

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

Ref.: Circular
RUNOR 1 – 805

Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información

Nos dirigimos a Uds. para comunicarles que esta Institución adoptó la siguiente resolución:

" 1. Aprobar 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" a que se refiere el Anexo a la presente Comunicación.

2. Dejar sin efecto (a partir de la entrada en vigencia de la presente comunicación) las disposiciones dadas a conocer mediante la Comunicación "A" 3198 para el caso de Entidades Financieras solamente, manteniendo su aplicación para las Cámaras Electrónicas de Compensación.

3. Establecer la vigencia de la nueva norma de la siguiente forma:

   a. A partir de la fecha de su emisión para las nuevas entidades que se autoricen.

   b. A partir de los 180 días corridos desde su emisión, para las Entidades Financieras que estén autorizadas a la fecha".

Saludamos a Uds. muy atentamente.

BANCO CENTRAL DE LA REPUBLICA ARGENTINA

Marcelo D. Fernández
Gerente de Auditoria Externa
de Sistemas

Pablo L. Carbajo
Subgerente General de Análisis
y Auditoria

ANEXO

Índice

Sección 1. Aspectos generales.

1.1. Eficacia.
1.2. Eficiencia.
1.3. Confidencialidad.
1.4. Integridad.
1.5. Disponibilidad.
1.6. Cumplimiento.
1.7. Confiabilidad.

Sección 2. Organización funcional y gestión de tecnología informática y sistemas.

2.1. Comité de Tecnología Informática. Integración y funciones.
2.2. Políticas y procedimientos.
2.3. Análisis de Riesgos.
2.4. Dependencia del área de Tecnología Informática y Sistemas.
2.5. Gestión de Tecnología Informática y Sistemas.

Sección 3. Protección de activos de información.

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

Sección 4. Continuidad del procesamiento electrónico de datos.

4.1. Responsabilidades sobre la planificación de la continuidad del procesamiento de datos.
4.2. Análisis de impacto.
4.3. Instalaciones alternativas de procesamiento de datos.
4.4. Plan de continuidad del procesamiento de datos.
4.5. Mantenimiento y actualización del plan de continuidad de procesamiento de datos.
4.6. Pruebas de continuidad del procesamiento de datos.

Sección 5. Operaciones y procesamiento de datos.

5.1. Responsabilidad del área.
5.2. Inventario tecnológico.
5.3. Políticas y procedimientos para la operación de los sistemas informáticos y manejadores de datos.
5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.
5.5. Mantenimiento preventivo de los recursos tecnológicos.

Índice

5.6. Administración de las bases de datos.
5.7. Gestión de cambios al software de base.
5.8. Control de cambios a los sistemas productivos.
5.9. Mecanismos de distribución de información.
5.10. Manejo de incidentes.
5.11. Medición y planeamiento de la capacidad.
5.12. Soporte a usuarios.

Sección 6. Banca electrónica por diversos medios.

6.1. Controles generales.
6.2. Operatoria y control de las transacciones cursadas por cajeros automáticos (ATM's).
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.
6.4. Operatoria y control de las transacciones cursadas por medio de Internet (e-banking).
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.
6.6. Operatoria y control de las transacciones cursadas por medio de atención telefónica (Phone Banking).
6.7. Operatoria y control de las transacciones cursadas por medio de otros mecanismos no contemplados en la presente normativa.

Sección 7. Delegación de actividades propias de la entidad en terceros.

7.1. Actividades Factibles de Delegación.
7.2. Responsabilidades propias de la entidad.
7.3. Formalización de la delegación.
7.4. Responsabilidades del tercero.
7.5. Implementación del procesamiento de datos en un tercero.
7.6. Control de las actividades delegadas.
7.7. Planificación de continuidad de la operatoria delegada.

Sección 8. Sistemas aplicativos de información.

8.1. Cumplimiento de requisitos normativos.
8.2. Integridad y validez de la información.
8.3. Administración y registro de las operaciones.
8.4. Sistemas de información que generan el régimen informativo a remitir y/o a disposición del Banco Central de la República Argentina.
8.5. Documentación de los sistemas de información.

El Directorio o autoridad equivalente de la entidad (Consejo de Administración, en el caso de entidades financieras cooperativas, o Funcionario de primer nivel jerárquico, en el caso de sucursales de entidades financieras extranjeras) es el responsable primario del establecimiento y la existencia de un área que gestione la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas para todos los canales electrónicos por los que las entidades financieras realizan el ofrecimiento de sus productos y servicios. Dicha área evidenciará una clara separación organizacional con relación a los sectores usuarios de la misma.

Del mismo modo, será responsable de que existan políticas generales y planes estratégicos de corto y mediano plazo, y de la asignación de los recursos necesarios para la mencionada área.

Debe estar involucrado con los aspectos generales que gobiernen la tecnología de la información y sus actividades relacionadas, los riesgos que conllevan, y evidenciar mediante documentación formal la toma de decisiones, el seguimiento y el control de lo establecido.

Los procedimientos que deben llevarse a cabo para el desarrollo de la tarea y control de las áreas de sistemas de información, los cuales involucran al Directorio, Consejo de Administración o autoridad equivalente, Gerencia General, Gerencia de Sistemas de Información (SI) y personal de la entidad, deben estar diseñados para proveer un grado razonable de seguridad en relación con el logro de los objetivos y los recursos aplicados en los siguientes aspectos:

1.1. Eficacia.

La información y sus procesos relacionados, debe ser relevante y pertinente para el desarrollo de la actividad. Debe presentarse en forma correcta, coherente, completa y que pueda ser utilizada en forma oportuna.

1.2. Eficiencia.

El proceso de la información debe realizarse mediante una óptima utilización de los recursos.

1.3. Confidencialidad.

La información crítica o sensible debe ser protegida a fin de evitar su uso no autorizado.

1.4. Integridad.

Se refiere a la exactitud que la información debe tener, así como su validez acorde con las pautas fijadas por la entidad y regulaciones externas.

1.5. Disponibilidad.

Los recursos y la información, ante su requerimiento, deben estar disponibles en tiempo y forma.

1.6. Cumplimiento.

Se refiere al cumplimiento de las normas internas y de todas las leyes y reglamentaciones a las que están sujetas las entidades financieras.

1.7. Confiabilidad.

Los sistemas deben brindar información correcta para ser utilizada en la operatoria de la entidad, en la presentación de informes financieros a los usuarios internos y en su entrega al Banco Central de la Republica Argentina y demás organismos reguladores.

Todos estos aspectos deben ser aplicados a cada uno de los recursos intervinientes en los procesos de tecnología informática, tales como: datos, sistemas de aplicación, tecnología, instalaciones y personas.

Las secciones siguientes de la presente norma enumeran una serie de requisitos mínimos que las entidades financieras deberán cumplir, los que serán sometidos a supervisión por parte de la Superintendencia de Entidades Financieras y Cambiarias.

2.1. Comité de Tecnología Informática. Integración y funciones.

Las entidades financieras deberán constituir un "Comité de Tecnología Informática" integrado, al menos, por un miembro del Directorio o autoridad equivalente, y el responsable máximo del área de Tecnología Informática y Sistemas.

Los directores, consejeros, y funcionarios definidos en el párrafo precedente, que integren el Comité de Tecnología Informática, asumen, respecto de sus demás pares del órgano directivo o, si correspondiera, de la autoridad máxima en el país, una responsabilidad primaria frente a eventuales incumplimientos a estas normas.

El Comité de Tecnología Informática deberá, entre otras gestiones:

- vigilar el adecuado funcionamiento del entorno de Tecnología Informática;
- contribuir a la mejora de la efectividad del mismo;
- tomar conocimiento del Plan de Tecnología Informática y Sistemas, y en caso de existir comentarios en relación con la naturaleza, alcance y oportunidad del mismo, el Comité deberá manifestarlos en reunión;
- evaluar en forma periódica el plan mencionado precedentemente y revisar su grado de cumplimiento;
- revisar los informes emitidos por las auditorías relacionados con el ambiente de Tecnología Informática y Sistemas, y velar por la ejecución, por parte de la Gerencia General, de acciones correctivas tendientes a regularizar o minimizar las debilidades observadas; y
- mantener una comunicación oportuna con los funcionarios de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, en relación con los problemas detectados en las inspecciones actuantes en la entidad y con el monitoreo de las acciones llevadas a cabo para su solución.

El Comité de Tecnología Informática deberá reunirse periódicamente a fin de llevar a cabo las tareas asignadas. La periodicidad mínima de dichas reuniones será trimestral, y en las mismas participarán, además de sus integrantes, los funcionarios que se consideren necesarios a fin de tratar un tema en particular.

A su vez, el mencionado Comité elaborará un acta en la cual se detallarán los temas tratados en cada reunión, así como los puntos que requerirán su seguimiento posterior. Dicha acta será transcripta en un libro especial habilitado a tal efecto y se enviará al Directorio, o autoridad equivalente, para su toma de conocimiento en la primera reunión posterior de dicho órgano.

2.2. Políticas y procedimientos.

El Directorio, o autoridad equivalente, debe procurar y observar la existencia de políticas y procedimientos para administrar el riesgo relacionado a los sistemas de información y la tecnología informática.

Las políticas son documentos de alto nivel, que representan la filosofía de la entidad y el pensamiento estratégico en la dirección de la misma. Para ser efectivas deben ser claramente escritas y concisas.

Los procedimientos son documentos escritos que describen de manera secuencial la forma de ejecutar una actividad para lograr un objetivo determinado, dentro de un alcance establecido. En dichos documentos se enuncian procesos operativos, se definen responsabilidades, se establecen los documentos (planillas, informes, registros) a emitir y controlar, y se detallan los controles necesarios, definiendo dónde y cuándo éstos deben realizarse.

Tanto las políticas como los procedimientos deben estar claramente escritos, formalmente comunicados, mantenerse actualizados, establecer la asignación de responsabilidades, y ser la base de la coordinación y realización de las tareas, como así también el instrumento que permita el entrenamiento sobre las actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas de la entidad.

2.3. Análisis de Riesgos.

El Directorio, o autoridad equivalente, será responsable de la existencia de mecanismos de control del grado de exposición a potenciales riesgos inherentes a los sistemas de información, de la tecnología informática y sus recursos asociados. Serán a la vez los responsables primarios de observar su continua ejecución.

Se deberá evidenciar la existencia de análisis de riesgos formalmente realizados y documentados sobre los sistemas de información, la tecnología informática y sus recursos asociados. Los mismos permanecerán disponibles para su revisión por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

Los resultados de los análisis mencionados y sus actualizaciones periódicas deben ser formalmente reportados al Directorio, o autoridad equivalente, que será el responsable primario de gestionar que las debilidades que expongan a la entidad a niveles de riesgo alto o inaceptable sean corregidas a niveles aceptables.

2.4. Dependencia del área de Tecnología Informática y Sistemas.

El área de Tecnología Informática y Sistemas -o la denominación que la entidad haya determinado usar para la función de la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas- dependerá a nivel organizacional, dentro de la estructura de la entidad financiera, de un lugar tal que no genere dependencia funcional de áreas usuarias de su gestión.

La entidad debe notificar formalmente la designación del responsable de área a la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias, cada vez que ocurra un cambio en la gestión.

2.5. Gestión de Tecnología Informática y Sistemas.

2.5.1. Planificación.

El Comité de Tecnología Informática y Sistemas, tendrá a su cargo asegurar que los sistemas de información y tecnologías relacionadas concuerden con las necesidades de negocio de la entidad financiera y se alineen con los planes estratégicos de la misma.

Se deberá evidenciar la existencia de un plan de tecnología y sistemas, formalizado y aprobado por el Directorio, o autoridad equivalente de la entidad, que soporte los objetivos estratégicos de la misma, contenga un cronograma de proyectos y permita demostrar el grado de avance de los mismos, la asignación de prioridades, los recursos y los sectores involucrados.

2.5.2. Control de gestión.

Se evidenciará la existencia de reportes formales, que sean el resultado del control ejercido por los sectores que dependen del área Tecnología Informática y Sistemas. Dichos reportes servirán como base para informar a instancias superiores, y deberán mantenerse, por lo menos durante 2 (dos) años, para su control por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

2.5.3. Segregación de funciones.

El área de Tecnología Informática y Sistemas deberá presentar una clara delimitación de tareas entre los sectores que estén bajo su dependencia.

El cuadro del punto 2.5.4. muestra, como referencia, las incompatibilidades existentes entre las funciones de un sector específico, con respecto a las actividades desempeñadas por otras áreas o sectores.

En el cuadro, donde se indica la intersección de dos funciones mediante la sigla “NO”, la entidad deberá tomar medidas en la segregación de tareas, a efectos de evitar su concentración.

Cuando en el cuadro se indica la intersección de dos funciones mediante la sigla “X”, esto implica que preferentemente estas tareas no deberían recaer en un mismo sector, y en el caso de que las mismas estuviesen concentradas, deberán evidenciarse claras medidas de control compensatorio.

En aquellos casos excepcionales, en que por razones de imposibilidad de estructura no pueda segregarse alguna de las funciones antes mencionadas, deberá evidenciarse la existencia formal y documentada de controles por oposición de intereses realizados por sectores independientes. Los mismos deben mantenerse por un plazo no inferior a 2 (dos) años, para su posterior revisión por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

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	SI	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	SI	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			

2.5.5. Glosario de funciones descriptas 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, y por naturaleza es el dueño de los datos.

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.

3.1. Gestión de la seguridad.

3.1.1. Dependencia del área responsable.

Las entidades financieras deben considerar en su estructura organizacional un área para la protección de los activos de información, con el fin de establecer los mecanismos para la administración y el control de la seguridad sobre el acceso lógico y físico a sus distintos ambientes tecnológicos y recursos de información: equipamiento principal, plataforma de sucursales, equipos departamentales, subsistemas o módulos administradores de seguridad de los sistemas de aplicación, sistemas de transferencias electrónicas de fondos, bases de datos, canales de servicios electrónicos, banca por Internet y otros.

El responsable de la protección de activos de información gestionará la implementación y el mantenimiento de la política de seguridad para los mismos, establecida por el Directorio, o autoridad equivalente de la entidad.

La ubicación jerárquica del área deberá garantizar, en forma directa, su independencia funcional y operativa de las áreas de tecnología y sistemas de información, del resto de las áreas usuarias y de la función de auditoría.

Deben definirse, documentarse y asignarse adecuados roles para los recursos humanos que la integran, considerando: misiones y funciones, responsabilidades, habilidades necesarias para cubrir el puesto y otros aspectos que las entidades financieras crean relevantes. Los recursos humanos que desempeñen la función deben contar con adecuados niveles de entrenamiento en la implementación de controles y el mantenimiento de políticas y sanas prácticas de seguridad.

3.1.2. Estrategia de seguridad de acceso a los activos de información.

De acuerdo con sus operaciones, procesos y estructura, las entidades financieras deben definir una estrategia de protección de activos de información, que les permita optimizar la efectividad en la administración y el control de sus activos de información.

Dicha estrategia debe considerar las amenazas y las vulnerabilidades asociadas a cada entorno tecnológico, su impacto en el negocio, los requerimientos y los estándares vigentes. Para ello deben asignar claramente roles y responsabilidades en materia de seguridad, comprometiendo a los máximos niveles directivos y gerenciales.

La estrategia de seguridad deberá contemplar el establecimiento de mecanismos de control para la detección, registro, análisis, comunicación, corrección, clasificación y cuantificación de los incidentes y de las debilidades en los accesos no autorizados a la información administrada en los sistemas de información.

Se valorará que la mencionada estrategia abarque, además de los recursos informáticos propios de la entidad, a sus grupos de influencia: sistema financiero, clientes de todo tipo, proveedores de recursos y sistemas de información, operadores de telecomunicaciones, requerimientos de los organismos de regulación y control, y otros entes externos vinculados directa o indirectamente.

3.1.3. Planeamiento de los recursos.

En los ciclos de gestión de las funciones informáticas, se deben considerar el planeamiento, la implementación y el mejoramiento continuo de los procesos de administración y control de seguridad sobre la protección de activos de información.

De acuerdo con los riesgos identificados en las metas y planes estratégicos, se deben elaborar planes operativos que contemplen los factores críticos para un efectivo control de las aplicaciones junto con las actividades del negocio que respaldan. Dichos planes operativos tendrán en cuenta las tareas a realizar con su correspondiente asignación de tiempos y recursos, las prioridades y la precedencia de cada una de ellas.

En los nuevos proyectos informáticos se deben contemplar los requerimientos de seguridad desde sus etapas iniciales, con el objetivo de asegurar el diseño y la implementación de apropiados controles y registros de seguridad, como así la correcta selección de tecnología que haga a la solución integral de la misma

3.1.4. Política de protección.

De acuerdo con su estrategia de seguridad, las entidades financieras deben desarrollar una política de protección de los activos de información. Ésta debe evidenciar claramente que es un instrumento que se utiliza para proporcionar dirección y apoyo gerencial con el objeto de brindar protección de los activos de información. Además, identificará los recursos críticos a proteger y los riesgos internos y externos de accesos no autorizados sobre los mismos.

El Directorio, o autoridad equivalente, deberá establecer una dirección política clara, y demostrar apoyo y compromiso con respecto a la protección de los activos de información, mediante la formulación, aprobación formal y difusión de la misma a través de toda la entidad.

Deberá ser implementada y comunicada a todo el personal y servir como base para el desarrollo de las normas, los manuales, los estándares, los procedimientos y las prácticas que gobiernen los aspectos de seguridad de los sistemas de información, los datos y la tecnología informática asociada.

La mencionada documentación deberá contemplar, como mínimo:

- objetivo, alcance, principios y requisitos de seguridad de acceso lógico;
- acuerdos, términos y condiciones de confidencialidad de los datos;
- procedimientos para la implementación de nuevos recursos y servicios de información;
- estándares para la clasificación de los activos de información (recursos tecnológicos, datos y ambientes físicos);
- procedimientos para el acceso y la autenticación de los usuarios;
- procedimientos para la generación y distribución de usuarios y claves de identificación personal (contraseñas, PIN, *tokens*, otros similares) para el ingreso a los sistemas;

- sanas prácticas de seguridad para la utilización y selección de claves de identificación personal;
- procedimientos para la comunicación de incidentes y debilidades relacionados con accesos no autorizados, pérdidas o daños a la información;
- mecanismos para la asignación y la utilización de los usuarios especiales y de contingencia;
- estándares para el empleo de aquellos utilitarios que permitan el alta, la baja o la modificación de datos operativos, por fuera de los sistemas aplicativos que los originan;
- procedimientos de control de cambios y puesta en producción de programas;
- procedimientos para el registro y comunicación de incidentes en materia de seguridad;
- prácticas de seguridad para la utilización del correo electrónico y navegación por Internet;
- procedimientos para la prevención, detección y eliminación de software malicioso,
- procedimiento a seguir para la detección de intrusos en las redes y plataformas informáticas, así como las acciones que deben implementarse luego de su detección;
- pautas mínimas de seguridad a contemplar en la adquisición de nuevos recursos tecnológicos, sistemas aplicativos y software de base, y
- toda aquella documentación que se considere relevante de acuerdo con las características propias de administración y control informático.

La política de seguridad y los documentos que la complementan deben someterse periódicamente a procesos de revisión y actualización, de acuerdo con la evaluación de riesgos y la complejidad de la entidad financiera, asegurando la correcta implementación de mejores prácticas de seguridad informática en los circuitos operativos y ambientes computadorizados de información. Asimismo, la mencionada documentación se deberá reconsiderar ante la implementación de nuevos programas y sistemas, cambios en las operaciones, actualizaciones tecnológicas y nuevas relaciones con terceros.

3.1.4.1. Clasificación de los activos de información - Niveles de acceso a los datos.

Las entidades financieras deben clasificar sus activos de información de acuerdo con su criticidad y sensibilidad, estableciendo adecuados derechos de acceso a los datos administrados en sus sistemas de información.

Esta clasificación deberá ser documentada, formalizada y comunicada a todas las áreas de la entidad, principalmente a los propietarios de los datos. La misma puede ser parte integrante de la política de protección de los activos de información, o formar un documento aparte.

Los niveles de acceso deben diseñarse considerando los criterios de la clasificación, junto con una adecuada separación de tareas, determinando qué clases de usuarios o grupos poseen derechos de acceso -y con qué privilegio- sobre los datos, sistemas, funciones y servicios informáticos.

La asignación de derechos de acceso debe otorgarse a través de un proceso de autorización formal del propietario de los datos, verificando periódicamente los niveles y privilegios otorgados a los usuarios.

3.1.4.2. Estándares de acceso, de identificación y autenticación, y reglas de seguridad.

Se deben implementar métodos de identificación y autenticación para controlar el acceso lógico a los sistemas y servicios informáticos, los que dependerán de la criticidad y el valor de los datos a proteger, debiéndose considerar:

- la modificación de las contraseñas maestras y de cuentas especiales "por defecto" de los sistemas operativos, de los subsistemas administradores de seguridad, de las bases de datos y de las herramientas para la administración y el control;
- el cambio obligatorio de las contraseñas de acceso en el primer inicio de sesión;
- 8 (ocho) caracteres de longitud para las claves provistas a todo sistema informático de la entidad;
- el control de la composición de las contraseñas (por ejemplo: caracteres alfabéticos, numéricos, especiales, mayúsculas y minúsculas);
- el registro histórico de las últimas 12 (doce) contraseñas utilizadas, evitando ser reutilizadas;
- el intervalo de caducidad automática de las mismas a los 30 (treinta) días;
- el bloqueo permanente de la cuenta del usuario ante 3 (tres) intentos de acceso fallidos;
- la desconexión automática de la sesión de usuario en la aplicación y en la red por tiempo de inactividad a los 15 (quince) minutos;
- la eliminación de las cuentas de usuario inactivas por un período mayor a 90 (noventa) días;
- la no utilización de denominaciones de usuario genérico para perfiles asignados a personas físicas;
- técnicas de encriptación, con algoritmos de robustez reconocida internacionalmente, para el archivo de las contraseñas;
- asignación de contraseñas para todas las cuentas;
- restricción de accesos concurrentes;
- la identificación única (ID) de usuarios;
- definición de opciones y menús para acceder a las funciones de los sistemas de información;
- la dinámica en la actualización de los derechos de acceso, revocando los usuarios que se desvincularan de la entidad y modificando los perfiles de aquellos que cambiaron de función;
- la permanente actualización de los sistemas operativos y herramientas con respecto a nuevas vulnerabilidades, y "*patches*".

Asimismo, se consideran sanas prácticas de seguridad:

- el mantenimiento de la información codificada por mecanismos de encriptación en los sistemas de bases de datos;
- la utilización de adecuadas herramientas para la administración y el control de la seguridad de acceso;
- la permanente actualización de las versiones de los sistemas operativos;

- la deshabilitación de los accesos remotos a los recursos de información;
- la utilización de restricciones en los días y horarios de conexión;
- la verificación de la identidad del usuario ante solicitudes de reactivación de cuentas;
- el uso de estándares nemotécnicos para los perfiles de acceso de usuarios, grupos y recursos de sistemas;
- el empleo de mecanismos de autenticación biométrica;
- la utilización de smart-cards como dispositivos de identificación de accesos;
- la utilización de "single sign-on", y
- la permanente incorporación de prácticas y estándares reconocidos de seguridad.

3.1.4.3. Programas de utilidad con capacidades de manejo de datos - Usuarios privilegiados y de contingencia.

Deben implementarse adecuadas restricciones para el empleo de los programas que permitan el alta, la baja o la modificación de datos operativos por fuera de los sistemas aplicativos, en las distintas plataformas.

Asimismo, deben desarrollarse mecanismos formales para la asignación y la utilización de usuarios especiales con capacidades de administración, que puedan ser usados en caso de emergencia o interrupción de las actividades. Los usuarios definidos con estas características deben contar con adecuadas medidas de resguardo y acceso restringido. Su utilización será registrada y se realizarán controles posteriores sobre los reportes de eventos, analizando la concordancia entre las tareas realizadas y el motivo por el cual se los solicitó.

3.1.4.4. Registros de seguridad y pistas de auditoría.

Con el objeto de reducir a un nivel aceptable los riesgos internos y externos de accesos no autorizados, pérdidas y daños a la información, se deben implementar adecuadamente:

- registros operativos de las actividades de los usuarios, las tareas realizadas y las funciones utilizadas;

- reportes de seguridad que registren la asignación de claves y derechos de accesos, empleo de programas de utilidad que permitan el manejo de datos por fuera de las aplicaciones, actividades de los usuarios privilegiados, usuarios de emergencia y con accesos especiales, intentos fallidos de acceso y bloqueos de cuentas de usuario, y

- reportes de auditoría que registren las excepciones y actividades críticas de las distintas plataformas.

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 a 10 (diez) años. Para ello, se utilizarán soportes de almacenamiento no reutilizables. 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.

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.

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,
- 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.

4.1. Responsabilidades sobre la planificación de la continuidad del procesamiento de datos.

El Directorio, o autoridad equivalente de la entidad financiera, es el responsable primario por la identificación, la valorización, la gestión y el control de los riesgos. Debe asegurar la existencia y la provisión de los recursos necesarios para la creación, mantenimiento y prueba de un plan de recuperación del procesamiento electrónico de datos. El mismo deberá ser operable y funcional, acorde a los requerimientos de negocio de la entidad financiera y de los organismos de control.

Deberá designarse formalmente un área o sector, que será responsable de la creación, mantenimiento y prueba satisfactoria del plan de recuperación del procesamiento electrónico de datos.

La continuidad es considerada como un proceso que se inicia con la recuperación durante la contingencia, y concluye con la vuelta a la normalidad una vez controladas las causas que generaron dicha contingencia.

4.2. Análisis de impacto.

La continuidad del procesamiento electrónico de datos, que en definitiva posibilita la continuidad de los negocios, deberá evidenciar que se han identificado los eventos que puedan ocasionar interrupciones en sus procesos críticos.

Es responsabilidad del Directorio, o autoridad equivalente, observar que se haya llevado a cabo una evaluación de riesgos para determinar el impacto de distintos eventos, tanto en términos de magnitud de daño como del período de recuperación y la vuelta a la normalidad.

Estas dos actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. La evaluación considerará todos los procesos de negocio y no se limitará sólo a las instalaciones de procesamiento de la información, sino también a todos los recursos relacionados.

Los resultados de la evaluación deben ser el soporte para la selección de mecanismos alternativos de recuperación y adopción de medidas preventivas para la confección del plan de recuperación y vuelta a la normalidad del procesamiento de datos.

Dichos resultados serán formalmente aprobados y tomados en conocimiento por el Directorio, o autoridad equivalente de la entidad financiera, y deben estar disponibles en forma permanente para ser auditados por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

4.3. Instalaciones alternativas de procesamiento de datos.

Las instalaciones alternativas de procesamiento de datos deben atender los requisitos mínimos establecidos por estas normas, pudiendo ser propias o de terceros.

El equipamiento de las instalaciones de procesamiento alternativo debe contemplar la capacidad de administración y gestión de todos los procesos de negocios clasificados como críticos para asegurar la actividad de la entidad financiera.

En el caso en que la entidad financiera cuente con sucursales, la instalación alternativa debe prever la existencia de equipamiento destinado a las telecomunicaciones para acceder al servicio mínimo de las mismas.

En caso de un siniestro o suceso contingente que torne inoperantes las instalaciones principales, la localización de las instalaciones alternativas deberá ser tal que no sean alcanzadas por el mismo evento. Además, deberán tornarse totalmente operacionales en condiciones idénticas, en una ventana de tiempo tal que no afecte la atención de los clientes, ni deje a la entidad fuera del proceso de compensación.

La selección de la localización antes mencionada deberá estar soportada por la evidencia documental de la existencia de un análisis de riesgo de eventos simultáneos, que estarán fehacientemente expresados en el mismo.

4.4. Plan de continuidad del procesamiento de datos.

Se debe evidenciar la existencia de un procedimiento escrito, aprobado formalmente, para atender a la continuidad del procesamiento de datos y actividades vinculadas, en el caso que se presenten contingencias o emergencias.

El documento deberá basarse en el mismo análisis de riesgo efectuado para determinar la localización de las instalaciones alternativas de procesamiento de datos, enunciando todos los posibles escenarios que harían que el plan entrara en funcionamiento.

El mismo deberá, como mínimo, contener lo siguiente:

- Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente. Estos deben incluir disposiciones con respecto a la gestión de vínculos eficaces a establecer con las autoridades públicas pertinentes, por ej.: entes reguladores, policía, bomberos y otras autoridades.

- Los nombres, direcciones, números de teléfono y "localizadores" actuales del personal clave.

- Las aplicaciones criticas y su prioridad con respecto a los tiempos de recuperación y regreso a la operación normal.

- El detalle de los proveedores de servicios involucrados en las acciones de contingencia / emergencia.

- La información logística de la localización de recursos claves, incluyendo: ubicación de las instalaciones alternativas, de los resguardos de datos, de los sistemas operativos, de las aplicaciones, los archivos de datos, los manuales de operación y documentación de programas / sistemas / usuarios.

- Los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales a las ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos.
- La inclusión de los planes de reconstrucción para la recuperación en la ubicación original de todos los sistemas y recursos.
- Todo otro recurso definido como soporte de los procesos de negocio a recuperar.

4.5. Mantenimiento y actualización del plan de continuidad de procesamiento de datos.

El plan de continuidad del procesamiento electrónico de datos debe mantenerse por medio de revisiones y actualizaciones periódicas para garantizar su eficacia permanente. Se debe evidenciar que existen procedimientos escritos a fin de asegurar que todo cambio en los procesos de negocio y en su tecnología relacionada se reflejen en las actualizaciones sobre el plan de continuidad.

Debe existir un responsable formalmente identificado para el mantenimiento y adecuación del plan de continuidad, al cual deberá asignarse la responsabilidad de las revisiones periódicas, la identificación de cambios y su actualización. Este proceso formal de control de cambios debe garantizar que se distribuya el plan actualizado a todos los responsables involucrados en el mismo.

4.6. Pruebas de continuidad del procesamiento de datos.

El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben permitir asegurar la operatoria integral de todos los sistemas automatizados críticos –de acuerdo con los análisis de riesgo previos-, a efectos de verificar que el plan está actualizado y es eficaz. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente del plan mencionado.

Deberá evidenciarse la existencia de un cronograma formal de pruebas que indicará cómo debe probarse cada elemento del plan, y la fecha en la cual cada una de las pruebas deberá ser efectuada.

En las pruebas deben participar las áreas usuarias de los procesos de negocio, quienes deben verificar los resultados de las mismas. Se deberá documentar formalmente su satisfacción con el resultado de la prueba como medio para asegurar la continuidad de los procesos de negocio en caso de que ocurra una contingencia. La auditoría interna de la entidad también deberá conformar la satisfacción por el resultado de las mismas a tal efecto.

El informe realizado por las áreas usuarias y de auditoría interna deberá ser tomado en conocimiento por el Directorio, o autoridad equivalente de la entidad, y mantenido en archivo para su control posterior por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.1. Responsabilidad del área.

El área de operaciones deberá evidenciar la existencia de un responsable único para la gestión, el control y el reporte de los centros productivos de procesamiento de datos, sean estos centralizados o distribuidos. La gestión operativa deberá asegurar el normal funcionamiento de la infraestructura de sistemas de información y la tecnología relacionada.

5.2. Inventario tecnológico.

Las entidades financieras deben contar con la capacidad de identificar sus activos informáticos y de información, las características, la localización y la criticidad e importancia de los mismos.

Sobre la base de esta información, las entidades financieras podrán asignar niveles de protección proporcionales a la importancia de los activos, realizar una continua categorización de los mismos, mantenerlos actualizados y efectuar el mantenimiento preventivo de sus recursos físicos.

Por ello, las entidades financieras deben elaborar y mantener un inventario de los activos asociados a cada sistema de información. Se debe identificar claramente cada activo, estableciendo su propietario y su clasificación en cuanto a seguridad.

El inventario, como mínimo, debe contener los siguientes elementos:

- recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia;
- activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems, otros), equipos de comunicaciones (routers, firewalls, switches, encriptadores, otros), medios magnéticos (cintas, discos, resguardos varios), otros equipos técnicos;
- servicios descentralizados en terceros: servicios informáticos y de comunicaciones, fabricas de software, otros.

5.3. Políticas y procedimientos para la operación de los sistemas informáticos y manejadores de datos.

Debe existir una adecuada planificación, y documentación escrita y actualizada, de las actividades que se desarrollan normalmente en el centro de procesamiento de información, que deberán incluir -como mínimo- el detalle de los procesos a realizar, los controles que se efectúan, los mecanismos para el registro de los eventos y problemas, los procedimientos sobre cancelaciones y reproceso en cada una de las actividades, las relaciones con otras áreas y los mecanismos de distribución de la información.

Deben establecerse procedimientos de control para garantizar la efectiva y correcta realización de cambios cuando corresponda, por ejemplo: modificaciones de programas en bibliotecas de producción o archivos, definiciones de diccionarios de datos, órdenes de corrida de programas, etc.

5.4. Procedimientos de resguardos de información, sistemas productivos y sistemas de base.

EL Directorio, o autoridad equivalente, es el responsable primario de la existencia de soluciones para el almacenamiento y resguardo de datos, programas y todo otro componente de información relevante para las funciones de negocio, para las acciones de recuperación del procesamiento de datos en caso de contingencias, de necesidades de reproceso y por requisitos de disposiciones legales y reguladoras.

Deberá evidenciarse la existencia de procedimientos donde esté formalmente documentada la metodología de resguardos utilizada, las responsabilidades del personal apropiado, las prioridades de resguardo, los ciclos de rotación, los lugares de almacenamiento, las convenciones de rotulación. Además, deberán establecer la frecuencia de las pruebas sobre los resguardos, el mecanismo de selección de resguardos históricos para la realización de las mismas, la participación de los usuarios propietarios de los datos en ellas, y otros puntos que la entidad considere relevantes.

Las pruebas de recuperación y de integridad de los resguardos de datos deben ser formalizadas y debidamente documentadas. Las pruebas deben abarcar tanto resguardos actuales como históricos. Las mismas deben contemplar la antigüedad y el medio de almacenamiento utilizado. La documentación del resultado de las pruebas debe evidenciar la participación y conformidad por los resultados obtenidos de los usuarios propietarios de los datos.

Los períodos de retención de los resguardos de datos, programas y todo otro componente de información (diarios, semanales, mensuales, etc.) deben asegurar la recuperación de los mismos ante cualquier inconveniente de procesamiento que se presente al momento más cercano anterior el evento contingente.

Los procedimientos para el resguardo de datos, programas y todo otro componente de información deben prever, como mínimo, la generación de 2 (dos) copias de resguardos sincronizadas, manteniendo el almacenamiento de una de ellas en una localización distinta a la primaria, ubicada a una distancia determinada de acuerdo con el análisis de riesgos simultáneos que la entidad haya formalmente realizado.

Cuando sea factible, las entidades financieras podrán desarrollar mecanismos de redundancia automática para los resguardos de datos (duplicado o espejado on-line), cuyo alcance deberá abarcar tanto resguardos actuales como históricos. En dicho caso, este resguardo podrá ser considerado como una de las copias enunciadas en el párrafo anterior.

Se deberán mantener inventarios de todos los resguardos, tanto en el sitio primario como en el secundario, con clara identificación de su denominación nemotécnica, el tipo de contenido, la fecha de resguardo, los ciclos de rotación, períodos de retención, cantidad de usos del medio, fecha esperada de destrucción, responsable del resguardo, fecha de última prueba del resguardo, responsable de la prueba, y otros datos que la entidad financiera considere relevantes.

5.5. Mantenimiento preventivo de los recursos tecnológicos.

Se deberá observar la existencia de una política para la realización de mantenimiento preventivo de los recursos tecnológicos que soportan a los sistemas de información y de los recursos relacionados. También se crearán procedimientos formales para llevar a cabo dicha tarea, que contarán con cronogramas de mantenimiento. Se deben documentar las tareas realizadas y mantener en archivo los reportes, como mínimo por el doble del período que se haya fijado para el ciclo de mantenimiento.

Los cronogramas de mantenimiento deben estar coordinados con los de producción a fin de no impactar en la operatoria normal.

Cuando las tareas de mantenimiento sean efectuadas por recursos humanos externos, deben contemplarse las medidas de control de acceso físico enunciadas en la presente.

5.6. Administración de las bases de datos.

Las bases de datos son, en casi todos los casos, el repositorio de la información crítica de las entidades financieras. Las fallas en el manejo de las mismas pueden ocasionar, en forma intencional o no, la modificación no autorizada, la destrucción o exposición de datos e información crítica.

Los responsables del área de protección de activos de información y el área de operaciones y procesamiento de datos deben considerar cuidadosamente las implicancias en la seguridad de los sistemas administradores de bases de datos.

Muchas veces, los sistemas de administración de bases de datos (DBMS) cuentan con la posibilidad de mantener un registro de los accesos que se han realizado a las bases, en todos sus niveles, pero son desactivados.

Sin embargo, estos sistemas brindan la posibilidad de modificar, agregar o eliminar datos. Adicionalmente, es posible modificar derechos de acceso a los mismos, con el consecuente riesgo que esto implica cuando se ha imposibilitado el control de las actividades efectuadas sobre las bases de datos.

En todos los casos se deberá evidenciar la existencia de un fuerte control por oposición de responsabilidades en las actividades que realizan los encargados de gestionar los sistemas administradores de las bases mencionadas. Los controles ejercidos deben estar en concordancia con la frecuencia de administración de los DBMS, ser formalmente documentados, y en caso de no ser efectuados por el área de protección de activos de información, deben ser reportados a ella, en especial cuando se detecten distorsiones en el uso normal o intrusiones sobre los datos.

Los reportes deben ser mantenidos al menos por 2 (dos) años, a efectos de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.7. Gestión de cambios al software de base.

Se deben controlar los cambios en el software de base e instalaciones de procesamiento de información.

Se deben establecer responsabilidades y procedimientos formalmente documentados, para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software de base o los procedimientos operativos de procesamiento por lotes. Los sistemas operativos deben estar sujetos a un control estricto de los cambios. Cuando se cambien los programas, se debe retener un registro de auditoría que contenga toda la información relevante.

Los procedimientos deben contemplar e identificar las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Los cambios en el ambiente operativo pueden tener impacto en las aplicaciones. Por este motivo, se debe considerar la existencia -como mínimo- de la siguiente información:

- aprobación formal de los cambios propuestos;
- identificación y registro de los cambios significativos realizados;
- comunicación de detalles de cambios a todas las áreas pertinentes.

Esta documentación deberá ser mantenida, como mínimo por 2 (dos) años, a efecto de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

5.8. Control de cambios a los sistemas productivos.

A fin de minimizar el riesgo de actualizaciones accidentales en el entorno productivo, ingresar programas no probados y evitar accesos no autorizados a los datos, las entidades financieras deben definir un adecuado esquema de separación entre sus ambientes informáticos de procesamiento (desarrollo, prueba y producción). Se deberá asegurar que los analistas y programadores de sistemas no tengan acceso al entorno productivo, ni los operadores accedan al ambiente ni a las herramientas utilizadas para el desarrollo y el mantenimiento de los sistemas de aplicación, de acuerdo con el cuadro del punto 2.5.4. sobre segregación de funciones.

El proceso de actualización de nuevas versiones de sistemas deberá ser estrictamente controlado y realizado por personal que no tenga relación con el área de desarrollo y mantenimiento, mediante mecanismos que garanticen la correspondencia entre los programas "fuentes" y los programas "ejecutables".

Asimismo, las nuevas versiones y las modificaciones de los programas aplicativos deben someterse a procedimientos formales de revisión, registro y aprobación, antes de la implementación definitiva en el ambiente de producción.

En los casos de implementaciones de sistemas informáticos adquiridos, desarrollados o mantenidos por servicios externos, se deben registrar adecuadamente los cambios efectuados, verificando que todos los programas "fuentes" en custodia se correspondan con los programas "ejecutables", antes de su puesta operativa en el ambiente de producción.

5.9. Mecanismos de distribución de información.

La información generada por los sistemas informáticos, sea ésta en medios electrónicos o en copias impresas, deberá contemplar los recaudos mínimos de seguridad a efectos de impedir su difusión a personas no autorizadas.

Los responsables del área de protección de activos de información y el área de operaciones y procesamiento de datos son responsables del análisis y la implementación de los controles necesarios para limitar la pérdida de confidencialidad en la distribución de la información, tanto dentro como fuera de la entidad financiera.

Se valorará la aplicación de medidas tales como: utilización de sobres cerrados, cofres de seguridad para el transporte, el acceso limitado a los nichos de distribución de listados y la seguridad en las comunicaciones de los medios que soportan información.

5.10. Manejo de incidentes.

Se debe evidenciar la existencia de procedimientos formalmente documentados para la gestión, registro, accionar y comunicación de anomalías de los sistemas productivos y de software de base.

Se deben considerar, como mínimo, las siguientes acciones:

- advertir y registrar los síntomas del problema y los mensajes que aparecen en pantalla, fecha y hora del incidente;
- dejar constancia de la comunicación a los sectores responsables de la resolución;
- documentar las acciones realizadas, fecha y hora de la resolución.

Asimismo, deben implementarse adecuados procesos de respuesta para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados los mismos.

5.11. Medición y planeamiento de la capacidad.

El área de operaciones y procesamiento de datos deberá evidenciar la realización de análisis y planificación de capacidad, los que deben contemplar los planes estratégicos de la entidad financiera, la expansión de la base de clientes activos, los nuevos productos y servicios, la implementación de nueva tecnología y la adición de nuevos usuarios, entre otros factores.

5.12. Soporte a usuarios.

Deberá existir una función -que, de acuerdo con la complejidad que presente la entidad financiera podrá ser un área, sector o persona- para el soporte, registro y seguimiento de los incidentes que surjan con los sistemas, la tecnología informática y los recursos asociados. De esta manera, se asegurará a los usuarios de los sistemas productivos, tanto internos como externos al centro de procesamiento de datos, que continuamente tengan disponibles y en correcto funcionamiento los recursos de sistemas de información y la tecnología asociada que los soporta.

Esta función deberá mantener un registro con los inconvenientes que hayan surgido (paradas de programa, fallos de sistemas, cancelación, fallas de hardware, y todo otro tipo de incidente relevante), cuyo detalle permita identificar el tipo de problema, el recurso afectado, el/los usuario/s involucrados, el tiempo de ocurrencia, la acción inmediata realizada, la derivación a los responsables, la resolución final de inconveniente, entre otros detalles que la entidad financiera estime registrar.

Esta documentación deberá ser mantenida como mínimo por 2 (dos) años, a efectos de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

A los efectos de la presente normativa, “la banca electrónica” se define como la entrega de los productos y servicios de las entidades financieras, a través de medios electrónicos, a los usuarios internos o externos (clientes) de la entidad.

En esta definición se involucra a las tradicionales sucursales de las entidades financieras -donde la explotación de los servicios electrónicos está destinada a usuarios internos de las mismas- y a los accesos de clientes a los productos y servicios por medio de dispositivos electrónicos de acceso directo, tales como: cajeros automáticos (ATM); dispositivos de auto-consulta; computadores personales en lo tradicionalmente denominado “home banking”, aunque en la actualidad los accesos pueden realizarse por computadores personales conectados a la Internet, desde cualquier emplazamiento, no solo desde el hogar del cliente; asistentes digitales personales (PDA); dispositivos móviles de comunicación con capacidad de navegación por Internet (teléfonos celulares, dispositivos móviles con capacidad de conexión a Internet, otros); banca telefónica por dispositivos de tonos, y toda otra tecnología presente o futura que sea de aplicación para que el usuario externo (cliente) acceda a los servicios ofrecidos por las entidades financieras.

6.1. Controles generales.

El Directorio, o autoridad equivalente, es el responsable primario del reconocimiento y comprensión de los riesgos y amenazas que cada uno de los distintos canales por los que se ofrecen productos y servicios presenta para la entidad financiera.

Deberá evidenciarse la existencia de análisis de riesgos formalmente realizados para cada uno de los canales y para los servicios por ellos ofrecidos.

Todos los aspectos precedentemente mencionados en la presente normativa deben ser considerados para aquellos canales por los cuales las entidades financieras ofrecen sus productos y servicios. No obstante, existe un conjunto adicional de requisitos particulares para algunos de ellos que son delineados en este apartado.

Independientemente del canal por el cual se ofrece el servicio, éste se conforma de una comunicación electrónica de datos entre el centro de procesamiento de datos y el dispositivo del cliente final usuario del servicio. En este sentido, toda comunicación electrónica deberá mantener, como mínimo, los criterios de confidencialidad e integridad de los datos en tránsito. Para ello, se deberá evidenciar la aplicación de mecanismos de encriptación de robustez reconocida internacionalmente.

El grado de especificidad y complejidad de las comunicaciones electrónicas, y la consecuente gestión que éstas requieren, conlleva a que se aplique a las mismas la existencia de un responsable de su administración y monitoreo permanente. Las tareas llevadas a cabo por dicho responsable deben estar formalmente documentadas. La documentación resultante deberá ser mantenida, como mínimo durante 2 (dos) años, a efectos de posteriores controles por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

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 un 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. Este requerimiento se aplica de igual forma cuando esta actividad sea tercerizada, y al menos uno de los responsables firmantes deberá ser un funcionario de la entidad financiera.

- 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.

  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 durante 10 (diez) 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.

  No deberá utilizarse papel de transferencia térmica, pues su legibilidad se pierde con el transcurso del tiempo.

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 durante 10 (diez) 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.

- 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.

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, se deben aplicar las siguientes medidas de seguridad:

- 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.

- La tarjeta de débito, habilitada para realizar compras a través de puntos de venta, deberá permitir 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).

  Las transacciones de compra deben, en todos los casos, requerir el ingreso de la clave de identificación personal, y se emitirá un comprobante que deberá ser firmado por el titular de la tarjeta, quedando una copia en poder del mismo.

- 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 durante 10 (diez) 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.

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.

- 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 deben ser resguardados en carácter de históricos y por un término no menor a 10 (diez) 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.

- 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 deben 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 durante 10 (diez) 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.

7.1. Actividades factibles de delegación.

Las entidades financieras podrán delegar en terceros actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, en las condiciones fijadas por la Comunicación CREFI – 2 en su Capítulo II, Sección 6, o posteriores modificaciones.

Las condiciones normativas y reguladoras serán exigibles y aplicables de igual forma cuando las actividades se realicen en dependencias de terceros.

No podrán delegarse actividades con proveedores que a su vez tengan contratada la función de auditoría interna y/o externa de las mismas.

7.2. Responsabilidades propias de la entidad.

El Directorio, o autoridad equivalente de la entidad financiera, debe establecer y aprobar formalmente políticas basadas en un previo análisis de riesgos, con el fin de gestionar eficientemente el proceso de delegación de actividades que le son propias, vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas.

La delegación de las actividades antes mencionadas, nunca debe entenderse como transferencia de las responsabilidades primarias enunciadas en la presente normativa.

Las políticas deben reconocer el nivel de riesgo al que se expone la entidad financiera en las relaciones de delegación de actividades en terceros. Las mismas deben ser apropiadas al tamaño y complejidad de las actividades delegadas.

Para toda actividad vinculada a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deberá evidenciarse la existencia de contratos que definan claramente el alcance de los servicios, las responsabilidades y acuerdos sobre confidencialidad y no divulgación.

En los casos de entidades que cuenten con servicios de tecnología delegados a terceras partes, el control de la gestión de las facilidades para la protección de activos de información debe ser realizado con recursos propios, ya sea en locación de la entidad o en locación del tercero.

7.3. Formalización de la delegación.

Los contratos deben fijar como mínimo: el alcance de las actividades; los niveles mínimos de prestación de servicios y su tipo; la participación de subcontratistas; los derechos a realizar auditorías por parte de la entidad; compromisos de confidencialidad; los mecanismos de resolución de disputas; la duración del contrato; cláusulas de terminación del contrato; los mecanismos de notificación de cambios en el control accionario y en los cambios de niveles gerenciales; el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los sistemas, ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios o de operar en el mercado, a fin de poder asegurar la continuidad de procesamiento.

Además, los contratos deben establecer claramente la inexistencia de limitaciones para la Superintendencia de Entidades Financieras y Cambiarias, en cuanto a: el acceso a los datos, la revisión y tenencia de toda documentación técnica relacionada (diseño de archivos, tipo de organización, etc.) y a la realización de auditorías periódicas en las instalaciones del proveedor, a fin de verificar el cumplimiento de todos los aspectos contemplados en estas normas.

7.4. Responsabilidades del tercero.

Los terceros, en los cuales se hayan delegado actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deben mantener la aplicación de las pautas mínimas establecidas en las presentes normas.

7.5. Implementación del procesamiento de datos en un tercero.

La delegación de las actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas, deben evidenciar una clara separación de actividades, en aquellos casos en que el tercero brinde servicios a múltiples organizaciones, ya sean entidades financieras o de otro tipo de negocio.

La gestión y la guarda de los datos de una entidad financiera evidenciarán una separación lógica y/o física de los datos de otra organización.

Los sistemas de administración de la seguridad de los datos, y de los programas relativos a una entidad financiera, tendrán un entorno de seguridad individual que pueda ser controlado y monitoreado exclusivamente por los responsables indicados por la propia entidad financiera.

7.6. Control de las actividades delegadas.

El Directorio, o autoridad equivalente de la entidad, es el responsable primario sobre el control y monitoreo continuo del cumplimiento de los niveles de servicios acordados, el mantenimiento de confidencialidad de la información y de todos los aspectos normados por la presente comunicación para las actividades que hayan sido delegadas.

El control y monitoreo deberán mostrar una continuidad en su ejecución, relacionada con el nivel de riesgos que la entidad haya analizado y asumido. Deberán existir planes de ejecución de controles y documentación formalizada de los mismos, como así también de los requerimientos de mejoras solicitados al tercero, en caso de incumplimientos.

7.7. Planificación de continuidad de la operatoria delegada.

El Directorio, o autoridad equivalente de la entidad, es el responsable primario en establecer la existencia de un plan de continuidad de las actividades delegadas en terceros, a los fines de no cesar con las actividades normales de la entidad financiera y asegurar la continuidad de los servicios ante cualquier situación que pudiera sufrir el proveedor externo por la cual dejara de prestar sus servicios.

Asimismo, el Directorio, o autoridad equivalente de la entidad, es responsable de asegurar que el proveedor de servicios cuente con un adecuado plan de recuperación del procesamiento de datos, acorde a los requerimientos de negocio de la entidad y los niveles de riesgo asumidos por la misma. Este plan deberá ser probado en forma integral con frecuencia anual, la gerencia de la entidad deberá asegurar su resultado satisfactorio, y mantener documentación formal de las pruebas realizadas.

8.1. Cumplimiento de requisitos normativos.

Las entidades financieras deben considerar, en el diseño de los sistemas aplicativos que procesan su información comercial y de gestión, la implementación de apropiados controles según los requerimientos legales y reguladores vigentes, establecidos en las distintas comunicaciones emitidas por el Banco Central de la República Argentina.

Los requisitos mínimos de gestión, implementación y control de tecnología informática para los sistemas de información que se detallan en los siguientes puntos son aplicables a todas las entidades financieras, independientemente del tamaño, estructura, volumen y naturaleza de sus procesos de negocios. Asimismo, no son excluyentes de todos aquellos mecanismos adicionales que las entidades consideren que deben formar parte de su estrategia de administración y control informático.

8.2. Integridad y validez de la información.

En los sistemas aplicativos de información se deben implementar controles automatizados que permitan minimizar errores en la entrada de datos, en su procesamiento y consolidación, en la ejecución de los procesos de actualización de archivos y bases, y en la salida de la información.

Los datos que se registren en los sistemas deben ser sometidos a controles programados que aseguren la integridad, validez, confiabilidad y razonabilidad de la información procesada, incluyendo: dígitos verificadores, validaciones de códigos, tipo y tamaño de campos, rangos de valores, signos, referencias cruzadas, registro de operaciones fecha-valor, correlatividad de las operaciones, plazos, cierres y reaperturas de períodos, entre otros.

Se deben contemplar controles programados que limiten la modificación y la eliminación de datos -básicos y pactados- de las operaciones concretadas, movimientos y saldos. Asimismo, se deben implementar procesos automáticos para el devengamiento de intereses, el cálculo de cuotas, el redondeo de las cifras, y la aplicación de movimientos.

Debe existir una adecuada integración entre los sistemas aplicativos que procesan la información de la entidad y el sistema aplicativo de contabilidad. Se registrarán automáticamente en cada cuenta contable, en forma correcta y oportuna, todos los movimientos producto de las operaciones efectuadas.

En el sistema que administre la información sobre los clientes, se deben implementar adecuados controles de integridad, validez y razonabilidad, considerando la identificación única del cliente y los datos obligatorios de acuerdo con las normas vigentes. Además, deberán realizarse procesos periódicos de control y depuración sobre los mismos.

Los parámetros que limiten el ingreso de datos deben tener adecuados niveles de acceso para su actualización, y restricciones en cuanto a la posibilidad de ser modificados a través de funciones específicas.

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. 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, manteniéndose disponible por un término no menor a 10 (diez) años, en soportes de almacenamiento no reutilizables, 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.

.

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 Republica Argentina, y que en ningún caso permitan su modificación fuera de los sistemas aplicativos que la originaron.

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
	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. "A" 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.
	6.3.		"A" 4609	único	6.3.		
	6.4.		"A" 4609	único	6.4.		
	6.5.		"A" 4609	único	6.5.		
	6.6.		"A" 3198		11.7.		Según Com. "A" 4609.
	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.
	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.