4124

ACUERDO INTERBANCARIO

Seguridade y de la infc para cajer automátic puntos de y tarjetas c crédito y d

Seguridades físicas y de la información para cajeros automáticos, puntos de venta, y tarjetas de crédito y débito

Asociacion Bancaria
y de Entidades Financieras
de Colombia
ASOBANCARIA

Seguridades físicas y de la información para cajeros automáticos, puntos de venta, y tarjetas de crédito y débito

Santa Fe de Bogotá, D.C., Colombia
Julio de 1999

ASOCIACION BANCARIA
Y DE ENTIDADES FINANCIERAS
DE COLOMBIA, ASOBANCARIA

Presidente
Jorge Humberto Botero

Vicepresidente
Jaime Alberto Gómez

Gerente de Administración del Riesgo
Claudia María Luna González

Gerente de Información
María Constanza Mejía Meneses

Coordinadora de Publicaciones
Martha Luz Forero C.

© Asobancaria
ISBN 958-9040-60-8

Edición
Asociación Bancaria y de Entidades
Financieras de Colombia, Asobancaria
Cra. 9ª Nº 74-08 Piso 9º Tel. 2496411 Ext. 440
Faxes 2119915 - 2175594

Diseño e impresión
Artes gráficas Asobancaria
Cra. 7ª Nº 17-01 Piso 3º
Tel. 3411100 Fax 3411161

No está permitida la reproducción total o parcial de este acuerdo ni su transmisión en ninguna forma o por cualquier medio, ya sea electrónico, por fotocopia, por registro u otros medios, sin el permiso previo y por escrito del editor.

CONTENIDO

1. INTRODUCCION

Las entidades financieras, siguiendo con su compromiso ante la sociedad en lo relacionado con la prestación de sus servicios, evalúan constantemente y revisan, entre otras cosas, los efectos causados por los avances tecnológicos y el impacto que producen en la operación bancaria.

Es por esto por lo que, al encontrar una gran relación entre las medidas de seguridad existentes en el marco tecnológico y los niveles de siniestralidad, se hace necesario definir algunas normas mínimas de seguridad que deben tenerse en cuenta en la instalación y adecuación de cajeros automáticos, puntos de venta, Pin Pad, y tarjetas débito y crédito.

El presente acuerdo es el resultado de los trabajos desarrollados por el Comité Técnico de Riesgo Informático, coordinado por la Gerencia de Administración del Riesgo de la Asobancaria. En él, además de determinar los requisitos mínimos de seguridad física y lógica, se dan algunas recomendaciones adicionales que pueden adoptarse según el criterio de cada institución.

Los demás temas abordados por este comité se incluirán en su debido momento en el presente documento, si su importancia así lo amerita.

En este marco, y con una concepción muy clara de lo que significa una eficiente administración integral del riesgo, la Asociación Bancaria seguirá mostrando resultados concretos que fortalezcan la seguridad general de las entidades financieras.

Este propósito atenderá los requerimientos presentes en las circulares externas 002 y 097 de 1998 de la Superintendencia Bancaria y el Acuerdo Interbancario de agosto de 1996 de la Asobancaria titulado *Requerimientos mínimos de seguridad física en las oficinas de las entidades financieras de Santa Fe de Bogotá*.

Los tipos de riesgo que caracterizan un ambiente de procesamiento electrónico de datos y los procedimientos que se requieren para el control y la seguridad merecen una especial atención de los directivos de las instituciones financieras.

Este acuerdo se enmarca dentro de los estándares internacionales que permitirán una homologación con sistemas comúnmente aceptados desde el punto de vista de la seguridad y la tecnología, y contempla las recomendaciones hechas por el Comité de Basilea en cuanto a supervisión bancaria[1].

Las áreas de seguridad deben efectuar revisiones periódicas y con intervalos de tiempo adecuados en cuanto al cumplimiento de las consideraciones mínimas de seguridad adoptadas mediante el presente acuerdo interbancario.

Las entidades que presten (directa o indirectamente) el servicio de cajeros automáticos, puntos de venta y dispositivos de acceso deben velar porque exista un plan de seguridad de funcionamiento como parte del plan general de seguridad en la institución, así como establecer y mantener procedimientos para revisar contratos de adquisición de tecnología (máquinas y programas) y su cumplimiento frente al acuerdo. También deben tenerse y mantenerse procedimientos para la identificación sistemática y la implementación de cualquier mejoramiento necesario de la seguridad en el funcionamiento de los dispositivos anteriormente mencionados.

Estos esquemas de seguridad deben contemplar además procedimientos para el manejo, el almacenamiento y el análisis de las fallas y de los datos de fallas procedentes de los diferentes puntos que intervienen en una operación que involucre procesamiento electrónico de datos.

De esta manera se analizan los aspectos físicos y lógicos que, en materia de seguridad informática, deben considerar las entidades financieras, las redes, los establecimientos comerciales y toda institución o área que preste este tipo de servicios.

Para la implementación y adecuación de las disposiciones de este acuerdo interbancario, las entidades deben evaluar el tiempo apropiado de ajuste de los elementos ya instalados, teniendo en cuenta la ponderación de los riesgos a que está expuesto cada cajero o punto de venta.

1. *Los riesgos del sistema de cómputo y telecomunicaciones*, Comité de Basilea, Suiza.

2. LA JUNTA DIRECTIVA DE LA ASOCIACION BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA, ASOBANCARIA

CONSIDERANDO

1. Que entre las entidades financieras existen diferencias estructurales en cuanto a la tecnología instalada para la prestación de servicios financieros mediante dispositivos electrónicos (máquinas y programas);

2. Que se hace necesario establecer medidas de seguridad que beneficien al sector financiero y a los clientes;

3. Que las entidades financieras, a través de los comités técnicos de la Asobancaria, han venido adoptando una serie de acciones para prevenir el delito informático;

4. Que se hace necesario crear mecanismos para evitar que los clientes de las entidades financieras sean afectados por las modalidades de fraude informático;

ACUERDAN

PRIMERO: Adoptar, mediante el presente acuerdo interbancario, los siguientes requerimientos mínimos de seguridad para cajeros automáticos, puntos de venta, y tarjetas crédito y débito.

3. SEGURIDAD EN CAJEROS AUTOMATICOS

En razón de que los cajeros automáticos prestan servicio permanente al público y de que las entidades desean aumentar la seguridad en las principales

ciudades del país, se requiere implementar medidas de seguridad preventivas, tendientes a minimizar los riesgos a que se encuentran expuestos; por este motivo es necesario tener en cuenta las disposiciones del acuerdo interbancario y las recomendaciones dirigidas a las entidades financieras.

Estas instituciones deberán elaborar una clasificación de sus cajeros automáticos con base en estudios realizados por las áreas que cada entidad designe o exigir dicha clasificación a las entidades que presten el servicio, la cual estará determinada por el nivel de riesgo a que estén expuestos, así:

Tipo A: Cajeros con nivel alto de riesgo.
Tipo B: Cajeros con nivel medio de riesgo.
Tipo C: Cajeros con nivel bajo de riesgo.

En el presente documento, mientras no se determine lo contrario ni se especifique el tipo de cajero, entiéndase que la disposición se aplica para todas las clasificaciones.

La clasificación de riesgos deberá basarse en los siguientes criterios:

Se considera un cajero tipo A el que se encuentra instalado en una zona de alto riesgo de vandalismo, poca iluminación, sitios no monitoreados por la policía ni por empresas de vigilancia que hacen recorridos, como por ejemplo a los centros comerciales, etcétera.

Los cajeros tipo B son aquellos que están instalados en zonas no muy desoladas, con cercanía a algún tipo de edificación que cuente con vigilancia y un grado medio de circulación de personas.

Los cajeros tipo C son los que están situados en zonas bien iluminadas, en la parte interior de los centros comerciales, muy cercanos a estaciones de policía o dentro de la oficina de la sucursal bancaria y cuya zona está caracterizada por un alto índice de circulación de personas en el día y en la noche.

Sin embargo, las entidades podrán adaptar otros aspectos que consideren importantes como reglas para dicha clasificación.

3.1 Seguridad física

LOCALIZACION. Para definir la localización del cajero automático deben tenerse en cuenta las siguientes normas:

3.1.1 EL SECTOR. El cajero debe localizarse en zonas residenciales, comerciales o industriales, teniendo en cuenta que lo importante es que quede situado sobre vías principales en las cuales haya afluencia de público tanto en el día como en la noche y evitando instalarlos en sitios solitarios, oscuros y marginados (focos de proliferación de marginados y de vandalismo).

Para la instalación de cajeros automáticos en un determinado sector, éste debe contar con vigilancia o monitoreo frecuente por parte de la policía o de la entidad dueña del cajero.

3.1.2 UBICACION. En lo posible, los cajeros automáticos deben ubicarse en instalaciones de entidades financieras, centros comerciales, almacenes de cadena o supermercados, evitando la selección de locales en bares, sitios de juegos de azar o casinos.

DE LAS INSTALACIONES. Se tendrán en cuenta los siguientes aspectos:

3.1.3 EL LOCAL. En los cajeros clasificados con categoría A, ninguna de las paredes laterales, ni piso ni techo, deben colindar con otra instalación no vigilada, con el fin de evitar penetración mediante rompimiento de muros, techos y placas, exceptuando aquellos ubicados en centros comerciales y locales de las oficinas de la entidad. En caso de no poder aplicar esta medida, el local deberá fortalecerse aplicando las normas definidas para cuartos de bóvedas (panelerías de alta resistencia) e implementando las medidas de seguridad descritas en el numeral 3.2.1 de este documento.

3.1.4 LAS PAREDES. En todos los cajeros, la construcción de las paredes de cerramiento del área del cajero tiene que ser piso-techo (de acuerdo con la altura del cubículo) y en panel metálico ajustado a medidas óptimas de seguridad; además, las paredes deben estar provistas de una división que separe con una puerta la zona usuaria y la zona supervisor del cajero, cuya función es permitir el mantenimiento o el reaprovisionamiento del cajero. En caso de encontrarse ubicado en una entidad financiera y ser administrado por la misma entidad, se deja una puerta que comunique el área interna o supervisor del cajero con el hall bancario para permitirles el acceso a los encargados de la administración de los cajeros automáticos, pero sólo en caso necesario.

3.1.5 LAS PUERTAS. La puerta de acceso del usuario al cajero automático debe estar elaborada en algún tipo de material resistente (vidrio templado o laminado) de seguridad, ser totalmente transparente para que permita la visibilidad de los clientes desde el exterior y contar con una señal que indique la presencia del vidrio, ubicada de manera tal que no deje ver el teclado del cajero, y

provista además de una cerradura que le brinde seguridad al usuario mientras realiza la transacción. En lo posible, la entidad debe buscar que el bloqueo de la puerta de acceso al cajero esté a cargo de un medio electrónico de alta confiabilidad y funcionamiento.

La puerta de acceso a la oficina de la entidad debe protegerse con una reja de seguridad o reforzarse con una cerradura en panel metálico.

Igualmente, la puerta usuario-supervisor debe elaborarse en material resistente al fuego, provista de una cerradura de alta seguridad de combinación o de dos cerraduras, y en el centro de la puerta contar con un visor (ojo mágico).

El mecanismo de cierre de la puerta usuario-supervisor debe ser de anclaje automático –tipo caja fuerte– y con bisagras internas o pasadores de activación automáticos. El sistema debe contar con un desbloqueo interno del sistema en caso de incendio o catástrofe.

3.1.6 LA ILUMINACION. Los cajeros automáticos han de contar con una buena iluminación interna y externa, que permita una perfecta visibilidad en horas de la noche; dichos elementos de iluminación tienen que estar debidamente protegidos para evitar su sustracción o daño.

3.1.7 LA CAJA FUERTE DEL CAJERO AUTOMATICO. La caja fuerte debe estar provista de dos cerraduras de seguridad que permitan un manejo dual y cuyas claves para la elaboración de duplicados de sus llaves queden bajo la responsabilidad de un área o de una persona específica para tal propósito. El material de las paredes de la caja fuerte del cajero debe ser acero acorazado o altamente resistente contra taladro, soplete, plasma, discos de corte, estar protegido con dispositivos de bloqueo y, en lo posible, mecanismos de apertura automática retardada. Estos elementos pueden acompañarse de componentes disuasivos de violación.

3.1.8 ANCLAJE CAJA FUERTE. La caja fuerte debe ser anclada al piso desde su interior, de acuerdo con las especificaciones de anclaje del proveedor.

Si el cajero se instala en espacio abierto (empotrado a la pared) y no forma parte del perímetro de un edificio, deberá disponer de una cabina anclada al suelo y construida con paneles metálicos reforzados.

3.1.9 LA VENTILACION. Todos los cajeros automáticos instalados en áreas geográficas de clima cálido deben tener aire acondicionado. La instalación de este requerimiento tiene que hacerse de manera tal que no facilite un hurto.

3.1.10 LA CERRADURA DE LA PUERTA A LA ZONA USUARIO DEL CAJERO. Preferiblemente, debe tener un punto regulado por un mecanismo de emergencia que libere el picaporte y permita la salida del cliente.

3.1.11 EL CABLEADO. En todos los casos, el cableado que sea necesario extender dentro del cajero debe quedar protegido en canaletas, de tal manera que no sea de fácil acceso ni que quede visible.

3.1.12 ACCESORIOS. Todos aquellos accesorios de iluminación, decoración y aseo deben prevenir desde su mismo diseño e instalación actos de vandalismo o terrorismo contra el cubículo a través de elementos de cierre y fijación que imposibiliten o dificulten su retiro o el ocultamiento de artefactos explosivos.

3.2 SEGURIDAD FISICA A TRAVES DE DISPOSITIVOS ELECTRONICOS

3.2.1 SISTEMA DE ALARMA. Los cajeros automáticos deben estar protegidos por un sistema de alarma adecuado al tipo de cajero y en lo posible contar con dos vías de comunicación totalmente distintas, de manera que la inutilización de una de ellas produzca la señal de alarma de la otra.

El sistema de alarma y de comunicaciones debe ser monitoreado permanentemente por una central de monitoreo propia o contratada y, en todos los casos, dicha señal ha de enviarse a la Policía Nacional.

3.2.2 CIRCUITO CERRADO DE TELEVISION. Los cajeros cuya clasificación corresponda a tipo A deben estar provistos de un circuito cerrado de televisión, distribuyéndolos y dando prioridad a los que presenten mayor frecuencia de reclamos. Así mismo, es preciso mantener un período apropiado de retención de la grabación de las imágenes.

Los sistemas de video destinados a la grabación de imágenes deben estar protegidos contra robo y provistos de generadores o acumuladores de energía.

3.2.3 SOLUCION ENERGETICA. El cajero automático, sin importar su ubicación, debe tener solución energética que le permita operar normalmente en caso de fallas del fluido eléctrico.

3.2.4 CONTROLES DISUASIVOS. Se deben tener anuncios que adviertan la existencia de componentes de seguridad e incluir medidas preventivas y recomendaciones en la pantalla del cajero.

3.3 OTRAS MEDIDAS DE SEGURIDAD

3.3.1 APROVISIONAMIENTO. La entidad que esté encargada del aprovisionamiento de los cajeros debe suministrar a sus funcionarios su custodia mediante escoltas para el transporte en efectivo, los cuales permanecerán con ellos hasta que se haya efectuado toda la operación de aprovisionamiento; esto se aplica también a los cajeros que no están ubicados en una oficina o sucursal bancaria.

El aprovisionamiento debe realizarse en un momento en el cual no se exponga a mayor riesgo a los clientes de una oficina (especialmente si el cajero se aprovisiona desde adentro) o en horas normales de trabajo, con el fin de reducir la exposición a riesgos a los funcionarios encargados de esta labor durante horas irregulares. Por ningún motivo este procedimiento debe llevarse a cabo en horas nocturnas.

3.3.2 INFORMACION AL CLIENTE. Se debe informar y prevenir al cliente en cuanto a la manera como se debe operar el cajero, servicios ofrecidos, puntos más cercanos a ese cajero en donde pueden atenderse sus sugerencias y reclamos, prevención del fraude y procedimiento para el bloqueo de la tarjeta.

3.3.3 VISIBILIDAD. El sitio debe garantizar al cliente la privacidad de su clave secreta. Por ello, la disposición del cajero con respecto a la visualización que tienen las personas desde la parte externa de la cabina no debe facilitar que se descubra la clave cuando se está digitando (ver numeral 3.1.6).

3.3.4 DISTANCIA ENTRE CAJEROS. En los casos en que existan grupos de cajeros sin cabina (empotrados consecutivamente en la pared o en módulos especiales en centros comerciales), es preciso dejar una distancia prudencial entre ellos que permita un grado de confidencialidad en la transacción que un usuario está efectuando.

3.4 RECOMENDACIONES

3.4.1 CAJILLA DE SEGURIDAD PARA LLAVES. La cajilla de seguridad se implementa en caso de que la puerta de acceso al área supervisor se abra mediante llaves, para prevenir el riesgo de extravío debido a la manipulación y constante desplazamiento. La cajilla ha de estar provista de una cerradura de combinación y empotraje en el área del supervisor, con acceso al área del usuario a través de una contrapuerta de cierre con llave.

3.4.2 HALL DE SERVICIO. El hall de servicio podrá tener un dispositivo electrónico que controle el tiempo de permanencia del usuario en el cajero.

3.4.3 TELEFONO. Procurar que cerca del cajero automático esté instalado un teléfono público para que el cliente pueda efectuar operaciones como el bloqueo de la tarjeta u otros servicios.

3.4.4. ALARMAS. Es importante dar una inmediata y adecuada atención a las alarmas generadas por un cajero automático, ya que éstas pueden activarse con el fin de orientar la atención hacia un lugar específico.

3.4.5. BLOQUEO DE TARJETAS. Las entidades y las redes podrán instaurar mecanismos de bloqueo de tarjetas que se operen desde el cajero automático como una opción más en la pantalla, que se caracterice por no requerir la lectura de la banda magnética. Por ejemplo, el cliente podría digitar su clave y algún otro código que permita que a través de las vías de comunicación existente viaje la orden de bloqueo.

De igual manera se podrá hacer uso de este medio (la pantalla del cajero) para dar recomendaciones al cliente sobre la prevención de ilícitos, pasos que deben seguirse en caso de fallas y uso adecuado de la tarjeta.

Así mismo, se podrán fijar horarios para la apertura y cierre de aquellos cajeros con un nivel específico de riesgo y clasificación.

3.4.6 CALCOMANIAS. Se recomienda no pegar ningún tipo de calcomanía o aviso en la puerta de acceso del usuario al cajero que imposibilite la visibilidad.

4. SEGURIDAD EN PUNTOS DE VENTA

Los puntos de venta, técnicamente conocidos como POS (*Point of Sale*), son un medio para efectuar transacciones comerciales mediante el uso de dispositivos de acceso electrónico tales como tarjetas débito, crédito e inteligentes. Por ello también requieren el establecimiento de unas normas mínimas que fortalezcan la seguridad en los establecimientos comerciales y demás sitios donde se encuentran instalados.

4.1 SEGURIDAD FISICA

4.1.1 MODULOS ESPECIALES. En los casos en que se requiera, se pueden instalar módulos especiales que permitan una adecuada instalación física del equipo

que compone el POS (Pin Pad, datáfono, cableado, etc.), con el fin de impedir que sean movilizados y mantener un control de inventario de los mismos.

4.1.2 TRUNCAMIENTO. Todos los comprobantes expedidos por un punto de venta en el que se haga uso de información confidencial y que necesite niveles de seguridad tales como el número de cuenta, el número de identificación personal, etc., deben tener enmascarada parte de dicha información. Por lo general se remplazan los últimos cuatro dígitos por asteriscos o se imprimen únicamente los últimos cuatro dígitos.

4.2 RECOMENDACIONES

4.2.1 PROTECTOR DE PIN PAD. En todos los puntos de venta podrá instaurarse el sistema de protector de Pin Pad, el cual cumple la función de cubrir el teclado mientras el usuario digita su clave.

4.2.2 MANTENIMIENTO. Dado que el servicio de mantenimiento de los puntos de venta se hace fuera de línea, es preciso que las entidades financieras que tienen puntos instalados en las oficinas y las redes que prestan este servicio implementen dichos procedimientos de tal manera que sean claros y definidos para mayor control y detección de intentos de fraude.

Las entidades y las redes que prestan este servicio deben implementar un registro de control para ruteros (personal enrutado para el mantenimiento de los POS), independientemente de si el servicio es directo o subcontratado.

En lo posible, las entidades financieras que presten este servicio en sus oficinas y las redes en los establecimientos comerciales y demás, deberán crear un procedimiento que permita identificar, de manera remota, los puntos de venta que están fuera de servicio por mantenimiento o por otra causa y detectar señales de alerta en los casos en que sea necesario.

5. SEGURIDAD EN DISPOSITIVOS ELECTRONICOS DE ACCESO (TARJETAS DEBITO Y CREDITO)

Los dispositivos de acceso requeridos para el uso de cajeros automáticos, puntos de venta instalados en las sucursales de las oficinas bancarias y establecimientos comerciales necesitan también la definición de unos requerimientos mínimos de seguridad, así como una serie de recomendaciones que generen

un impacto positivo en los temas de seguridad física y lógica de estos procedimientos.

5.1 DE LAS OPERACIONES

5.1.1 CODIGO DE VERIFICACION. Las entidades que expiden las tarjetas débito y crédito deben asegurar que estos dispositivos tengan implementado el mecanismo de código de verificación, conocido técnicamente como CVV, CVC, CVT u otros equivalentes.

Este es un valor de chequeo criptografiado derivado de campos específicos de los datos, los cuales pueden ser el número de cuenta, fecha de servicio, llaves CVK, etcétera.

El CVV escrito sobre la tarjeta durante la transacción se envía al HSM (*Host Security Module*), el cual recalcula el CVV y lo compara con el recibido para confirmar la validez de la tarjeta.

5.1.2 TRANSPORTE, CUSTODIA Y ENTREGA DE TARJETAS DEBITO Y CREDITO. Las entidades deben incorporar internamente procedimientos, controles y seguridades en el transporte, custodia y entrega de las tarjetas débito y crédito, más aún si este servicio es subcontratado. Adicionalmente, las áreas de auditoría deberán expedir una certificación en cuanto al cumplimiento de estos procedimientos. La entrega de las tarjetas tiene que hacerse de manera personalizada, exclusivamente al beneficiario de la misma.

La entidad financiera debe darle una capacitación clara y sencilla al usuario (verbal o escrita), en la cual se le expliquen los cuidados, la responsabilidad directa, las prevenciones, los beneficios, la seguridad que se debe tener en los cajeros automáticos, puntos de venta en establecimientos de crédito y oficinas de las entidades, incluyendo además los procedimientos claros y definidos de cómo operar en caso de pérdida, robo y retenciones no autorizadas.

En lo posible, las entidades deben informar continuamente a sus empleados en todas las áreas (incluyendo este aspecto en el proceso de vinculación), usuarios y clientes de las diferentes modalidades de fraude a que están expuestos y de los controles internamente establecidos.

5.1.3 COMPROBANTE DE TRANSACCION. Todos los cajeros automáticos y los puntos de venta deben imprimir en el recibo (volante en papel) de la transacción,

únicamente los últimos cuatro dígitos del número de la cuenta del cliente o hacer truncamiento mediante el uso de asteriscos.

5.1.4 ATENCION DE RECLAMOS. Las entidades deben contar con un área de atención al cliente, mediante la cual se solucionen los problemas de las operaciones no exitosas; este programa de atención puede crearlo directamente la entidad o solicitar los servicios a un tercero, siempre y cuando la responsabilidad de su eficiencia esté a cargo de la entidad que lo contrata.

Las entidades deben revisar constantemente el servicio prestado por las redes, en cuanto al direccionamiento y enrutamiento de la información, así como las normas mínimas de seguridad que tienen que cumplir para alcanzar los objetivos de seguridad propuestos.

5.1.5 ENCRIPTACION. En la Circular Externa 002 de 1998, expedida por la Superintendencia Bancaria, se establece que debe encriptarse como mínimo el NIP (Número de Identificación Personal); sin embargo, las entidades tienen que encriptar la información que en su opinión deba estar protegida y cubierta, como por ejemplo el número de cuenta, el nombre del usuario, etcétera.

5.1.6 ORIGEN DE LAS TRANSACCIONES. Las entidades deben confirmar la autenticación del origen de las transacciones por cualquier mecanismo que asegure que la información transmitida por una terminal financiera sea reconocida y validada por el sistema central y viceversa.

Algunas de las anteriores consideraciones en materia de seguridad de las transacciones efectuadas mediante el uso de tarjetas débito y crédito están consignadas en la Circular Externa 002 de 1998, expedida por la Superintendencia Bancaria.

6. SEGURIDAD DE LA INFORMACION EN LAS COMUNICACIONES

Teniendo en cuenta que la información y el transporte electrónico de datos se realizan a través de diversos dispositivos electrónicos, se define la siguiente estructura mínima, caracterizada por diferentes niveles para la seguridad de la información.

El propósito que se busca con el establecimiento de controles mínimos de seguridad de la información en las comunicaciones es evitar al máximo que la información sea interceptada o interrumpida.

Así mismo, las entidades podrán fijar niveles de confidencialidad de la información teniendo en cuenta la clasificación que para todos los casos se ha utilizado en el presente acuerdo interbancario, significando que la información de mayor confidencialidad debe clasificarse como tipo A, la de medio grado de confidencialidad como tipo B y la información que puede no requerir todos los controles en la estructura de seguridad en las comunicaciones como tipo C.

El proceso que se le debe dar a la información en las diferentes entidades financieras, así como en cada una de sus áreas relacionadas con las operaciones en cajeros automáticos y puntos de venta a través de tarjetas de banda magnética (esquema que puede aplicarse en parte también a la nueva tecnología de tarjetas inteligentes que trabajan con microcircuitos), deben tener en cuenta los siguientes aspectos:

6.1 CERTIFICACION

Es preciso que en las entidades se establezca un área que conozca en detalle quiénes actúan en la red en el nivel de operación de máquinas y programas o de una combinación de ambos esquemas.

La definición de esta área permitirá certificar qué usuarios están o no autorizados y facilitará la detección de los ingresos no aprobados a los diferentes sistemas de telecomunicación y procesamiento de datos de la entidad.

En esta área se debe buscar un mecanismo que permita almacenar la información de cada usuario, las llaves públicas y privadas que se manejan, los niveles o atributos que se le han asignado, un histórico que permita conocer los diferentes estados del usuario en cuanto a si ha sido suspendido, cancelado, activado, modificado, ambientes en los cuales ha estado involucrado (revisión, producción, etc.), lo cual se puede lograr mediante la utilización de tarjetas de identificación electrónica que envíen y transmitan los datos de acceso en cuanto a fecha, lugar, plataforma, área, etc., a una central de control o mediante la implantación de un esquema administrativo de control que permita hacer el seguimiento adecuado a este tipo de actividades.

Gracias a esto el usuario tendrá niveles de acceso a los sistemas de información de acuerdo con normas preestablecidas para tal propósito, y permitirá además que se identifiquen claramente los usuarios que comparten plataformas tecnológicas.

6.2 AUTENTICACION

Debe existir un método de autenticación que verifique el origen, contenido, calidad y estructura en que viaja la información relacionada con las transacciones de los usuarios en cada uno de los tramos donde se realiza la comunicación y, en los casos en que se pueda, confrontarla con la información previamente almacenada.

Este tipo de autenticación debe efectuarse mediante una vía segura y con la utilización de llaves de comunicación individuales en cada uno de los tramos.

6.3 VALIDACION

En este proceso de seguridad en las comunicaciones deberán verificarse las firmas digitales y las claves de acceso a cada uno de los sistemas con prueba de identidad clara e irrefutable que garantice cómo, quién y cuándo hizo la conexión.

Superados los anteriores pasos en la estructura de seguridad en la comunicación, se considera la conexión válida para ejecución e inicio de procesos con la información.

6.4 ENCRIPTACION

Las entidades financieras y las redes que soportan esquemas tecnológicos para el manejo de la información en los procesos que se relacionan con las transacciones efectuadas desde un punto de venta o un cajero automático a través de la utilización de tarjetas crédito y débito deben garantizar que dicha información viaje cifrada, es decir, que esté encriptada.

Las entidades deben encriptar como mínimo los campos en donde se transmita el número de identificación personal o clave (NIP). Dicho proceso ha de implementarse a través de *hardware* en diferentes puntos dentro de la oficina (Circular Externa 002 de 1998, Superintendencia Bancaria).

Para los puntos situados en establecimientos comerciales y las transacciones que se realicen con tarjetas desde las oficinas, la encriptación se implementará preferiblemente desde el teclado o desde algún punto de la oficina. Además, debe garantizarse que el número de identificación personal (NIP) esté protegido en todos los puntos de la transmisión.

Para tal efecto tienen que incluirse en los procedimientos de comunicación dentro de las oficinas unos procesos de cifrado de la información que contemplen, por lo menos, algoritmos certificados a nivel mundial tales como RSA, *Data Encryption Standard* (DES), Triple DES (encripta la información tres veces con claves diferentes) y el *International Data Encryption Algorithm* (Idea), entre otros.

Es preciso tener en cuenta que dicha información, en función de los servicios ofrecidos por la entidad, puede viajar a manera de voz, datos, fax, video y combinación de los anteriores.

Las entidades deben tener presentes los tramos entre los cuales se da la comunicación y los requisitos de encriptación de cada uno de ellos. Para efectos de encriptar información que sale de la oficina o sucursal bancaria es necesario que se haga a través del método de encriptación por *hardware*, siendo opcional que en el interior de la oficina se maneje la encriptación por *software* a través de algoritmos certificados internacionalmente para cifrar la información.

Los dos elementos importantes que hay que tener en cuenta en la encriptación son el algoritmo de encriptación y el manejo de claves.

6.5 NO RECHAZO

Las entidades deben velar porque en el mecanismo instaurado para el control de la información esté presente permanentemente el paso conocido como "No Rechazo", el cual significa la prueba irrefutable de la identidad del emisor de la información, la integridad de los datos recibidos y enviados, lo cual servirá a su vez como complemento para las pistas de auditoría a nivel aplicativo.

La anterior estructura de seguridad debe aplicarse para las áreas que manejen la información de las claves, NIP (Número de Identificación Personal), cintas de transmisión de video o archivos de video almacenados en disco duro, números de cuenta, cupos asignados, información sobre créditos, características propias de la transacción; en sí, toda la información involucrada en una operación con tarjeta a través de un punto de venta o un cajero automático.

En la estructura de seguridad de la información es preciso contemplar las características específicas que requieren los diferentes ambientes, tales como correo electrónico e Internet.

Dicha estructura debe acondicionarse a los lineamientos y directrices de las áreas de auditoría y de quienes controlan y evalúan el desempeño de los dispositivos a través de *hardware* y *software*.

6.6 CONTROL DE ADMINISTRACION (PUERTOS Y DIRECCIONES EN LA COMUNICACION DE DATOS)

Es necesario contar con las guías adecuadas para el control de puertos y direcciones asignadas (LU, circuitos virtuales, direcciones IP, etc.) en la conexión de una terminal financiera, una conexión Internet o cualquier conexión que la entidad utilice para el flujo de transacciones financieras, con el propósito de dar seguridad en la plena identificación de cada conexión. Este control debe permitir diferenciar entre puertos (direcciones) de pruebas y de producción.

6.7 IDENTIFICACION DE TERMINALES

Se debe mantener una metodología de asignación de terminales locales y remotas (incluyendo cajeros automáticos) que permita identificar, registrar, establecer y verificar la pertenencia y acceso a la entidad en el momento del ingreso en los sistemas principales.

6.8 INTERCAMBIO DINAMICO DE LLAVES

Las entidades deben utilizar el intercambio dinámico de claves de comunicación (llaves) entre los sistemas de encriptación implantados con una frecuencia que garantice la máxima seguridad y evite conocer las llaves iniciales de codificación, dificultando así la obtención de los datos y acatando las disposiciones que para tal efecto determinó la Superintendencia Bancaria a través de la Circular Externa 002 de 1998.

6.9 MONITOREO DE ESTADO DE TERMINALES EN COMUNICACIONES

Es preciso contar con un sistema y un procedimiento de monitoreo que garanticen el aviso de una anomalía y la atención inmediata de recuperación por eventos de falla en las comunicaciones en las terminales financieras (en cajeros automáticos y puntos de venta es muy importante, puesto que puede tratarse de la comisión de un delito).

6.10 MANTENIMIENTO DE EQUIPOS

Las entidades deben crear un plan de mantenimiento de equipos de comunicación que garantice el funcionamiento de las conexiones y su flujo transaccional, incluyendo los registros respectivos de dicho mantenimiento, siempre con la responsabilidad del área donde se realiza la operación, acompañado de un procedimiento de control sobre las personas que lo realizan y un archivo histórico de los cambios efectuados, teniendo en cuenta los diferentes niveles de acceso a los sistemas de información.

En el área de producción no se deben tener equipos sin identificación, apagados indefinidamente o inutilizados por reposición, pues esto aumenta los riesgos de intromisión no deseada.

6.11 MODIFICACIONES A LA CONFIGURACION DE LA RED DE COMUNICACIONES

En los casos en que se necesite, las entidades deben tener un control específico sobre los equipos de análisis de comunicaciones (como por ejemplo los analizadores de protocolo), en cuanto a su ubicación, motivo de utilización, archivos grabados, con el fin de delimitar las responsabilidades y minimizar los riesgos de interceptación internos en la entidad.

Se debe velar porque exista un procedimiento de modificaciones o inclusiones a la configuración de la red de comunicaciones, que registre los cambios de manera estándar, con una verificación previa de pruebas de campo o situaciones similares a las de producción.

6.12 RECOMENDACIONES

- Se debe tener en cuenta que los problemas generados por fallas físicas y técnicas de los equipos involucrados en un ambiente de procesamiento de datos y comunicaciones, podrán ocasionar inconvenientes de tipo administrativo y de control de las operaciones; igualmente, problemas en las comunicaciones pueden causar dificultades de seguridad física.

- Dado que las entidades cuentan con diferentes áreas y posiblemente diferentes plataformas tecnológicas entre ellas, entre sus oficinas, etc., hay que detectar en la estructura de seguridad física y lógica todos los posibles puntos de exposición a riesgo y establecer de la manera más clara posible los controles administrativos y procedimientos que deben tenerse en cuenta.

- Toda información confidencial relacionada con las operaciones con tarjetas débito, crédito e inteligente que por motivo alguno haya requerido la impresión de un reporte escrito (papel), debe contemplarse dentro de un esquema de seguridad para información preliminar o borrador, teniendo en cuenta su clasificación en los niveles de confidencialidad, las copias que se han generado del documento, el destino de cada una de ellas y verificar que el destino corresponda a usuarios autorizados en el proceso de certificación. Los usuarios autorizados deben velar porque esa información no quede libre de acceso y permanezca bajo llave.

- Procurar y verificar que las entidades con las que se tiene relación en cuanto al diseño, tecnología, elaboración de tarjetas, centros de realce y entrega de plásticos tengan creados procedimientos de control y seguridad en cuanto a la información que manejan sobre las tarjetas o los usuarios.

ANEXO

INDICE DE NORMAS ICONTEC RELACIONADAS CON LOS TEMAS CONTENIDOS EN EL PRESENTE ACUERDO INTERBANCARIO

El Instituto Colombiano de Normas Técnicas ha generado una serie de normas relacionadas con el tema del procesamiento electrónico de datos y las tarjetas plásticas a través de máquinas y programas.

La siguiente es una relación breve de algunas de las normas más relacionadas con estos aspectos, las cuales se encuentran a disposición en el Icontec.

NTC 2363 (Establece funciones, incluye procesos principales, equipos utilizados, presentación y organización de datos, programación y operación de computadores, equipos periféricos y aplicaciones particulares).

NTC 2364 (Procesamiento de la información, codificación y clasificación de caracteres para intercambio de información, tablas de códigos, caracteres de control de transmisión, extensiones de códigos, dispositivos y otros).

NTC 2365 (Procesamiento de la información, estructura de caracteres intermitentes y sincrónicos destinados a la transmisión, sentidos de paridad, encadenamientos).

NTC 2439 (Procesamiento de la información).

NTC 2552 (Sistemas para el procesamiento de la información, comunicación de datos, interfaces, conexión y asignación de pines).

NTC 2553 (Procesamiento de la información. Comunicación de datos, controles de enlace, datos de alto nivel, convenciones de direccionamiento, dígitos binarios).

NTC 2554 (Organización de datos, términos y definiciones).

NTC 2634 (Vocabulario, control, integridad y seguridad de la información).

NTC 2676 (Elementos para informática. Características dimensionales, físicas y magnéticas).

NTC 2732 (Interconexión de sistemas abiertos).

NTC 2777 (Uso de paridad para la detección de errores en la transmisión).

NTC 2869 (Banca y servicios financieros. Tarjetas bancarias. Banda magnética. Contenido de datos de la pista TRACK 3. Definiciones sobre características físicas de la tarjeta, posición y dimensión de los datos en relieve, funcionamiento del material magnético, especificaciones de codificación de la pista 3).

NTC 2869 (Estructura de archivo y rotulado de cintas magnéticas para intercambio de información).

NTC 2909 (Banca y servicios financieros. Tarjetas para transacciones financieras. Definiciones y especificaciones de localización de los datos realzados, tarjetas no realzadas tamaño alternativo, sistemas de numeración de cuenta de transacciones financieras).

NTC 2921 (Símbolos de documentación y convenciones aplicables a diagramas de flujo de datos, de programación y de sistemas).

NTC 2922 (Interfaces entre sistemas computarizados y los procesos técnicos).

NTC 2968 (Tecnología de la información, comunicación de datos, términos y definiciones, medios y técnicas de transmisión).

NTC 2969 (Banca y requisitos financieros. Tarjetas de identificación. Técnicas de registro. Localización de pistas de solo lectura. Pistas 1 y 2).

NTC 2970 (Banca y servicios financieros. Técnicas de registro. Localización de caracteres realzados en tarjetas de tipo ID-1).

NTC 2971 (Banca y servicios financieros. Seguridad física y electrónica. Administración y requerimientos del PIN (Número de Identificación Personal, NIP). Ciclo de vida del PIN. Administración de claves).

NTC 3213 (Comunicaciones. Características de las redes de área local LAN).

NTC 3214 (Banca y servicios financieros. Técnicas de registro en banda magnética, material magnético, características de desempeño, técnicas de codifica-

ción, especificaciones de codificación para pistas de solo lectura y de lectura-escritura).

NTC 3270 (Banca y servicios financieros. Seguridad física y electrónica. Requisitos para la autenticación de mensajes, procedimientos de aprobación para algoritmos de autenticación).

NTC 3349 (Define los principales conceptos básicos que involucran la confiabilidad, el mantenimiento y la disponibilidad en el campo del procesamiento de datos).

NTC 3431 (Definiciones, localización del material magnético, localización de las pistas de datos codificados, comienzos de la codificación).

NTC 3451 (Tarjetas de circuitos integrados con contactos. Características físicas).

NTC 3500 (Contiene definiciones y consideraciones en comunicaciones con la utilización del protocolo de nivel de paquete X.25 en redes de área local LAN).

NTC 3560 (Procedimientos y desarrollo. Guía para la adquisición de sistemas de computación. Establece recomendaciones para tener en cuenta en la adquisición de sistemas de computación).

NTC 3585 (Sistemas de procesamiento de la información. Auditoría. Programa de aseguramiento de calidad para el *software* previamente desarrollado utilizando aplicaciones no críticas).

NTC 4077 (Establece definiciones y términos de conceptos utilizados en el procesamiento de la información).

NTC 4079 (Términos y definiciones relacionados con el procesamiento de datos).

NTC 4094 (Unidades de procesamiento aritméticas, registro y convertidores. Facilita la comunicación internacional en el procesamiento de la información).

Este acuerdo se terminó de imprimir
en el taller de artes gráficas
de Asobancaria en julio de 1999
Santa Fe de Bogotá, D.C., Colombia