# Requerimientos de seguridad y calidad en el manejo de información a través de canales de distribución de productos y Servicios Financieros

(Proyecto de Circular – Junio 2007)

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007

Biblioteca Luis Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

**Conferencista:**
**Pablo A. Malagón T.**

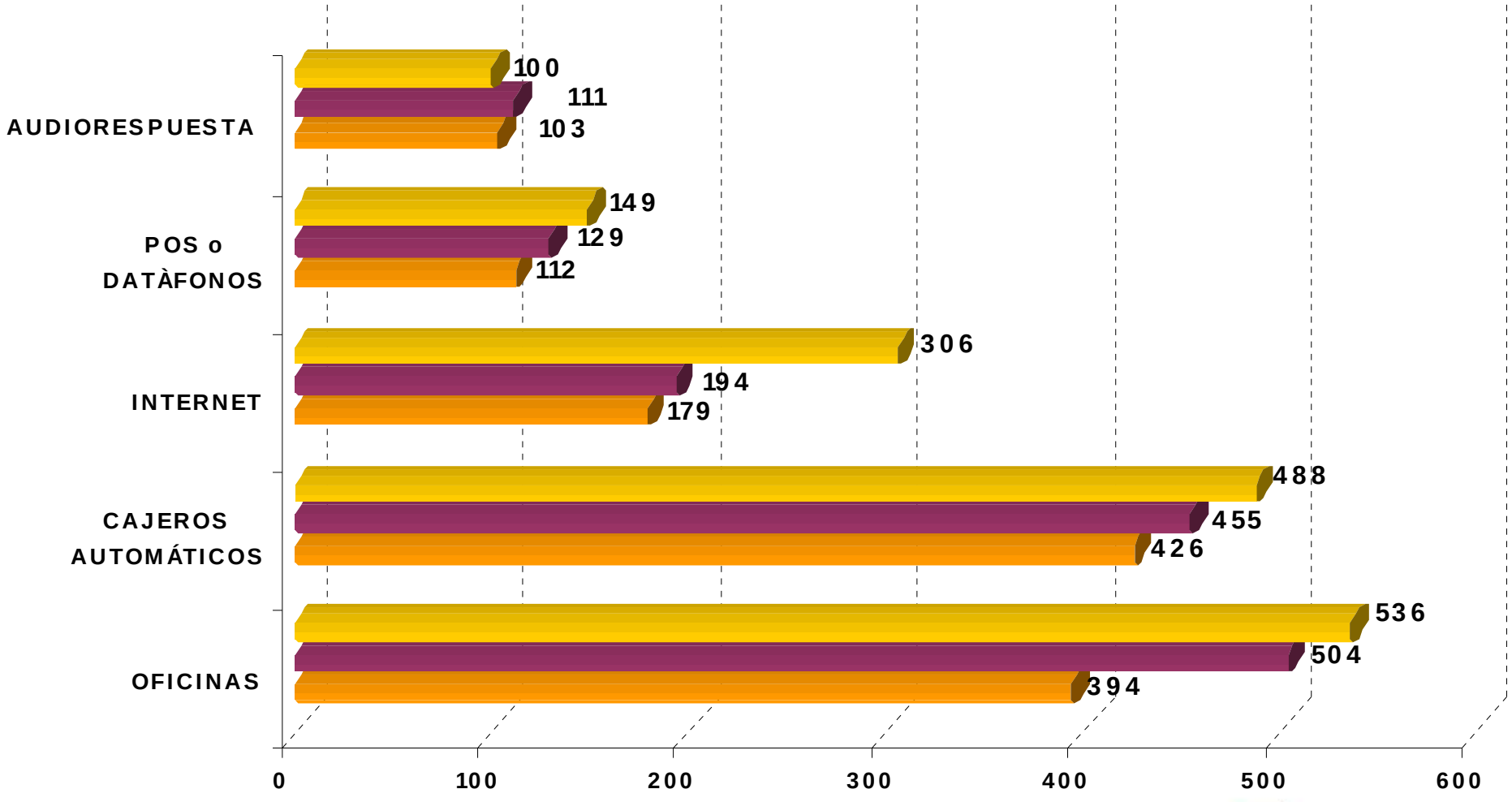
ACIS

# Agenda

1. Antecedentes
2. Sistema de Administración de Riesgos Operativos (SARO)
3. Requerimientos del proyecto de Norma
   - Consideraciones
   - Ámbito de aplicación
   - Estructura del proyecto

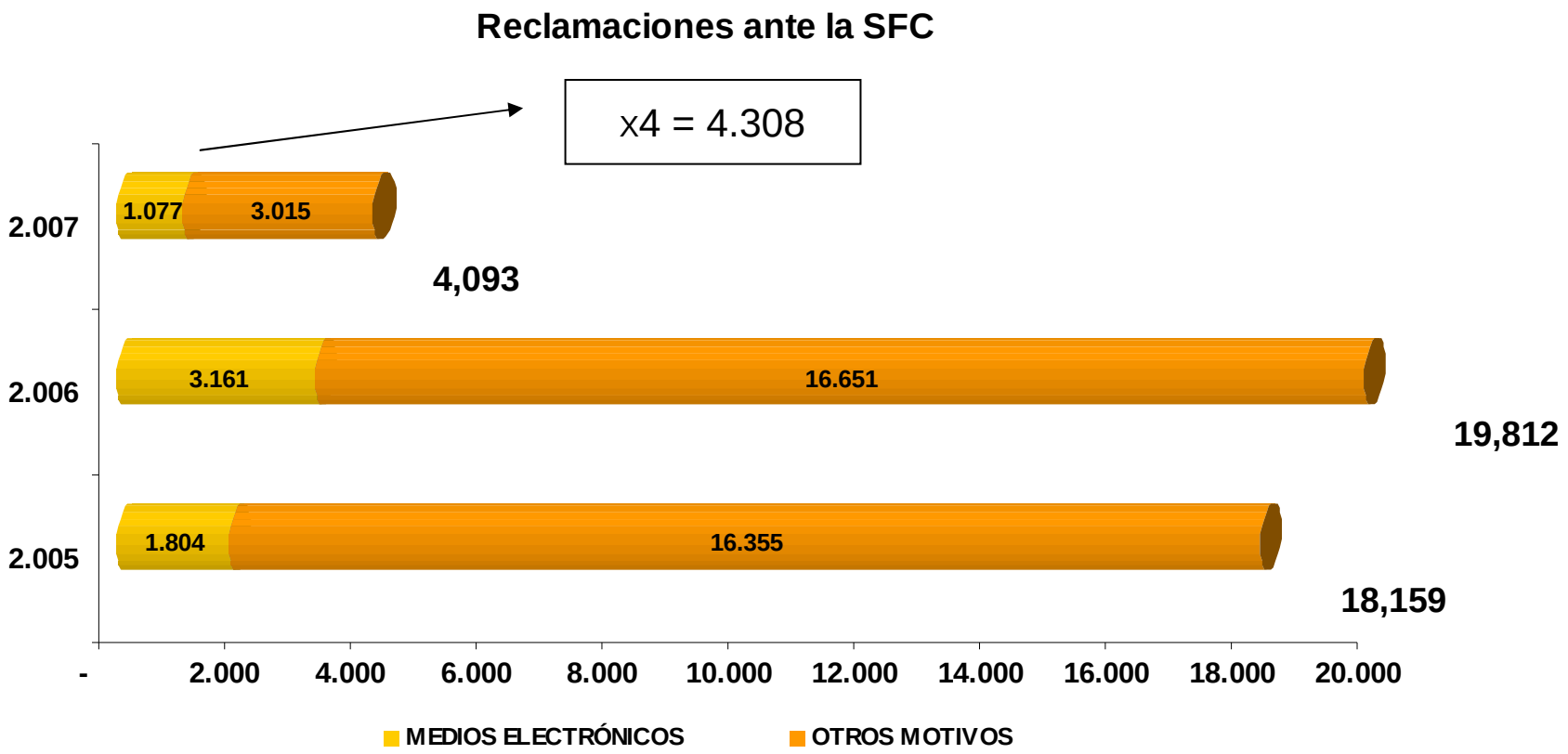
# 1. Antecedente - Transaccionalidad

**(millones)**



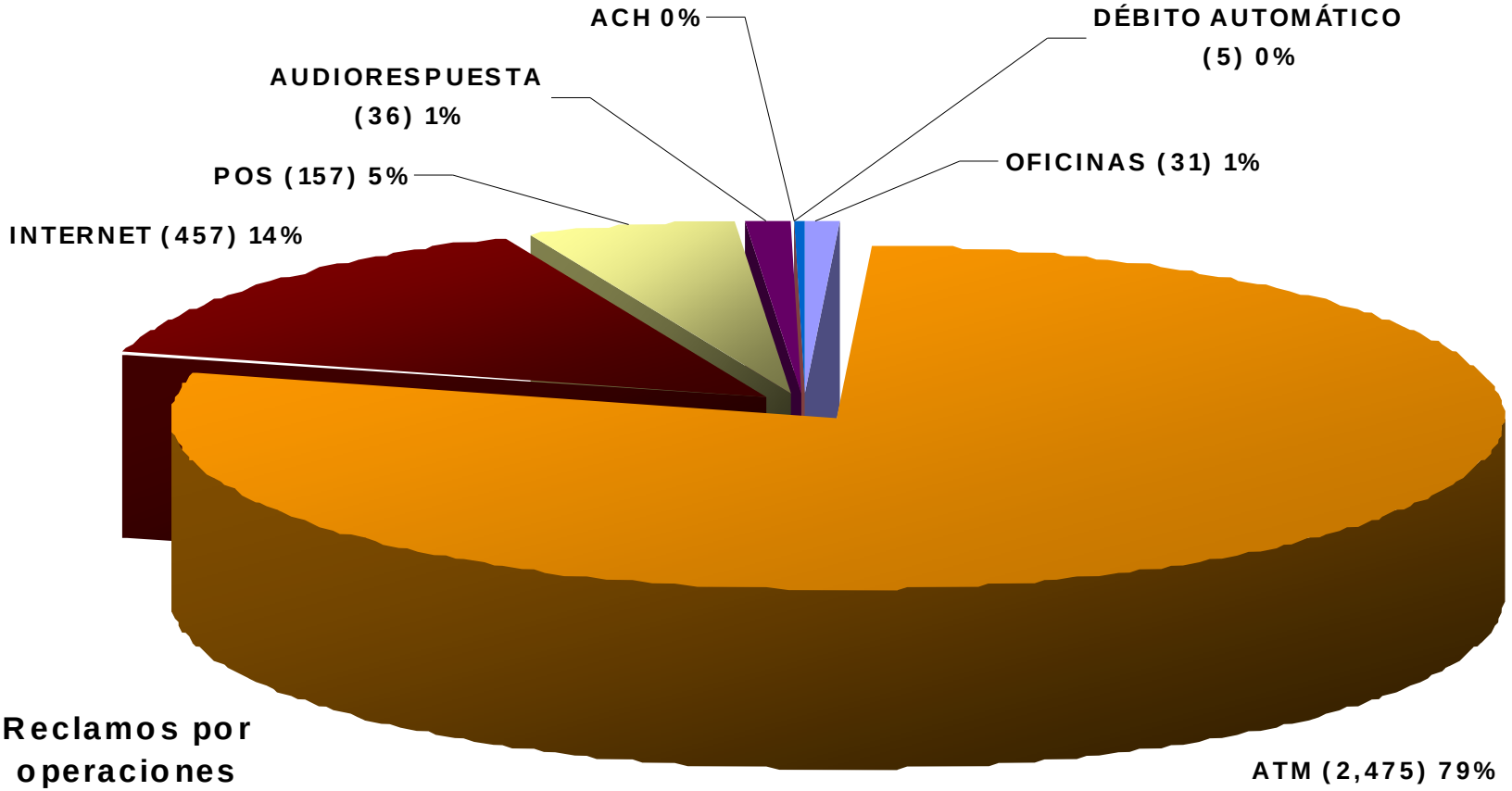

Fuente: SBIF

# Antecedente - Quejas




- Fuente: SFC - Sistema FED (Flujo electrónico documental).
- El dato para 2007 corresponde al acumulado al primer trimestre.
- Medios electrónicos incluye: ATM, Internet, POS és de datáfono, débito a cuenta sin autorización de titular, falla en red de oficina, reclamo por audiorespuesta, reclamo por internet y retiro en cajero

# Antecedente - Quejas




**Reclamos por operaciones electrónicas: año 2006**

# 2. Sistema de Administración de Riesgos Operativos (SARO)

**Riesgo Operativo**

Es la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Esta definición incluye el riesgo legal y reputacional asociados al los factores de riesgo operativo.

## Factores

- Recurso humano
- Procesos
- Tecnología
- Infraestructura
- Externos

## Clasificación de Eventos

- Fraude interno
- Fraude externo
- Relaciones laborales
- Clientes
- Daños de activos físicos
- Fallas tecnológicas
- Ejecución y Admon. de procesos

# Etapas del SARO

- **Alistamiento y preparación:** estructura, políticas, objetivos, alineación con planes estratégicos.
- **Identificación R.O.:** todos los procesos.
- **Medición:** cualitativa/cuantitativa. Perfil de riesgo Inherente
- **Control:** Planes de acción y Adm. continuidad del negocio.
- **Monitoreo:** evaluar efectividad de los controles y seguimiento a niveles de riesgo residual.

# Elementos del SARO

- Políticas, objetivos: cultura y compromiso.
- Procedimientos: operación de SARO.
- Documentación: soporte a la gestión.
- Estructura organizacional:
  - Junta Directiva
  - Representante legal
  - Unidad de Riesgo Operativo
  - *Funcionarios*

# Elementos del SARO

- Registro de eventos: todos.
- Órganos de control: evaluación del SARO.
- Plataforma tecnológica: sistemas necesarios.
- Divulgación de la información: revelación de la gestión del RO.
- Capacitación: periódica para todos los funcionarios.

# 3. Requerimientos del proyecto de Norma

- Consideraciones
- Ámbito de aplicación
- Estructura del proyecto

# Consideraciones

Medidas tendientes a:

- Actualizar la normatividad vigente.
- **Mitigar los riesgos** asociados a los medios y canales de distribución de productos y servicios.
- Mejorar el servicio en la atención al cliente.
- Proteger al consumidor financiero.
- Incrementar la confianza en el sector financiero.

# Ámbito de aplicación

Las instrucciones de que trata el presente numeral deberán ser adoptadas por todas las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC), con excepción de las siguientes entidades:

–Fondo de Garantías de Instituciones Financieras “Fogafin”,
–Fondo de Garantías de Entidades Cooperativas “Fogacoop”
–Fondo Nacional de Garantías S.A. “F.N.G. S.A.”
–Fondo Financiero de Proyectos de Desarrollo “Fonade”
–Los Almacenes Generales de Depósito
–Los Fondos de Garantía que se constituyan en el mercado público de valores
–Los Fondos Mutuos de Inversión
–Los Fondos Ganaderos
–Las Sociedades Calificadoras de Valores y/o Riesgo
–Las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior
–Los Corredores de Seguros y de Reaseguros
–Los Comisionistas Independientes de Valores
–Las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación
–las Entidades Administradoras del Régimen de Prima Media con prestación definida, excepto aquellas que se encuentran autorizadas por la ley para recibir nuevos afiliados

# Estructura del Proyecto

- Definiciones.
- Obligaciones Generales:
  - Seguridad y Calidad.
  - Documentación.
  - Divulgación.
- Obligaciones adicionales por tipo de canal.
- Reglas de actualización del software.
- Obligaciones por tipo de medio – Tarjetas.
- Análisis de Vulnerabilidades.

# Estructura del Proyecto - Definiciones

## Criterios de Seguridad de la información

a) **Confidencialidad:** Hace referencia a la protección de información cuya divulgación no está autorizada.
b) **Integridad:** La información debe ser precisa, coherente y completa desde **su creación hasta su destrucción**.
c) **Disponibilidad**: La información debe estar en el momento **y en el formato que se requiera ahora y en el futuro**, al igual que los recursos necesarios para su uso.

## Criterios de Calidad de la información

a) **Efectividad:** La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
b) **Eficiencia:** El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
c) **Confiabilidad:** La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

# Estructura del Proyecto - Definiciones

**Cifrado fuerte**

Técnicas de cifrado, con algoritmos de robustez reconocidos internacionalmente, que proporcionan una adecuada relación entre el nivel de procesamiento y la seguridad requerida por la información.

**Operación**

El conjunto de acciones que permiten el intercambio de datos a través de los canales de distribución, como por ejemplo, una consulta de saldo, cambio de clave, actualización de datos básicos del cliente, etc. y que no implican movimiento de dinero.

Las acciones que permiten movimiento de dinero (transacciones) tales como: retiros, transferencias, depósitos, pagos, etc.

# Obligaciones Generales: Seguridad y Calidad (1)


- Gestionar la seguridad de la información →Podrán tener como referencia los estándares ISO 17799 y 27001
- La información confidencial enviada a los clientes por e-mail → cifrada y libre de software malicioso
- Evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo deberá ser única y personalizada.
- **Brindar la posibilidad de identificación con otros mecanismos de autenticación.**
- Permitir a los clientes personalizar las condiciones bajo las cuales se les prestará servicios.

# Obligaciones Generales: Seguridad y Calidad (2)


- Ofrecer la posibilidad de manejar una contraseña diferente por canal.
- Brindar la posibilidad inmediata de cambiar la clave de la tarjeta débito en el momento que el cliente lo considere necesario.
- Elaborar el perfil de las costumbres transaccionales de sus clientes.
- Segregación de funciones del personal que administre, opere, mantenga y, en general, tenga la posibilidad de acceder a los dispositivos y sistemas usados en los distintos canales.
- Sincronizar los relojes (SIC).
- Considerar la atención de personas que pudieran requerir una atención especial, con el fin de que no se vea menoscabada la seguridad de su información.

# Obligaciones Generales: Seguridad y Calidad(3)


- Tercerización – Outsourcing:
  - Criterios de selección
  - Plan de contingencia del servicio convenido
  - Contratos → niveles de servicio, acuerdos de confidencialidad, propiedad de la información, normas de seguridad informática y física , procedimientos para cuando hay evidencia de alteración o manipulación de equipos o información, y para la entrega y destrucción de la información manejada.
  - Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.

# Obligaciones Generales: Documentación

- Dejar constancia de las operaciones realizadas.
- Mantener estadísticas actualizadas de la prestación de servicios a través de cada uno de los canales.
- Conservar todos los soportes y documentos donde se hayan establecido los compromisos.
- Llevar un registro de las consultas hechas por los funcionarios sobre los productos de los clientes.
- Disponer de un sistema de registro de operaciones: fecha, hora, cuentas, valor y costo para el cliente, equipo (IVR – Internet – Móvil)

# Obligaciones Generales: Divulgación de Información

- Concientizar (informar, capacitar, entrenar y formar) acerca de las medidas de seguridad que deberán tener en cuenta para la realización de operaciones por cada canal
- Expedir soporte en papel o por medios electrónicos.
- Informar a sus clientes y usuarios, previo a su realización, el valor de la operación, cuando ella tenga costo.
- Establecer las condiciones bajo las cuales los clientes podrán ser informados en línea, acerca de las operaciones realizadas con sus productos.
- Expedir paz y salvo por todo concepto, dentro del procedimiento de cancelación de un producto o servicio.

# Obligaciones adicionales por tipo de canal

Oficinas

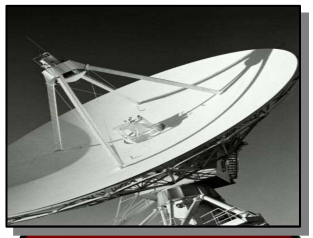
Cajeros automáticos

Datáfonos

Audiorespuesta

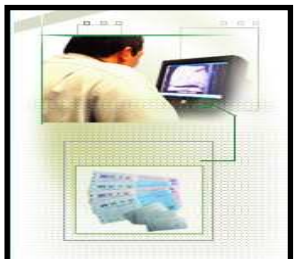
Call Center

Internet



Sistema de Acceso Remoto

Dispositivos móviles



Nuevos Canales

# Oficinas


- Los sistemas informáticos deben contar con soporte por parte del fabricante o proveedor y cumplir al menos con el nivel de seguridad C2 (protección de acceso controlado).
- Contar con Cámaras de Video grabación.
- Cifrado fuerte con los sitios centrales.
- Establecer procedimientos para atender de manera segura y eficiente a sus clientes en todo momento.

# Cajeros Automáticos

(ATM's)


- Sistemas de video grabación que asocien los datos y las imágenes de cada transacción.
- Cifrado fuerte con los sitios centrales.
- El lugar donde se instalen los cajeros automáticos deberá considerar las medidas de seguridad físicas para su operación y estar acorde con las especificaciones del fabricante
- Ocultar en los soportes de las operaciones la información confidencial, con excepción de los últimos cuatro (4) dígitos o caracteres.
- Implementar mecanismos de autenticación que permitan confirmar que el cajero es un equipo autorizado.
- Receptores de cheques: con módulo lector.
- Receptores de efectivo: con módulo lector.

# POS (punto de pago a través de datáfonos)


Datáfono

- El POS y el PIN Pad deberán ser a prueba de apertura.
- Cumplir los estándares
  - EMV (Europay, MasterCard, VISA).
  - PCI PED (Payment Card Industry PIN Entry Device).
- Validar automáticamente la autenticidad del datáfono, así como el medio de comunicación a través del cual operará.
- Establecer procedimientos que permitan identificar a los funcionarios autorizados para mantenimiento.
- Velar por que la información de los clientes no sea almacenada o retenida por el comercio.
- Contar con mecanismos que reduzcan la posibilidad de que terceros puedan ver la clave digitada.

# Sistemas de audio respuesta

(IVR)

Audiorespuesta

- Permitir la confirmación de la operaciones.
- Permitir transferir la llamada a un funcionario de la entidad.

# Centro de atención telefónica

(call center)


- Área dedicada exclusivamente.
- Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información.
- Dotar a los equipos de los elementos necesarios que impidan el uso de dispositivos almacenamiento.
- Equipos solo para la prestación de servicios por ese canal.
- No permitir la navegación por Internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información a menos que se cuente con un sistema de registro

# Sistemas de Acceso Remoto


Cifrado por hardware para el intercambio de información.

FIPS-140-2 (Federal Information Processing Standard),

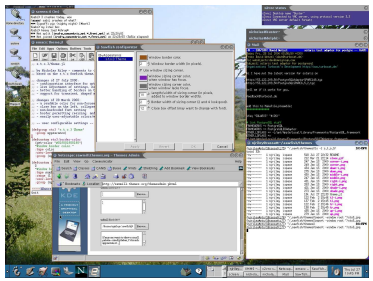
# Internet


- Implementar los algoritmos y protocolos de cifrado fuerte.
- Efectuar pruebas de vulnerabilidad y penetración.
- Adoptar mecanismos que reduzcan la posibilidad de capturar información.

# Nuevos canales


- Cumplimiento de las obligaciones generales.
- Análisis de los riesgos operativos → Junta Directiva y los órganos de control.
- Remitir a la SFC,45 días antes:
  - Procedimiento que se adoptará para la prestación del servicio.
  - Tecnología que utilizará.
  - Medidas de seguridad y controles adoptados.
  - Planes de contingencia.
  - Análisis de riesgos y medidas de tratamiento.
  - Plan de capacitación sobre uso y riesgos.

# Actualización de Software



- Mantener tres ambientes independientes.
- Ambientes de desarrollo y producción compatibles.
- Contar con procedimientos y controles para llevar el software a producción.
- Mantener actualizada la documentación del software, sus pruebas y los sistemas donde opera.

# Tarjetas débito y crédito

- Establecer y documentar los procedimientos de: emisión, transporte, recepción, custodia, entrega, devolución y destrucción.
- Cifrar la información de los clientes que sea remitida a los proveedores y fabricantes.
- Cuando la clave (PIN) haya sido asignada por la entidad vigilada, esta deberá ser cambiada en la primera operación.
- **Emitir tarjetas personalizadas.**
- Al momento de la entrega de la tarjeta a los clientes, ésta deberá estar inactiva.

# Análisis de Vulnerabilidad

- Estar basado en hardware de propósito específico (appliance).
- Generar de manera automática por lo menos dos veces al año un informe consolidado de las vulnerabilidades encontradas.
- Tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.
- Tomar como referencia la lista de nombres de vulnerabilidades CVE (*Common Vulnerabilitis and Exposures*).
- Tener en operación solo los protocolos, servicios, aplicaciones, usuarios y equipos necesarios para el desarrollo de su actividad.

# ¡ Gracias !