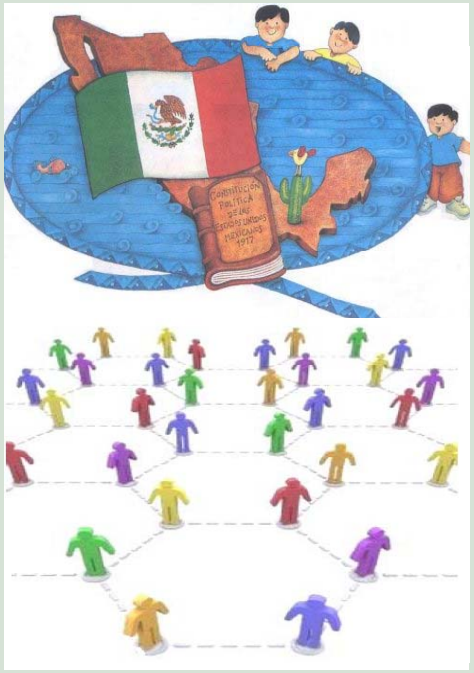
La Seguridad en la Banca y Comercio Electrónico

Ing. Benjamín Bernal Díaz, CNBV

México: Un Gran País



Población: 107.6 millones [1]

- 26.7 millones con acceso a Internet [2]

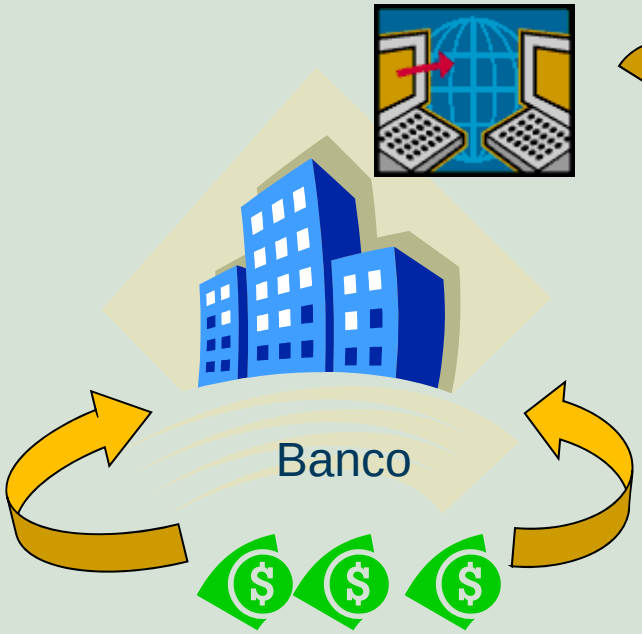
Economía: 11 lugar a nivel mundial [3]

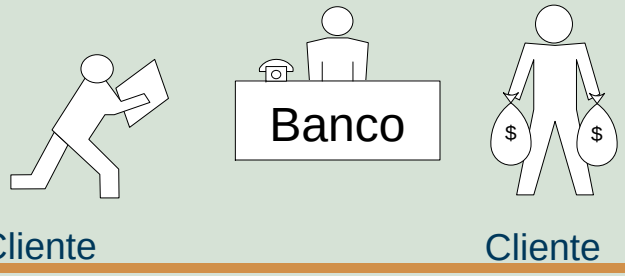
Infraestructura bancaria actual

- 42 Bancos
- Sucursales Bancarias: 10,487 [4]
- Cajeros Automáticos: 30,005 [4]
- Terminales Punto de Venta: 454,620 [5]
- 62 Millones de Tarjetas de Débito [6]
- 22 Millones de Tarjetas de Crédito [6]

Fuente: 1) INEGI (Instituto Nacional de Estadística y Geografía), 2009, 2)AMIPCI (Asociación Mexicana de Internet), 2009. 3)FMI. 4) CNBV, Junio 2009. 5) Banco de México, Marzo 2009, 6) Banco de México, Septiembre 2009

Servicios Banca Electrónica en Instituciones Financieras

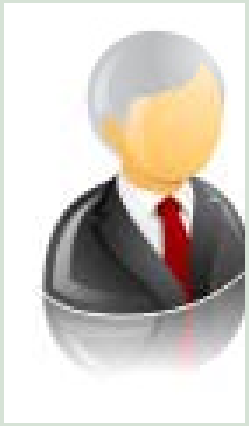




Consideraciones

- Recursos de los clientes
- La información es procesada electrónicamente
- Activos = Información = $$$

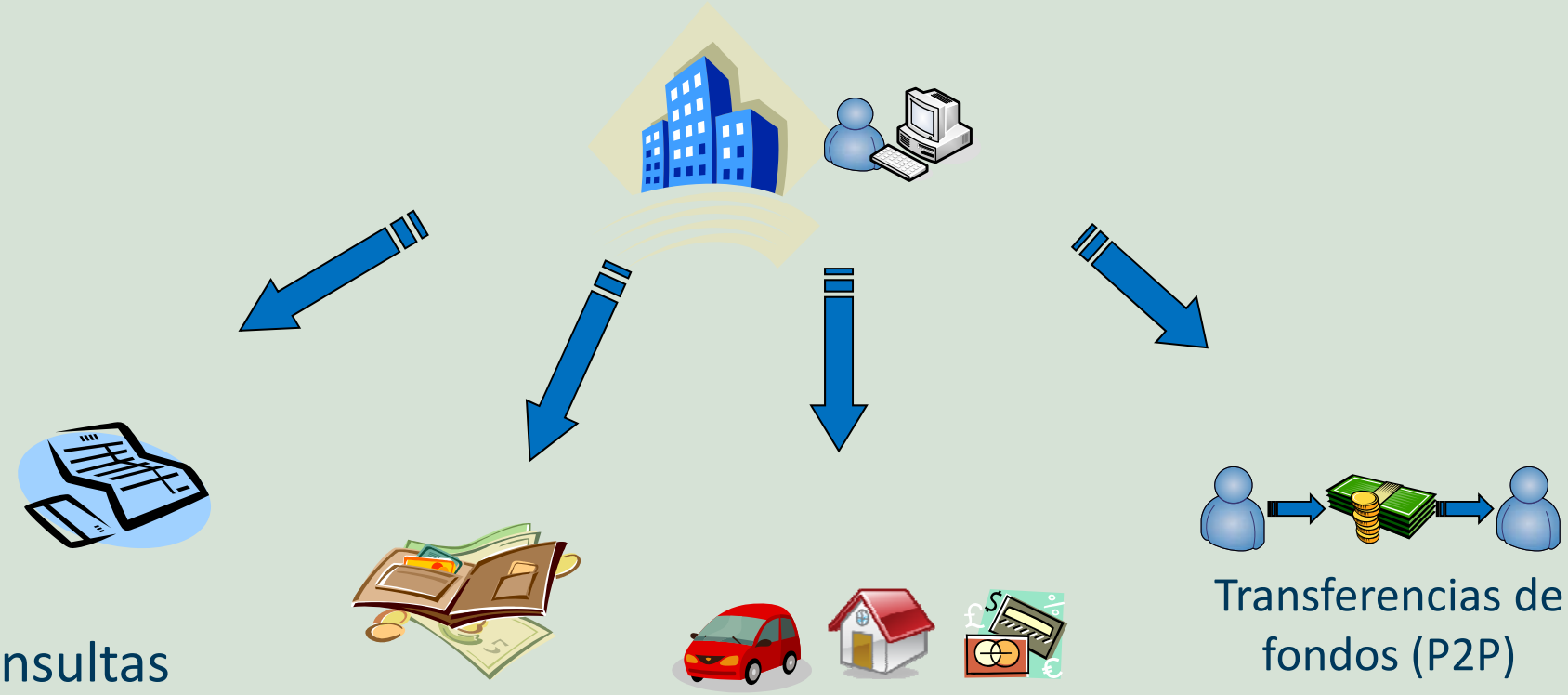
Banca Electrónica



Medios Electrónicos

Servicios y operaciones bancarias que las Instituciones realizan con sus Usuarios a través de Medios Electrónicos

Servicios de Banca por Internet



Consultas

Pagos

Solicitud de préstamos

Transferencias de fondos (P2P)

Banca por Internet y sus amenazas

- Incentivos altos
  - Monto que se puede operar
  - Anonimato
  - Facilidad (2003 -2006)

- Factores
  - Externos
  - Internos

Factores

- Robo de contraseñas
  - Keyloggers / Mouseloggers Registran y almacenan toda la información ingresada a través del teclado o los movimientos del *mouse*, incluyendo contraseñas
  - Phishing Envío de correo electrónico pidiendo información como si proviniera del Banco
  - Pharming Conduce al usuario a un sitio con el mismo nombre del original, pero ubicado en un servidor web puesto por el atacante
  - Spyware Al bajar o abrir un archivo, se instala un programa espía
  - Engaños (Ingeniería Socia)
- Controles débiles

Factores, cont.

Controles Débiles

Contratos no específicos

Alta de Servicio en línea

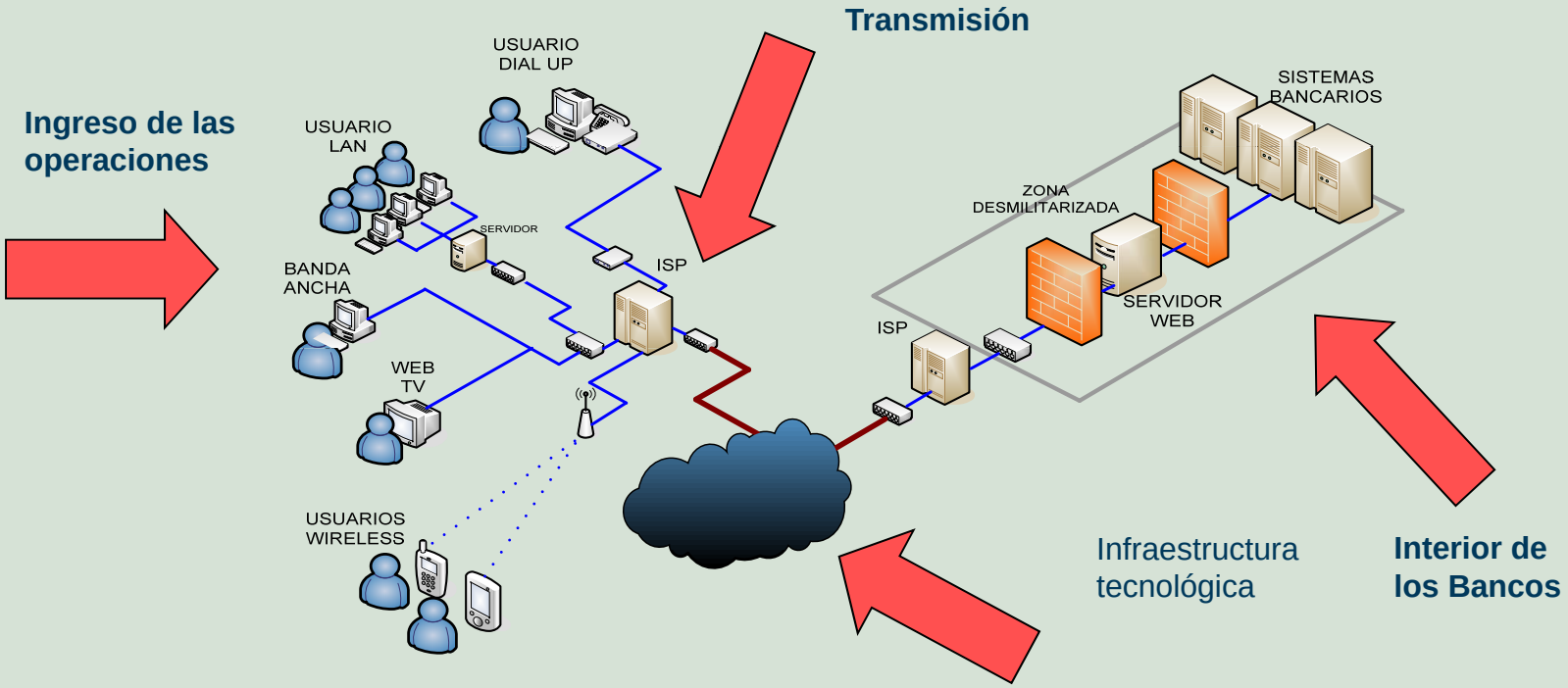
Admon. Contraseñas
Sin longitud mínima
"Débiles" (11111)

Una contraseña
+ Usuario =
Recursos

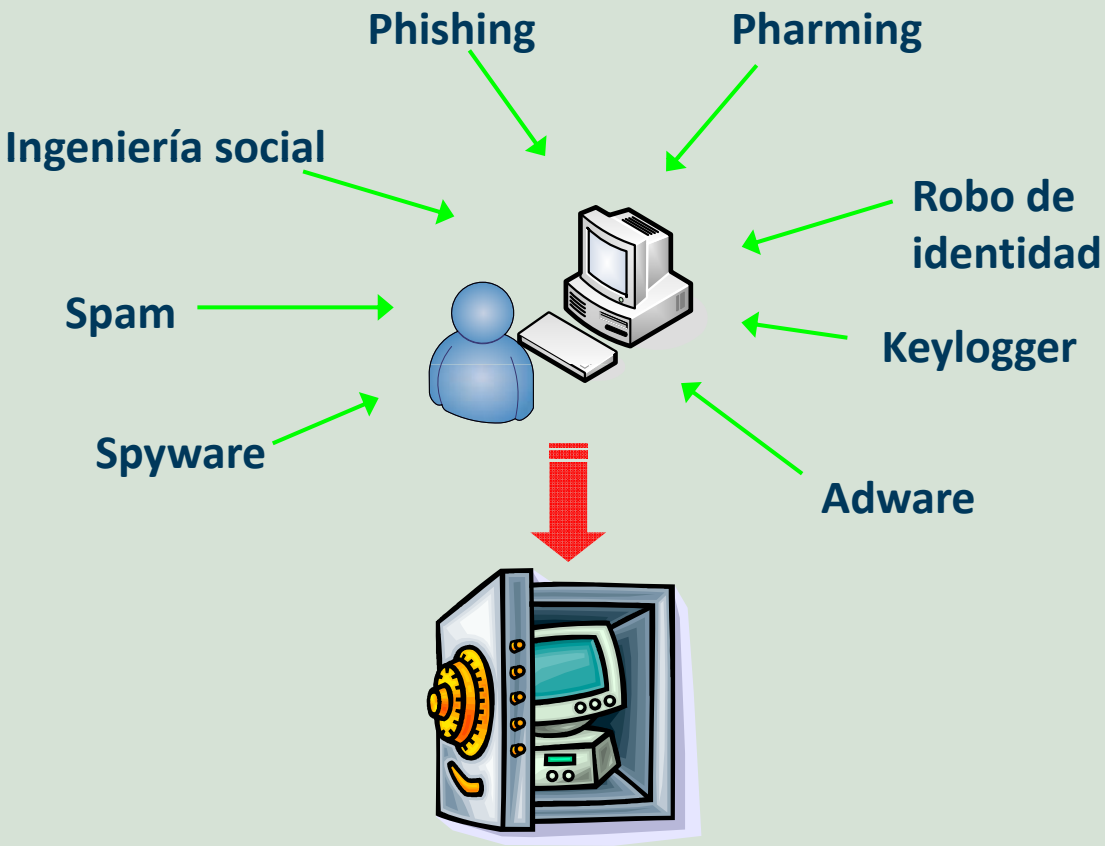
Falta de sistemas antifraude

Falta de información al Cliente (Capacitación)

Puntos de Control



Factores de Riesgo



Mitos

- "Internet no es seguro, la información esta expuesta"
- "Los bancos conocen mi contraseña"
- "Desconfío de Internet"
- "Internet es de muy alto riesgo"
- "Me da miedo que mi pago no pase, prefiero ir a la sucursal"

Realidades

- Los riesgos están asociados al manejo de la información (contraseñas y factores de autenticación)
- Existen controles regulatorios que los bancos han implantado ofreciendo servicios seguros
- El correcto uso de la tecnología y de controles operativos permite proporcionar servicios seguros
- “Eficiencia: Es como estar en dos lugares a la vez”

Banca por Internet y sus amenazas

Regulación: Circular Única de Bancos

- Uso de los Medios Electrónicos

  Versión vigente: Emitida en marzo de 2006

- Control Interno

- Administración de Riesgos

Controles Regulatorios

- Éxito en la implantación por parte de los bancos = “Servicio Seguro”
- Circular Única de Bancos (Capítulo X):

1) 2º Factor de autenticación 2) Registro de cuentas 3) Notificaciones 4) Límites de operación	**Clientes**
1) Prevención de fraudes 2) Registro de bitácoras 3) Seguridad: datos y comunicaciones	**Back-Office**
1) Contratos	**Aceptación del Cliente**

Dos Factores de Autenticación

- Para operaciones monetarias con terceros y otros bancos (pagos, transferencias, etc.)
  - Algo que el Usuario Sabe:
    - Identificador de Usuario + Contraseña
  - Algo que el Usuario Tiene:
    - Generador de contraseñas dinámicas (OTP)
  - Algo que el Usuario Sabe:
    - Huella digital

Uso del Segundo Factor de Autenticación

- Autenticación doble (Usuario-Sitio)
  - Ingreso de factores de autenticación (Usuario + Contraseña + Contraseña Dimánica)
    - Autenticar al usuario: “Bienvenido Usuario”
  - Validación del sitio
    - Información para autenticar al banco. (Próximo)

- Uso del Segundo Factor de Autenticación
  - Ingreso al servicio
  - Registro de cuentas destino
  - Establecimiento de límites
  - Transacción monetaria
  - Establecimiento / Cambio notificación de operaciones

Controles

- Registro de cuentas destino
  - ✓Monto, beneficiario, cuenta
  - ✓Tiempo para habilitar la cuenta (Próximo)
- Establecimiento de límites de operación
  - ✓Beneficiario, monto, fecha, frecuencia
- Notificaciones
  - ✓Establecer un medio para recibir notificaciones de operaciones y cambios en parámetros de operación

Seguridad de la Información

- Medidas de Seguridad para enviar, almacenar y procesar información de clientes y operaciones
  - ✓ Telecomunicaciones seguras con mecanismos de cifrado
  - ✓ Contraseñas y Factores de Autenticación con mecanismos de cifrado
  - ✓ Bitácoras de operaciones
- Revisiones periódicas de seguridad
- Sistemas de prevención de fraudes: comportamiento transaccional

Administración y Control de Contraseñas

- Proceso seguro para generar, entregar y desbloquear contraseñas
- Estructura de la Contraseña (características mínimas, datos no comunes)
- Bloqueo por inactividad
- Bloqueo por intentos fallidos
- Controles en el uso de *preguntas secretas*

Información a Clientes

- Información en el contrato respecto los riesgos en el uso de la banca electrónica
- Recomendaciones para prevenir y detectar fraudes
- Conformación de operaciones sobre transferencias, registro de cuentas, y modificación de información crítica
- Soporte técnico a Clientes
- Campañas sobre los riesgos, amenazas y uso de Banca por Internet

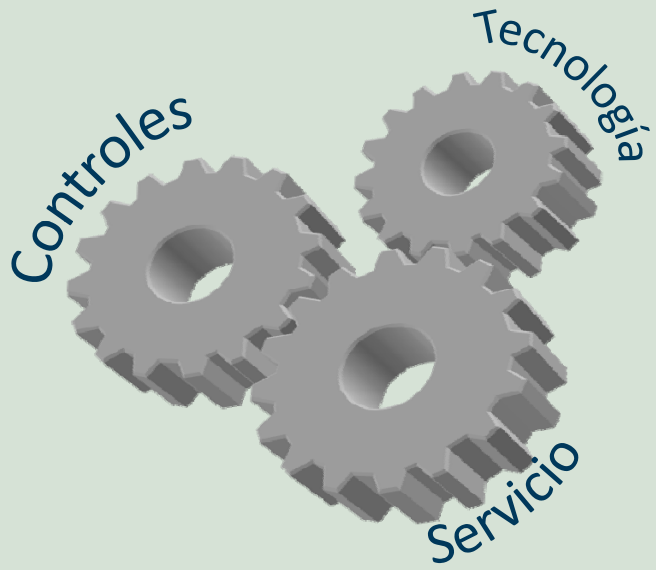
Factores de Éxito

- Implantación de controles no tecnológicos
  - Logística
  - Relación y conciencia con los clientes
- Controles funcionales
  - Uso
  - Bloqueo
  - Mecanismos preventivos
- Uso de Generadores Dinámicos Contraseñas (OTP)
  - Tiempo
  - Operaciones monetarias
  - Modificación de datos (límites, notificación de operaciones, recuperación de contraseñas)

Recomendaciones

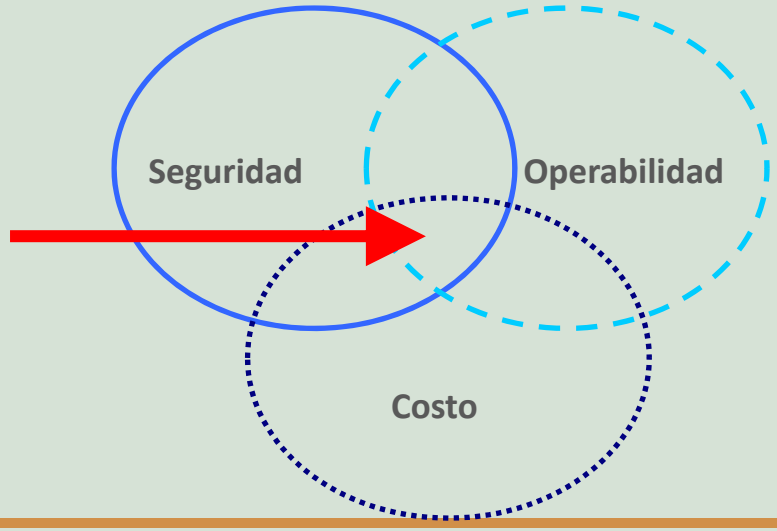
- Cuida los elementos de seguridad para ingresar a los servicios de banca por internet (tus contraseñas y tu segundo factor de autenticación)
  - **No proporcionar esta información a nadie**. **Los bancos NO la piden ni informan de actualizaciones por correo electrónico**
- Protege tu equipo de cómputo con herramientas de seguridad (antivirus, firewall, actualizaciones del sistema operativo)
- Cuando accedas al servicio identifica plenamente a tu Banco
  - Mensajes de bienvenida
  - Verifica tu información
- Ten actualizados los datos para que tu Banco pueda notificarte a cerca de accesos y transacciones que realizas a través de la Banca por Internet
- Identifica el número de atención a clientes de los servicios de banca por Internet de tu banco y reporta cualquier anomalía en el servicio

Retos para la Banca Electrónica



La tecnología no es suficiente para mantener la seguridad, se requiere de una adecuada implementación

Lo óptimo es llegar al balance:



Gracias...

Ing. Benjamín Bernal Díaz, CNBV
bbernal@cnbv.gob.mx