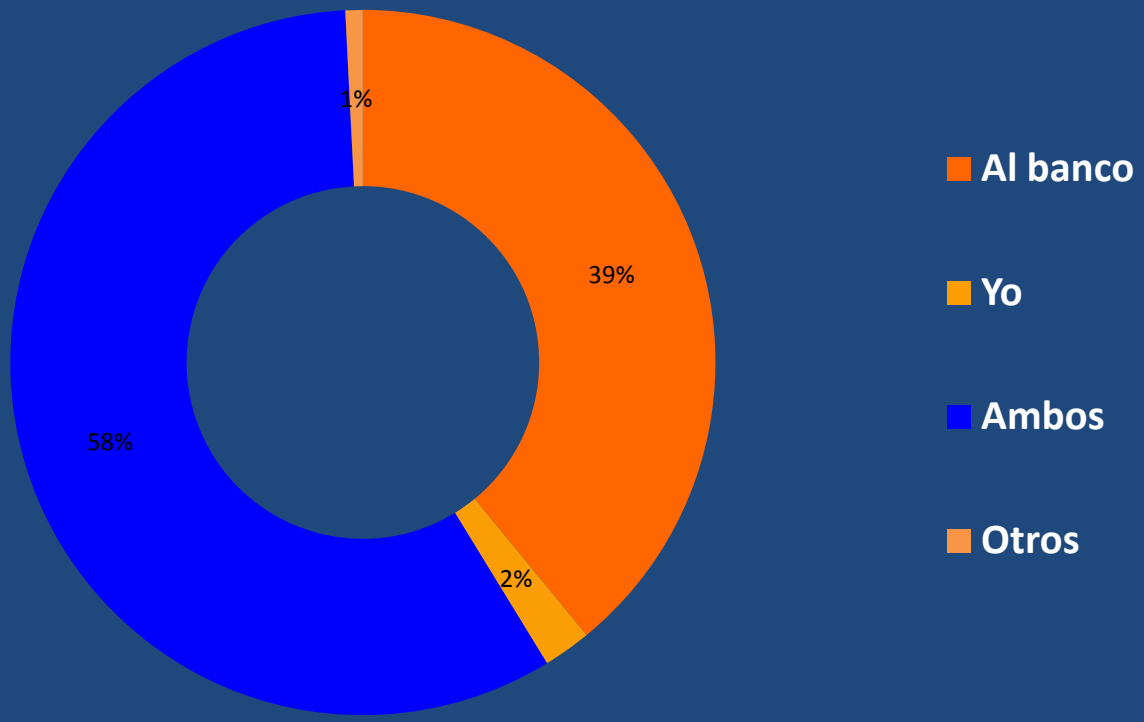
Algunos comentarios respecto de la regulación a aspectos técnicos de Seguridad en Internet

Dr. Alfredo Alejandro Reyes Krafft

39% Considera que los bancos son responsables de la seguridad

¿A quién consideras responsable de la seguridad de la banca por Internet?



NOTA: **En 2008 el usuario consideraba al banco en un 83% responsable de la seguridad de la banca por Internet.**

603 respuestas. Fuente :Encuesta en línea realizada por Elogia

Percepción vs Realidad

- 43% de los usuarios manifiestan que no compran en línea porque no confían en la seguridad de las transacciones (AMPCI 2006 Y 2007)

La tecnología no se *percibe* como segura

- 36% tiene miedo de proporcionar datos personales (AMIPCI 2005)
- Solo el 72% de los internautas son usuarios de servicios bancarios y de estos solo 12.5% usan banca *por internet* (AMIPCI 2008)
- El 95% de los usuarios de la banca por Internet la utilizan principalmente para consulta de saldos (AMIPCI 2008)
- El 39% de los usuarios de la banca por internet consideran como único responsable al Banco por su seguridad (AMIPCI 2008)

La Problemática

- La dificultad de proteger la información valiosa crece todos los días:
  - **SISTEMAS**
    - \+ FACILIDAD DE USO = − SEGURIDAD
    - \+ FUNCIONALIDAD = − SEGURIDAD
  - **REDES**
    - \+ COMPLEJAS = − SEGURAS
    - \+ FORMAS DE ACCESO = − SEGURAS

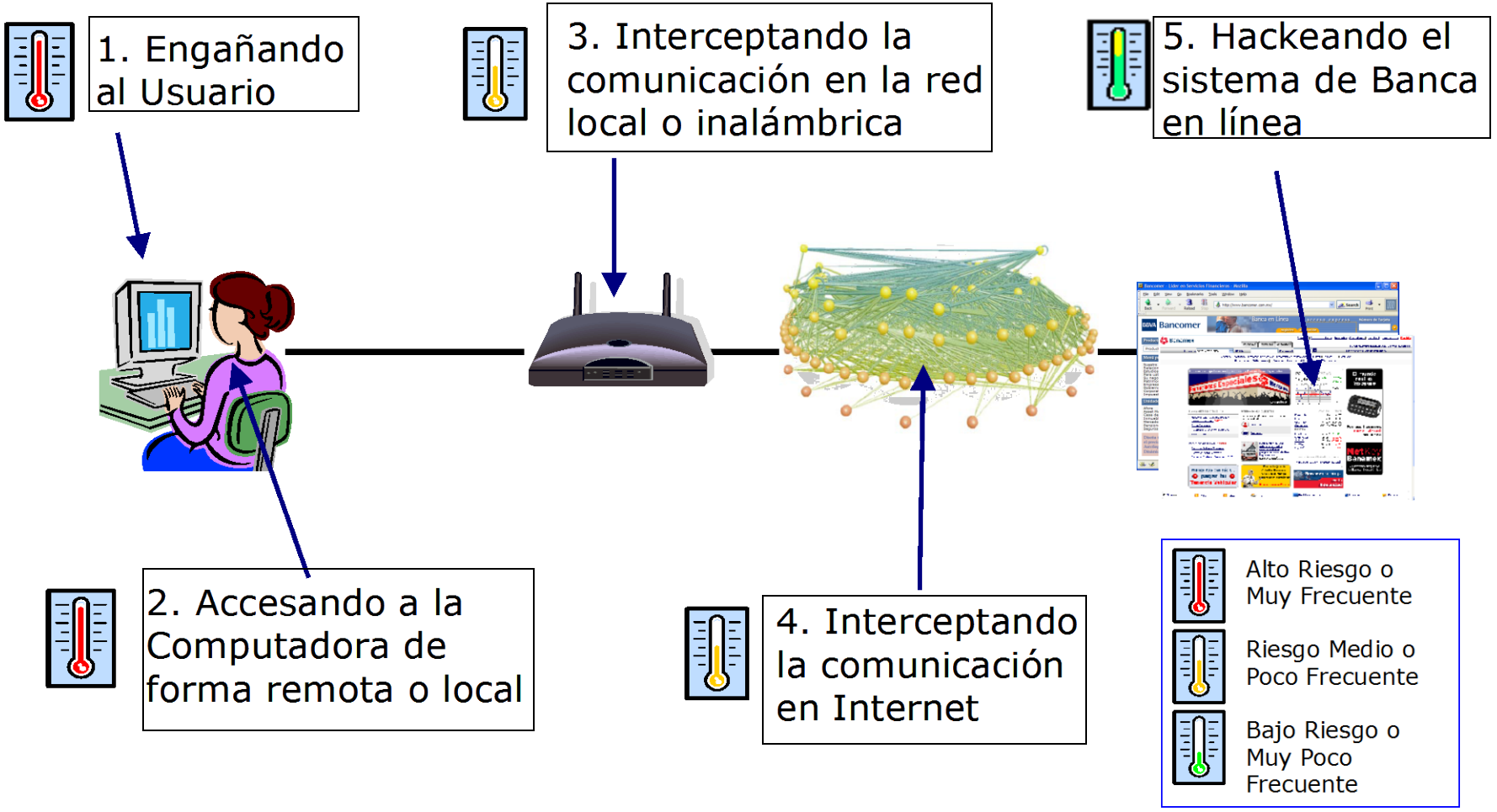
¿Cómo piensa un Atacante?

- **SIEMPRE** va a buscar el camino más fácil

- Formas de penetrar:
  1. Adivinando o descifrando contraseñas
  2. Explotando vulnerabilidades en el diseño o configuración de sistemas o equipos
  3. Interceptando comunicaciones
  4. Utilizando ingeniería social

  (casi siempre usan una combinación de las anteriores)

Puntos de Ataque



Aspecto Legal:

Un ejemplo, el capítulo X de la Circular Única Bancaria

Ley de Instituciones de Crédito

Artículo 52.- Los bancos pueden ofrecer servicios a sus clientes a través de medios electrónicos siempre que se establezcan en los contratos que celebren:

I. **“Las operaciones y servicios cuya prestación se pacte;**

II. **Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y**

III. **Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate”.**

El uso de esos medios de identificación, “**en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio**.”

La CNBV emitirá **reglas para la instalación y uso de esos medios electrónicos**

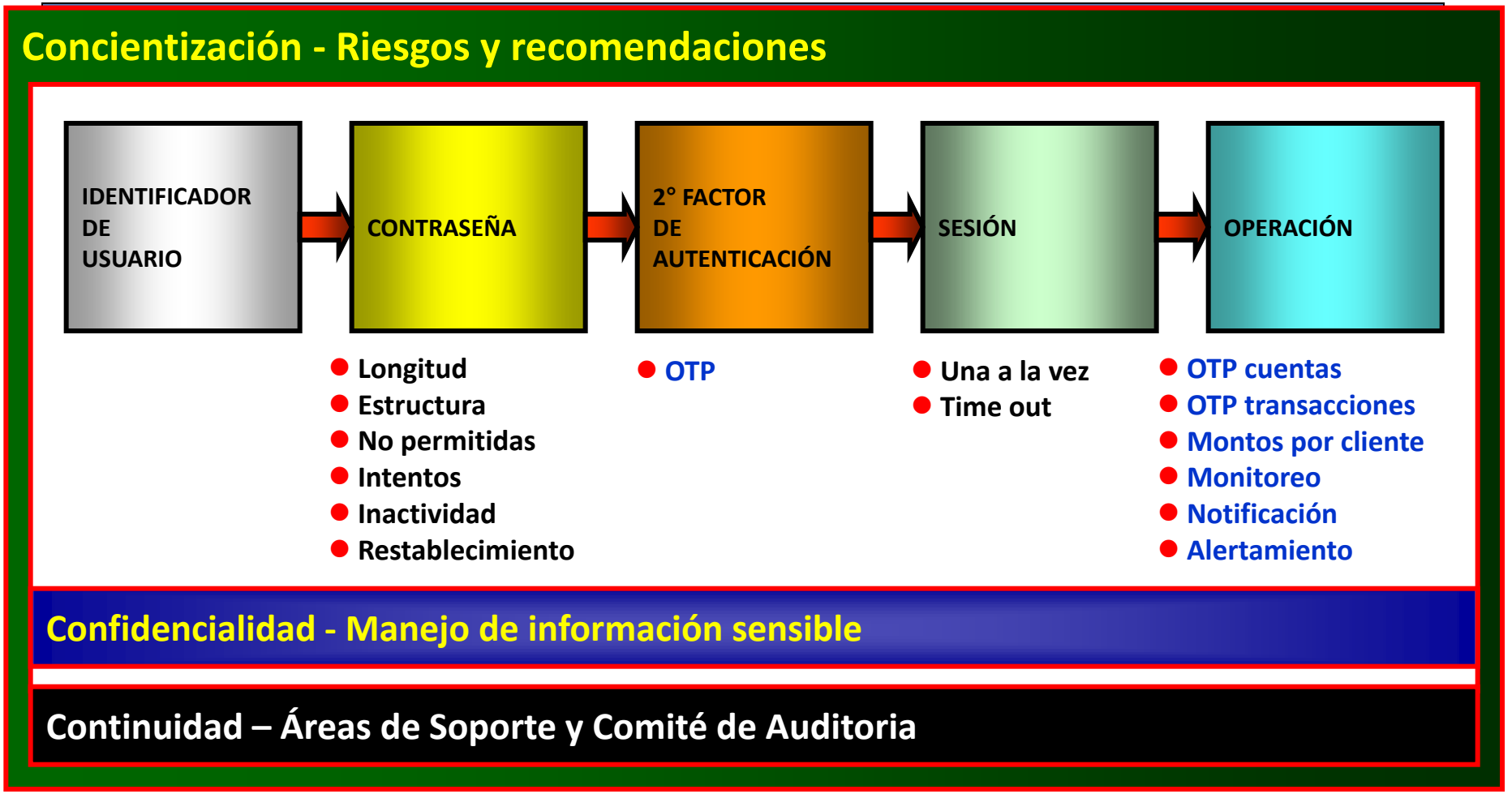
Reforma art. 52 LIC

(febrero 2008, DOF)

- Previo acuerdo con sus clientes, el Banco podrá "**suspender o cancelar el trámite de operaciones"** siempre que cuente con "**elementos suficientes** para presumir que los medios de identificación fueron utilizados en forma indebida" o detecten algún error.
- También restringir la disposición de los recursos (hasta por 15 días y 10 mas si se ve involucrada la autoridad correspondiente), en caso de que detecte probables hechos ilícitos cometidos en virtud de la operación respectiva.
- Todo lo anterior deberá ser **notificado al cliente** respectivo .

Medios Electrónicos

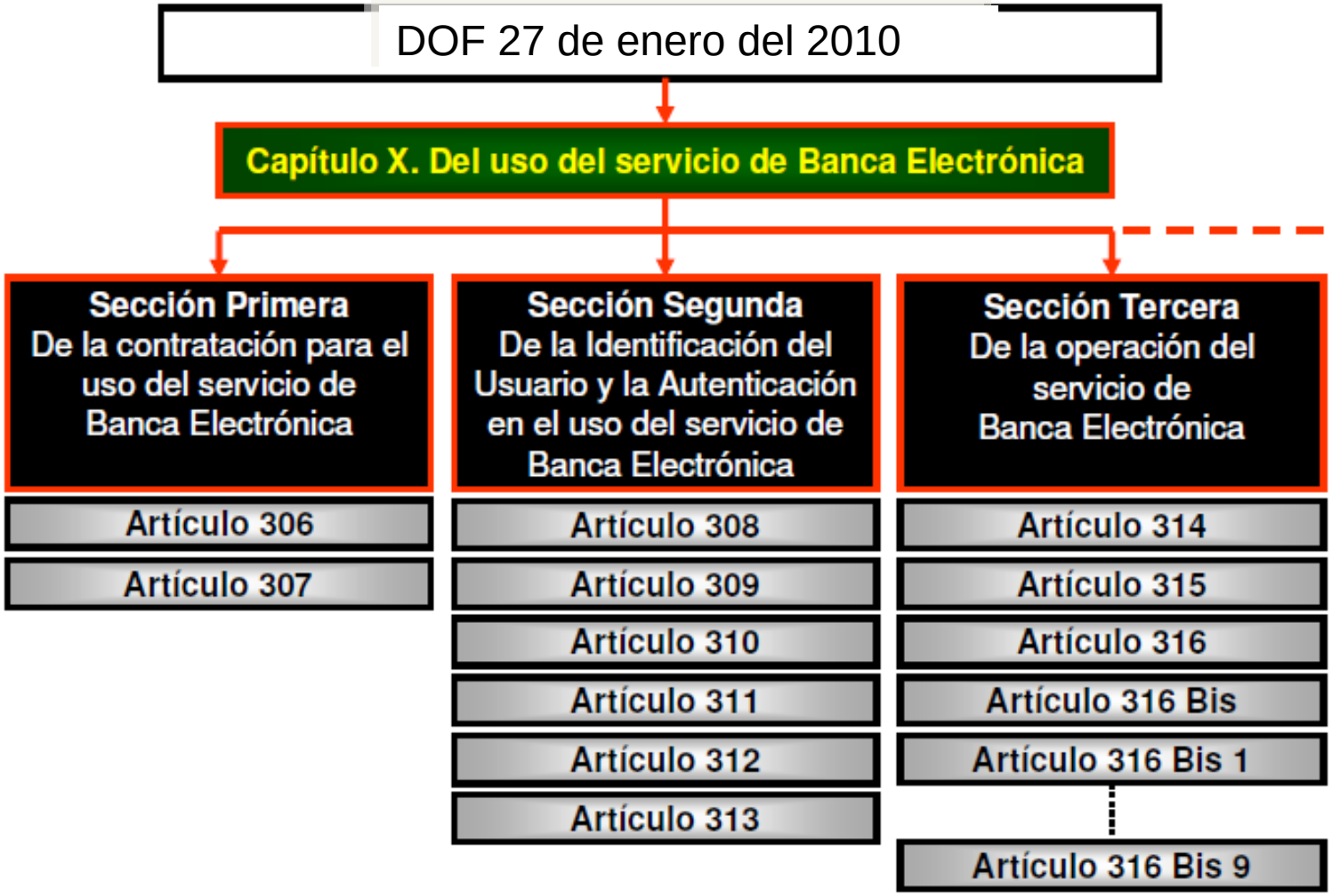
- *ESQUEMA CIRCULAR ÚNICA BANCARIA*



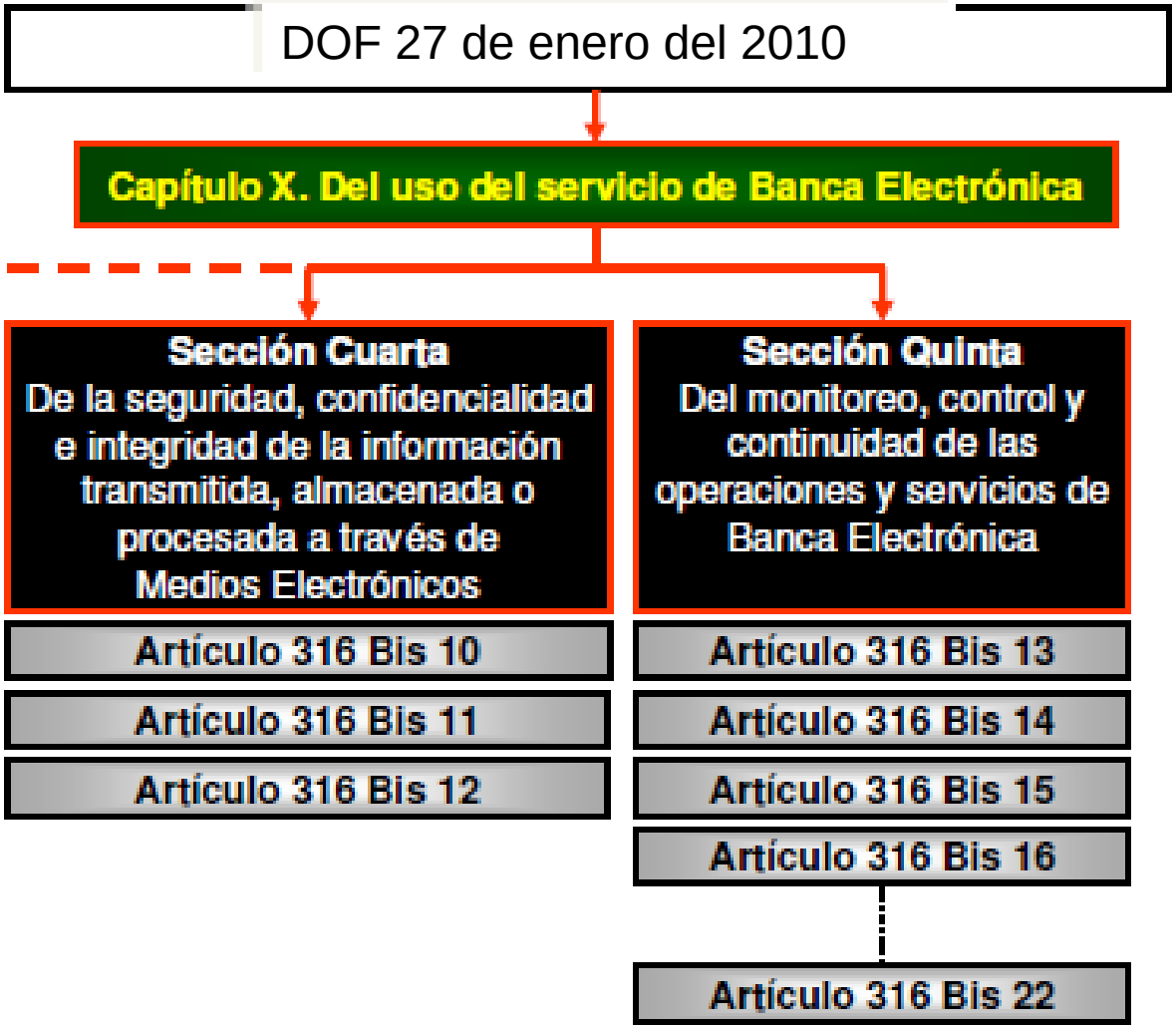
Circular Única Bancaria
ADMINISTRACIÓN DEL RIESGO TECNOLÓGICO

- **Evaluar la vulnerabilidad**
- **Controles internos:**
  - Mantener **políticas y procedimientos**
  - **Registros** de auditoria.
  - Niveles de **disponibilidad** y tiempos de respuesta
- **En canales:**
  - Asegurar **confidencialidad** en la generación, almacenamiento, transmisión y recepción de las claves de identificación y acceso.
  - Medidas de control que garanticen la **protección, seguridad y confidencialidad** de la información generada.
  - Políticas de operación, **autorización y acceso** a los sistemas, bases de datos y aplicaciones.
  - Medios adecuados para **respaldar** y, en su caso, **recuperar** la información.
  - Planes de **contingencia**,
  - Mecanismos para la identificación y resolución de:
    - **Fraudes**.
    - **Contingencias**
    - El **uso inadecuado** por parte de los usuarios,

CAPITULO X
ESTRUCTURA



CAPITULO X
ESTRUCTURA



CAPITULO X
DEFINICIONES

- Banca Electrónica: al conjunto de servicios y operaciones bancarias que las Instituciones realizan con sus Usuarios a través de Medios Electrónicos.

  → Servicios de Banca Electrónica:

  - Banca Host to Host
  - Banca Móvil
  - Banca por Internet
  - Banca Telefónica Audio Respuesta
  - Banca Telefónica Voz a Voz
  - Pago Móvil

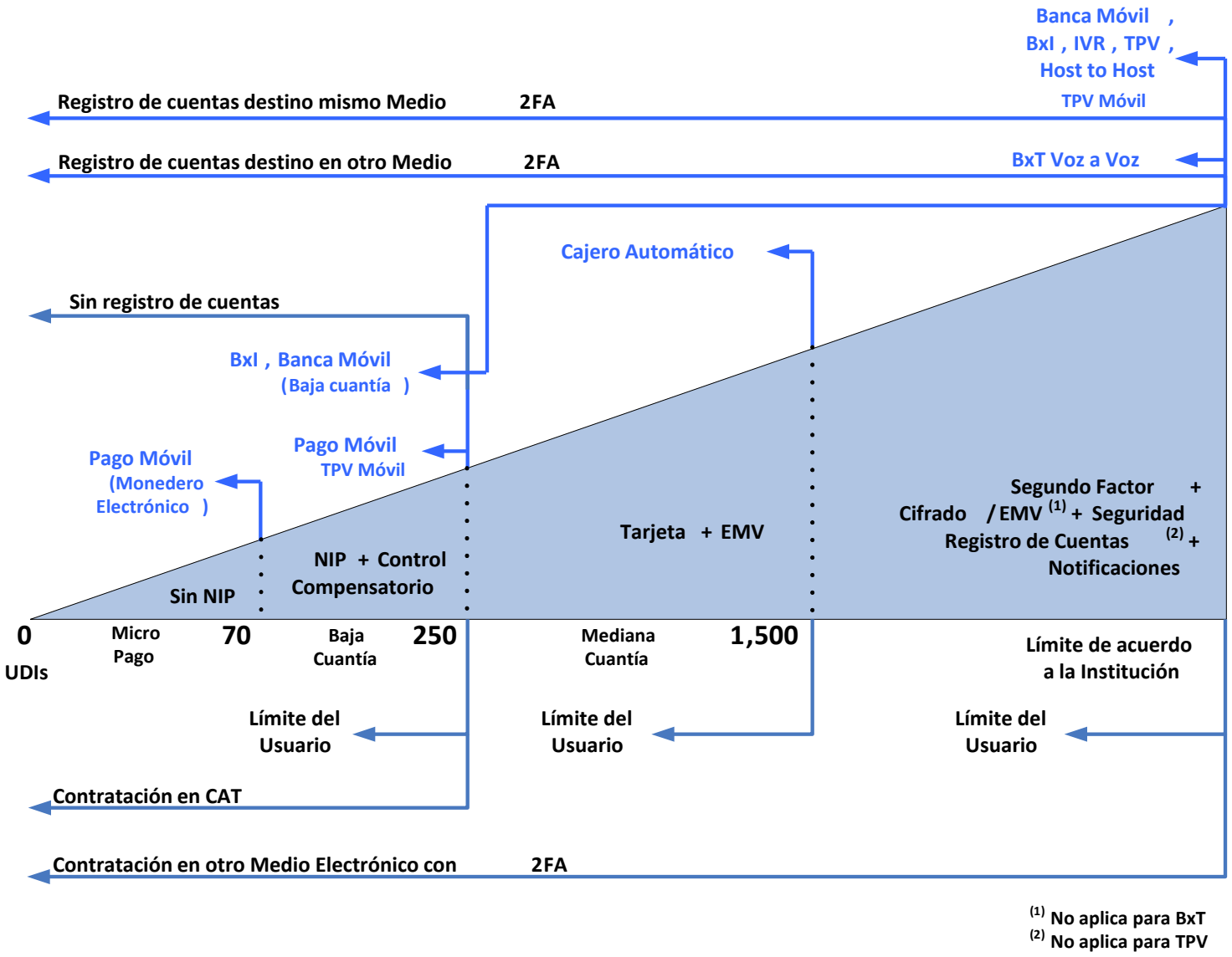
  → Dispositivos de Acceso:

  - Cajero Automático
  - Teléfono Móvil
  - Terminal Punto de Venta

CAPITULO X
MANEJO SIMPLIFICADO DEL RIESGO

- Considerando:
  - El Servicio de Banca Electronica o Dispositivo de Acceso
  - Las operaciones permitidas
  - El monto de la operación monetaria (en su caso, acumulados diarios y mensuales)
- Se determina el:
  - Identificador de Usuario
  - Factor de Autenticación
  - En su caso, el segundo Factor de Autenticación
  - Autenticación de la Institución por el Usuario

Controles de acuerdo al grado de riesgo



(1) No aplica para BxT
(2) No aplica para TPV

CAPITULO X
FLEXIBILIDAD

- Sin embargo, en algunos requerimientos la Comisión permite cierta flexibilidad, … pero

  → Las Instituciones que, en su caso, obtengan autorización de la Comisión para operar en forma diferente a lo establecido, asumirán los riesgos y por lo tanto los costos de las operaciones realizadas que no cumplan con lo previsto y que no sean reconocidas por los Usuarios. Las reclamaciones derivadas de estas operaciones deberán ser abonadas a los Usuarios a más tardar cuarenta y ocho horas posteriores a la reclamación.

¿La legislación orientada a mecanismos o herramientas de seguridad nos da “más” seguridad o nos la quita?

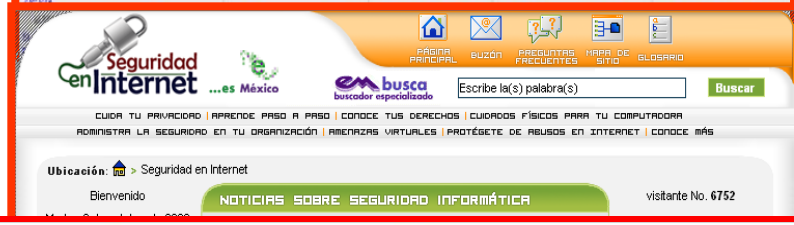
- Ladrón “invierte” en formas de ataque
- Estandarizar mecanismos de seguridad implica fomentar “uniformidad”
- Y por ende mas **RIESGO…**

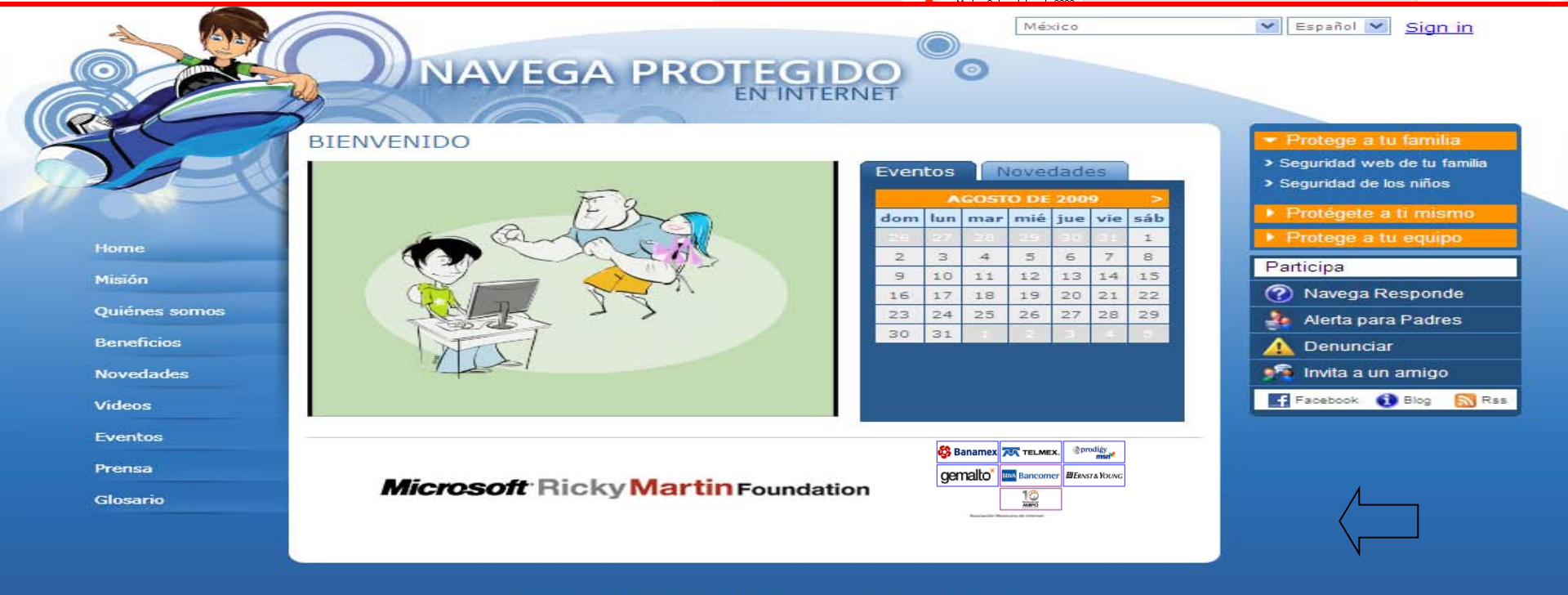
"Ni tanto que queme al santo... ni tan poco que no lo alumbre"

Medidas Adicionales

- Alertas sobre retiros o depósitos
- Software antiespía
- Mecanismos de cooperación interbancaria
- Redes neuronales (Monitoreo)

http://www.navegaprotegido.org.mx/
http://www.seguridad.unam.mx/usuario-casero/
http://www.eseguridad.gob.mx
http://asi-mexico.org





www.conectateseguro.org

Muchas Gracias

Dr. Alfredo A. Reyes Krafft

aareyes@krafft.mx