Fourth Annual Latin America Privacy & Cybersecurity Symposium

KPMG

OneTrust
Privacy Management Software

ICC MEXICO
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

iapp

EGADE Business School
Tecnológico de Monterrey

JONES DAY

DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE FINANCIAMIENTO COLECTIVO

PRINCIPIOS REGULACIÓN

- Adecuado **balance**

- Misma **actividad** mismos **riesgos**

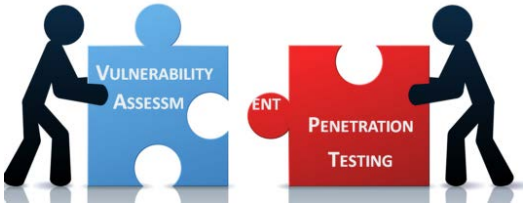
  mismo **estándar regulatorio**

- **Regulación diferenciada** *La CNBV y el Banco de México, para la regulación que les corresponda emitir, podrán considerar, además de las actividades que las ITF estén autorizadas a realizar conforme a lo previsto en esta Ley y diferenciar, cuando lo estime procedente, dicha regulación tomando en cuenta el número o monto de las Operaciones, el número de Clientes que tengan, modelos de negocios, activos intermediados o nivel de capital neto, entre otros*

JONES DAY

DISPOSICIONES DE CARÁCTER GENERAL APLICABLES A LAS INSTITUCIONES DE FINANCIAMIENTO COLECTIVO

RIESGOS



JONES DAY

Plan de Continuidad de Negocio

Debe permitir:

- La continuidad en la prestación de servicios y en la realización de procesos.
- El restablecimiento oportuno de operaciones.
- La mitigación de las afectaciones producto de dichas contingencias.

El plan de continuidad de negocio debe someterse a pruebas de funcionamiento y suficiencia, al menos anualmente, o antes si ocurre un cambio significativo que pueda afectar la estrategia de recuperación.

Requerimientos mínimos del Plan

- Desarrollar un análisis previo de impacto al negocio que considere, entre otros:
  - ➢ La totalidad de los servicios y procesos (incluyendo los críticos).
  - ➢ Los recursos mínimos necesarios (humanos, logísticos, materiales, etc.).
  - ➢ Los escenarios relevantes (desastres, sabotajes, ataques cibernéticos, etc.).
- Señalar los procesos que tendrán prioridad en la recuperación.
- Considerar acciones de prevención, contingencia, restauración y evaluación

Aviso a la CNBV aquellas que se presenten en cualquiera de los canales de atención al público o al interior de la propia ITF, cuando duren más de 30 minutos. Dentro de los 60 minutos notificar a la

cIberSeGuriDaD

Se implementarán **controles internos** que procuren garantizar la seguridad de la infraestructura tecnológica en que soportan las operaciones las IFC, a fin de procurar la confidencialidad, integridad y disponibilidad de su información.

Obligaciones del Director General:

- Implementar controles internos en la Infraestructura Tecnológica propia o provista por terceros.
- Pruebas de penetración (al menos dos al año) y vulnerabilidades (anual).
- Contar con registros de auditoría íntegros para monitorear la actividad de los usuarios de la infraestructura tecnológica.

Otras obligaciones:

- Realizar revisiones de seguridad para verificar los controles aplicables a la Infraestructura Tecnológica. (por lo menos una vez al año).

Definiciones clave:

- Evento de Seguridad de la Información: cualquier suceso que suponga una afectación a la seguridad de la información.
- Incidente de Seguridad de la Información: aquel evento de seguridad que se haya materializado y causado afectación.

Contar con una persona que, entre sus funciones, se desempeñe como **CISO** ***(Chief Information Security Officer)***. Principales funciones:

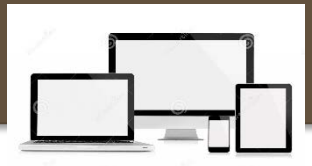
- Diseñar el Plan Director de Seguridad, que es aquel que establece la estrategia de seguridad a corto, mediano y largo plazo de la IFC.
- Implementar indicadores de riesgo en materia de seguridad de la información, a fin de monitorear los riesgos.

- Notificación de Eventos e Incidentes de Seguridad de la Información a la CNBV.
- Registro en bases de datos de los eventos de seguridad relevantes y de los Incidentes de seguridad de la información.

JONES DAY

Contenido:

- **Operaciones y servicios** que se pueden realizar.
- Mecanismos de **identificación y autenticación**.
- Términos y condiciones de uso.
- Celebración y **notificación** de operaciones.
- Atención de **aclaraciones**
- Mecanismos y procedimientos para **evitar el uso indebido.**



Autenticación del Cliente

- Se realiza con Factores de Autenticación, que pueden ser:
  - Contraseñas (al menos 6 caracteres alfanuméricos o especiales) o NIP.
  - Dispositivos generadores de contraseñas dinámicas de un solo uso (OTP).
  - Autenticación por métodos biométricos, previa autorización de la CNBV *¿por qué?*.
- Se puede solicitar a la CNBV la aprobación de algún otro tipo de FA, mostrando evidencia que la tecnología utilizada es de calidad igual o mejor que los FA ya definidos.
- La IFC deberá mantener procedimientos que garanticen la seguridad de la custodia, distribución, asignación y reposición de los FA.

Identificación de la IFC

- La IFC deberá establecer mecanismos y procedimientos para que sus clientes puedan verificar la autenticidad de la plataforma al iniciar sesión.
  - Ejemplo: Información que el cliente conozca o haya proporcionado a la IFC como nombre, alias, imágenes.
  - ***L****** M***** I*****

Sesión del cliente

- Para inicio de sesión, se requiere del identificador único (al menos 6 caracteres alfanuméricos o especiales) y un FA.
- La sesión inactiva expira a los 5 min.
- Si se detecta alguna modificación en los parámetros de la sesión, esta se termina de manera automática.
  - Ejemplo: Cambio de ubicación geográfica de forma inmediata.
- Solo se puede iniciar una sesión, por lo que se bloquea el inicio de sesión si se intenta iniciar sesión de manera simultánea desde otro dispositivo

Celebración y notificación de Operaciones

- Las operaciones como registro o modificación de cuentas destino y la instrucción para realizar compromisos de inversión, requieren un segundo FA distinto al utilizado para iniciar sesión.
- El cliente debe confirmar la operación y sus características, previo a que esta se ejecute.
- La IFC confirmará inmediatamente al cliente la realización de operaciones.

Atención de aclaraciones

- Para la operación de los centros de atención telefónica o canales electrónicos de mensajería ***(AI)***, la IFC deberá:
  - Mantener controles de seguridad física y lógica en su infraestructura tecnológica
  - Delimitar las funciones de los operadores sin que estos puedan registrar la información del cliente
  - Mantener bitácoras de accesos y actividades de los operadores.

JONES DAY