

# LEYES DEL SIGLO XX PARA DELITOS DEL SIGLO XXI:

Los desafíos de la  
regulación en la cibernética

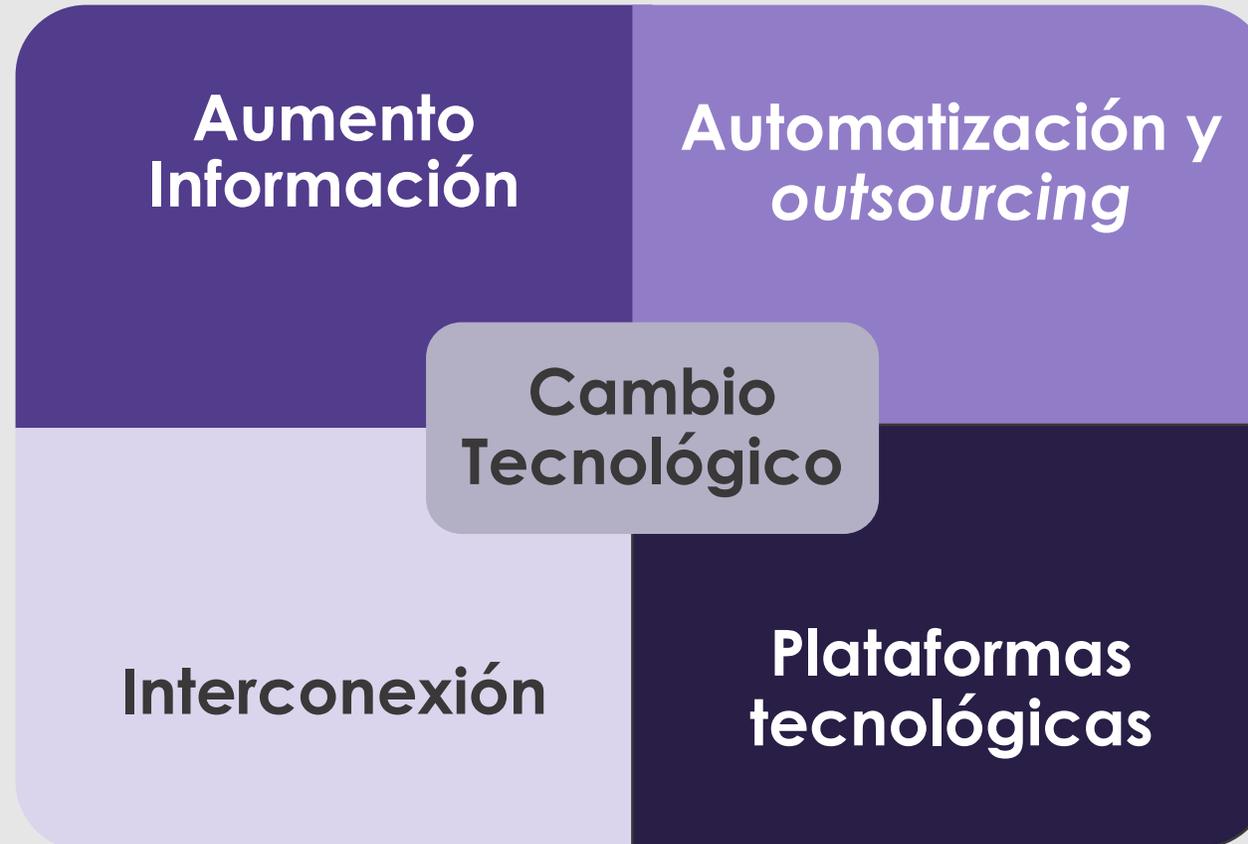
Kevin Cowan



COMISIÓN  
PARA EL MERCADO  
FINANCIERO



# Cambios tecnológicos (un desarrollo positivo) aumentan vulnerabilidad a ciberataques



La industria de seguros en Chile no ha sido ajena a estos desarrollos

# Aumenta el número y sofisticación de ciberataques

Incidentes de Ciberseguridad Corporativos Detectados a nivel global



Fuente: PWC, "Turnaround and Transformation in Cybersecurity, Key Findings from the The Global State of Information Survey"

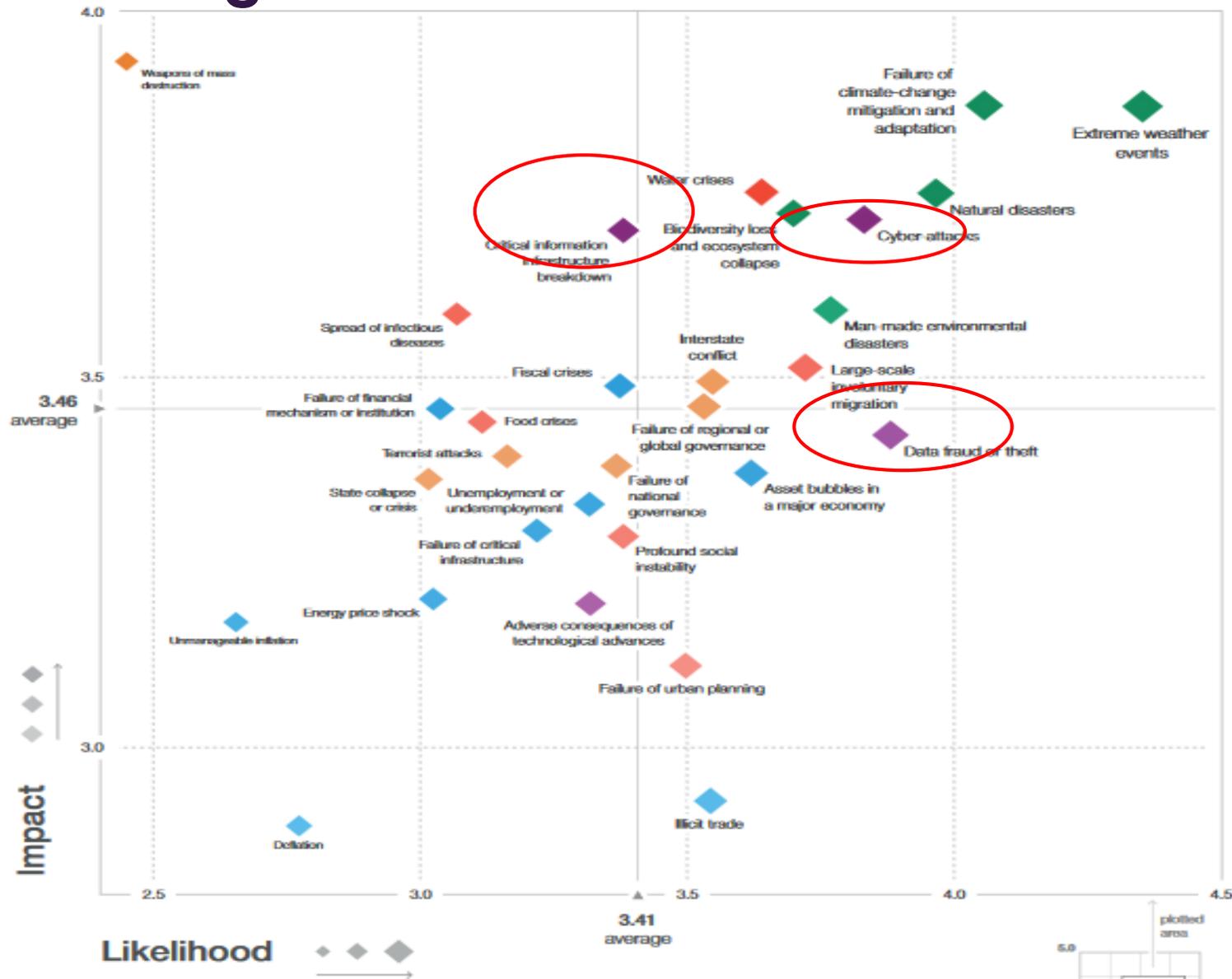
# La naturaleza de los ciberataques

## A nivel global....

- 1** Principal blanco dentro de la industria financiera son los bancos (90%). Compañías de Seguros son el segundo blanco (7%).
- 2** Un 43% son fraudes, seguidos por violaciones de datos (34%), interrupciones servicio (23%).
- 3** Tamaño pérdidas no está correlacionado con tamaño institución, y vulnerabilidad mayor en empresas menor tamaño.
- 4** 260 millones de registros violados en instituciones financieras en periodo 2015-17.

# Los riesgos Ciber se ha instalado como uno de los principales riesgos

Fuente: "The Global Risk Landscape", WEF, enero 2019.



# Los Principales Fuentes de Riesgos en la Industria de Seguros

## Activos Información

- Datos clientes
- Datos propios

## Continuidad servicio

- Pago RRVV + siniestros
- Gestión de seguros

## Integridad de los sistemas

- Pagos
- Activos financieros

Estos riesgos han llevado a que este sea un tema de máxima relevancia en las discusiones de la IAIS: Encuesta KIRT 2017 y *Issues Paper on Cyber Risk to the Insurance Paper (2016)*.

# El riesgo cibernético y la ciberseguridad son componentes claves del riesgo operacional.

- La identificación y mitigación de las fuentes de riesgo operacional es una pieza central de la regulación y supervisión prudencial en general, y de la industria de seguros en particular.
- IAIS - ICP 8.1.3: “El sistema de gestión de riesgos debe cubrir al menos la suscripción y las reservas, la gestión de activos y pasivos, las inversiones, la gestión de riesgos de liquidez y concentración, la gestión de riesgos operacionales, la conducción de negocios y el reaseguro y otras técnicas de reducción de riesgos.”

# Sin embargo, hay características que hacen importante un tratamiento diferenciado y detallado de la ciberseguridad

- **Tendencia:** Creciente relevancia y ampliación puntos de entrada de ataques.
- **Intencionalidad:** de extraer recursos o hacer daño
- **Evolución:** no es estático => importancia de compartir información
- **Posibles efectos en sistema:**
  - Interconexión
  - Proveedores comunes

# Dada su relevancia y especificidad los *standard setters* han desarrollado guías o principios específicos

- **G-7:** Fundamental Elements of Cybersecurity for the Financial Sector ('G7FE'), October 2016.
- **IAIS:** Application Paper on Supervision of Insurer Cybersecurity, November 2018.
- **IOSCO:** Guidance on cyber resilience for financial market infrastructures, June 2016.
- **FSB:** Cyber-resilience: Range of practices, December 2018,

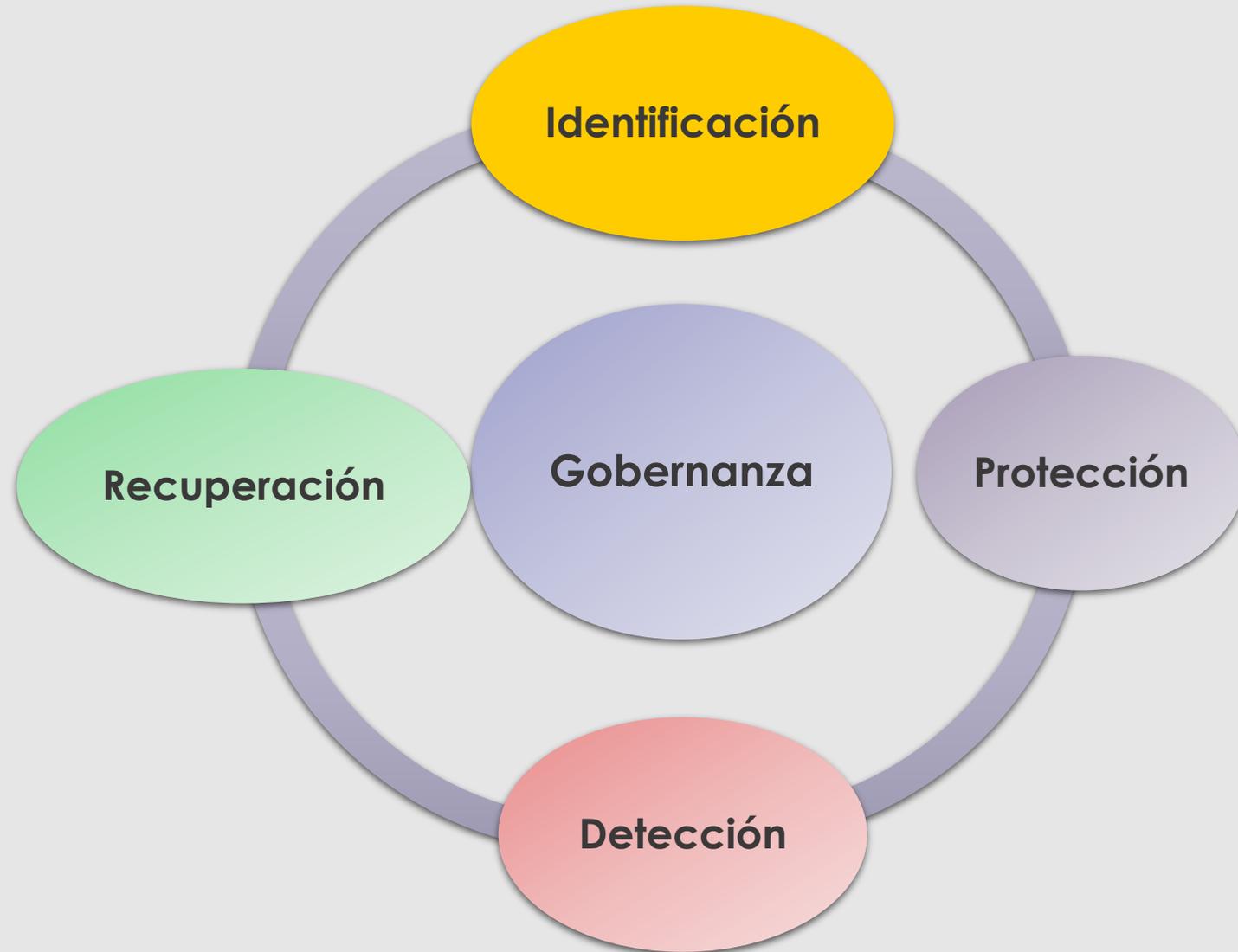
# Estos Enfoques Comparten Los Siguietes Elementos



# Estos Enfoques Comparten Los Siguietes Elementos



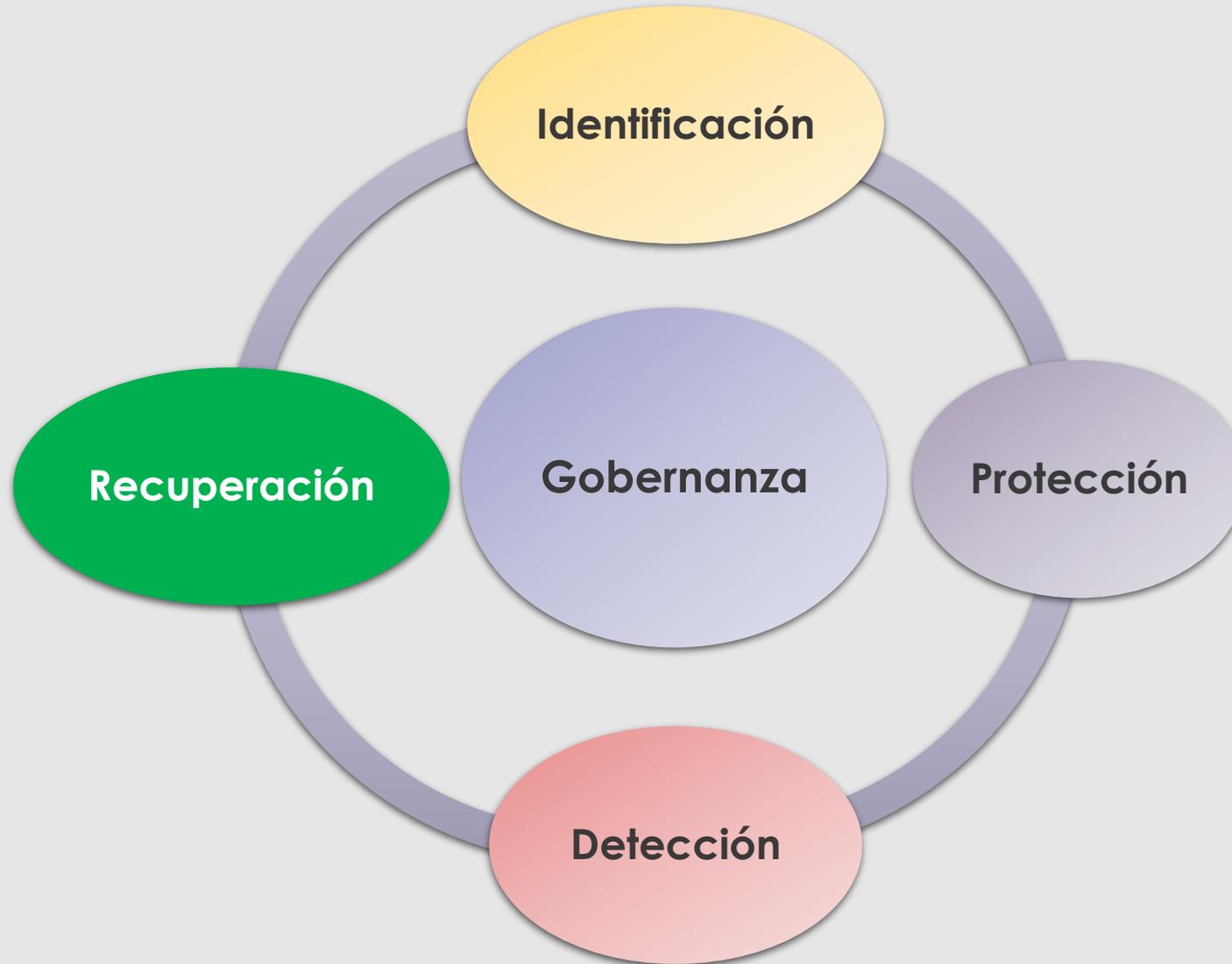
# Estos Enfoques Comparten Los Siguietes Elementos



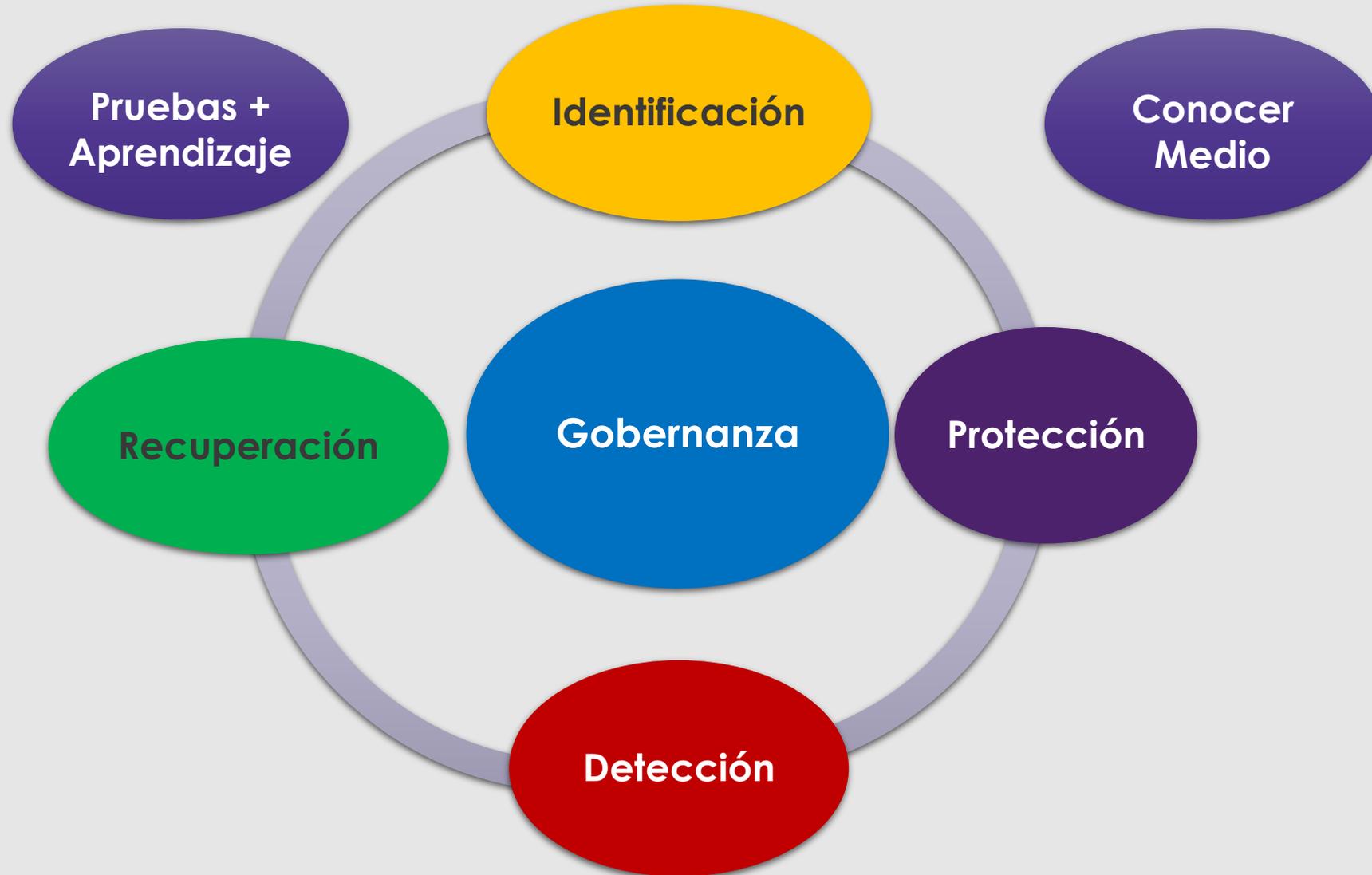
# Estos Enfoques Comparten Los Siguietes Elementos



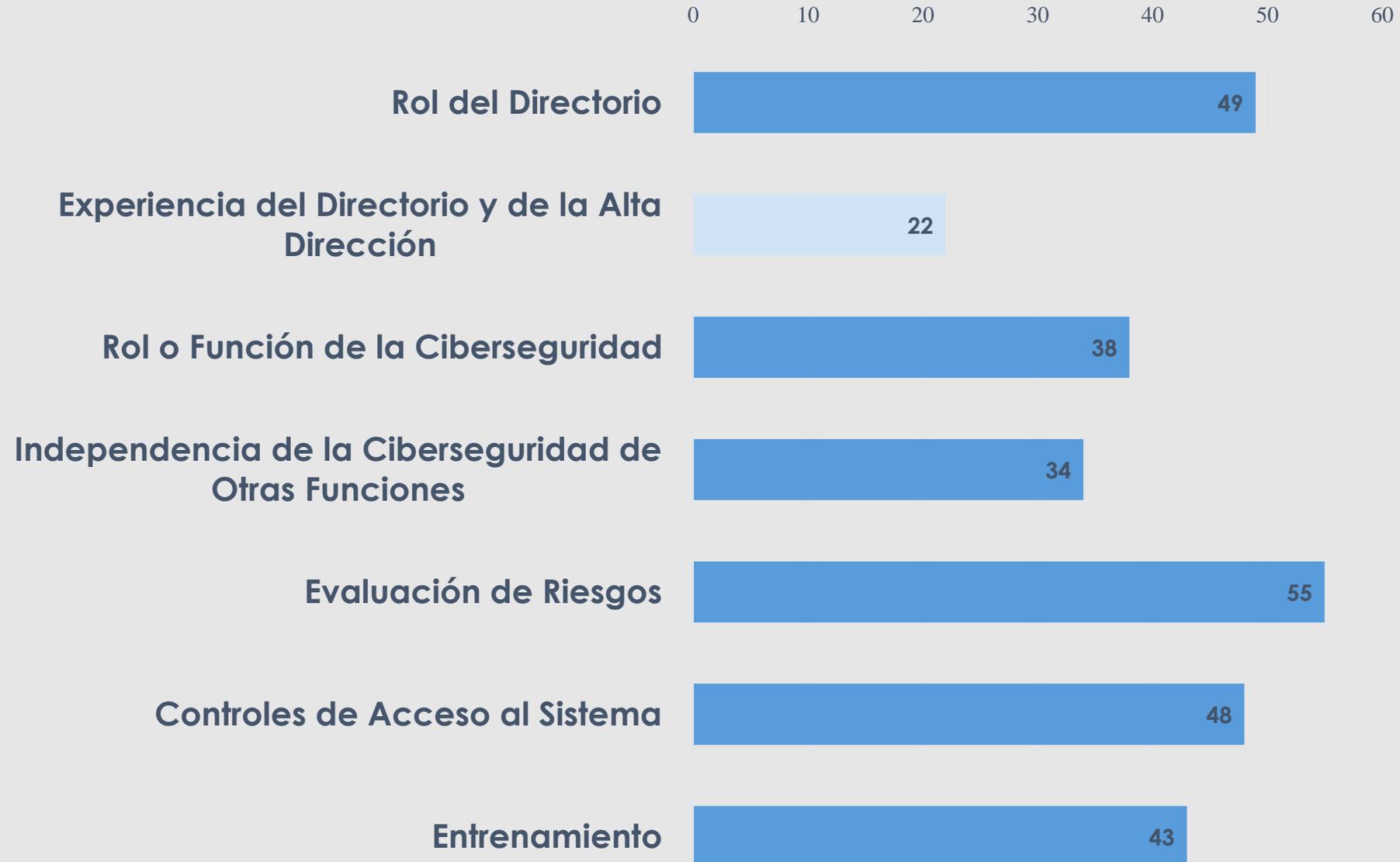
# Estos Enfoques Comparten Los Siguietes Elementos



# Estos Enfoques Comparten Los Siguietes Elementos



# ¿Como han ido avanzando países específicos?



# ¿Como han ido avanzando países específicos?



# Mercado asegurador Chile: ¿Cómo anda la ciberseguridad?

- Amplia diversidad de estándares en la industria.
- Una brecha relevante: involucramiento del directorio, en particular en algunas instituciones miembros de grupos internacionales.

## Inversión en Ciberseguridad 2018

	Primas	Utilidad	Inversión Ciberseguridad		
	MM\$		MM\$	% Primas	% Utilidad
CSV	6.125.174	422.886	5.578	0,09	1,36
CSG	2.274.434	93.056	3.358	0,15	3,61
Total	8.397.608	515.942	9.116	0,11	1,77

# Regulación y Supervisión de Chile

En la actualidad el tema de Ciberseguridad se norma y supervisa en el contexto del Riesgo Operacional (NCG 325 y 309).

## Consultoría Especializada

- Insumos para supervisión y regulación
- Septiembre 2019

## Norma Riesgo Operacional

- Ciberseguridad + *Outsourcing*
- mejores prácticas internacionales (IAIS, OSFI, APRA, etc...)

## Reforzamiento CMF

- Capacitación
- Revisión estructuras

**Es un ámbito donde el corto plazo se van a provechar sinergias y ventajas comparativas en fusión SBIF/CMF.**

# Relevancia Proyecto de Ley para Riesgos Operacionales y Ciberseguridad

- En línea con los estándares internacionales (ICPs de IAIS) el proyecto de Ley fortalece la capacidad de la CMF para regular y supervisar el riesgo operacional, incluyendo la Ciberseguridad.
- Mayores facultades para establecer estándares vinculantes de gestión de riesgo de la compañía.
- Requerimiento de capital para riesgo operacional.
- Facultad de la CMF para imponer requerimientos patrimoniales adicionales en aquellos caso donde el proceso de supervisión detecte riesgos residuales relevantes (Pilar 2).

# En ciberseguridad es crucial un enfoque coordinado

- **CEF:** Grupo de trabajo Riesgo Operacional
  - Prioridad: infraestructuras de mercado
  - Intercambio de información
  - Ámbito de coordinación en la regulación y supervisión
  - Misión FMI
- **Trabajo CMF en valores:** fortalecimiento equipo supervisión, estándares PFMI, consultoría BID.
- **Integración CMF/SBIF:** compartir experiencias, conocimiento y coordinación
  - SBIF ha emitido normativa con la obligación de informar al regulador los incidentes operacionales relevantes, y el mantener una base de incidentes en este ámbito.
- **Ley de Ciberseguridad.**

# La industria de seguros puede jugar un rol relevante mitigando y gestionando ciberseguridad

- El aumento del riesgo de ciberataques ha llevado a un mayor desarrollo de productos de seguros especializados, complementado coberturas en pólizas “tradicionales”
- A pesar de ser un mercado aún pequeño (2.5 billones vs 277 billones de prima en seguro de propiedades globalmente) está creciendo a 25% al año (OECD 2017).
- En Chile se ve un patrón similar: componente de seguros de fidelidad e incipiente como producto individual, con un importante rol de reaseguros.
- Más allá del rol de transferencia de riesgos, la industria puede jugar un rol importante en la gestión de riesgos
  - Identificación ex ante
  - Incentivos de gestión por precio
  - Respuesta especializada

## ...pero hay importantes desafíos para este rol

- Riesgos nuevos y dinámicos, con datos limitados.
- Acceso a información de las empresas para *underwriting*.
- Acumulación de riesgos.
  - Software común
  - Proveedor TI común
- Capacidad técnica compañías.
- De la mano de la conciencia de riesgos en la empresa.
- Conducta de mercado: adecuado entendimiento pólizas y conceptos de ciberseguridad (*trato justo*).

# Mensajes Finales

- Dada la naturaleza del negocio y los cambios tecnológicos, los riesgos cibernéticos son una amenaza creciente para el sistema financiero en general, y las compañías de seguro en particular.
- Esta amenaza engloba efectos negativos tanto sobre las compañías como sobre sus clientes, que confían a las instituciones datos y recursos.
- Para la CMF este es un tema prioritario.
- La CMF está trabajando en reforzar el marco normativo y en su capacidad de supervisión de ciberseguridad, en forma coordinada con otros entes supervisores y siguiendo mejores prácticas globales.
- La ley de SBR/CBR reforzará esta capacidad de supervisión.

# Mensajes Finales

- Más allá del marco de regulación y supervisión, es prioritario un involucramiento de los Directorios y la alta administración (*tone from the top*) en identificar y gestionar apropiadamente los riesgos cibernéticos, así como las respuesta a los eventos.
- Lo anterior requiere un esfuerzo individual, pero también se requiere una coordinación a nivel de industria en especial en el intercambio de información.
- La industria de seguros puede jugar un rol valioso no solo en cubrir riesgos cibernéticos, sino que en apoyar a empresas a identificar, mitigar y gestionar estos riesgos.
- Sin embargo este rol trae múltiples desafíos tanto en abordar el riesgo técnico como las definiciones de conducta de mercado.

# LEYES DEL SIGLO XX PARA DELITOS DEL SIGLO XXI:

Los desafíos de la  
regulación en la cibernética

Kevin Cowan



COMISIÓN  
PARA EL MERCADO  
FINANCIERO

