

---

# Proyecto implementación CAT- FFIEC

Cristian Guerra Bahamondes

**Disclaimer:** El contenido y los datos mostrados en esta presentación han sido modificados por motivos de confidencialidad, las opiniones de esta presentación no representan a la Corporación BCI y están expresadas por el autor con un objeto de educación.



# Índice

---

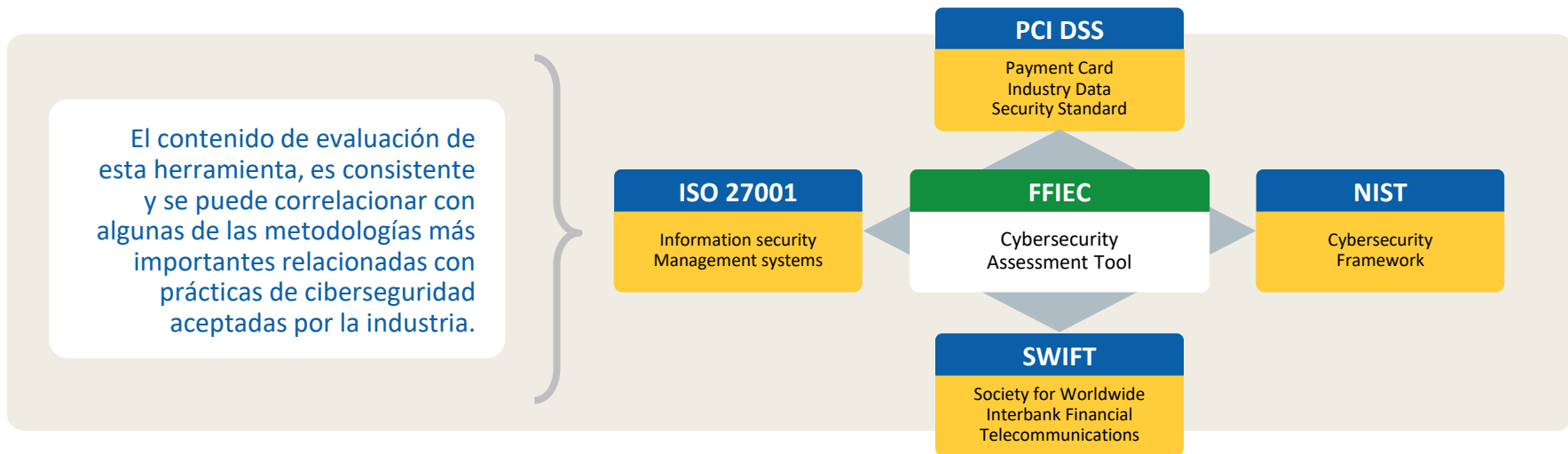
- 1.- Qué es CAT-FFIEC y cuándo nace
- 2.- Participantes del modelo y versiones
- 3.- De qué está compuesto
- 4.- Aplicación a la Banca
- 5.- Beneficios y lecciones aprendidas

# Qué es CAT- FFIEC y cuándo nace...



Corresponde al **Consejo Federal de Examinación de las Instituciones Financieras** (Federal Financial Institutions Examination Council) el cual es **un órgano interinstitucional del gobierno de los Estados Unidos**.

En junio del año **2015** nace el Cat FFIEC (Cybersecurity Assessment Tool) como una herramienta de evaluación de ciberseguridad, recomendada por FFIEC, para las instituciones financieras que están bajo su fiscalización en Estados Unidos. Su objetivo principal es ayudar a las instituciones financieras a identificar sus riesgos y determinar su preparación en materias de ciberseguridad.



# Participantes del modelo y versiones

## Las instituciones que conforman FFIEC son:



Junta de Gobernadores del Sistema de la Reserva Federal (FRB)



Corporación Federal de Seguro de Depósitos (FDIC)



Administración Nacional de Cooperativas de Crédito (NCUA)



Oficina del Contralor de la Moneda (OCC)



Oficina de Protección Financiera del Consumidor (CFPB)

**1ra. Versión  
Junio 2015**

**2da. Versión  
Mayo 2017**



# De qué está compuesto el CAT- FFIEC



Está conformado **por 5 (cinco) dominios**, los cuales, a su vez poseen diferentes tipos de **controles (494 controles)** orientados a dar seguridad razonable a las organizaciones.

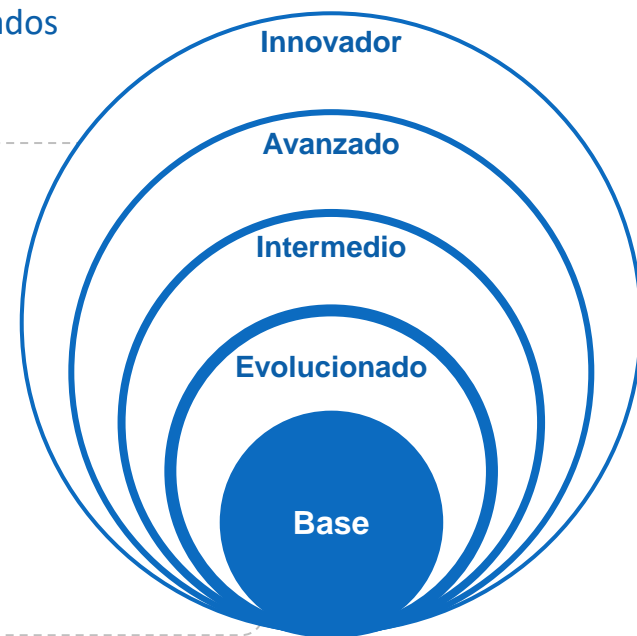
Para conocer cuántos controles se aplican a las organizaciones es necesario conocer el **perfil del Riesgo Inherente** existente en la organización y en base a esto se puede determinar el **nivel de madurez** (existen 5 niveles de Madurez).

## Dominios

- **Dominio 1:** Cyber Risk Management and Oversight
- **Dominio 2:** Threat Intelligence & Collaboration
- **Dominio 3:** Cybersecurity Controls
- **Dominio 4:** External Dependency Management
- **Dominio 5:** Cyber Incident Management and Resilience

## Niveles de Madurez

- Nivel base
- Nivel Evolucionado
- Nivel Intermedio
- Nivel Avanzado
- Nivel Innovador



# ¿Cómo se calcula el perfil de riesgo inherente?

40 preguntas sobre 5 dimensiones

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

1) Technologies and Connection Types

2) Delivery Channels.

3) Online/Mobile Products and Technology Services

4) Organizational Characteristics.

5) External Threats.

# Presentación de Riesgo Inherente x Madurez

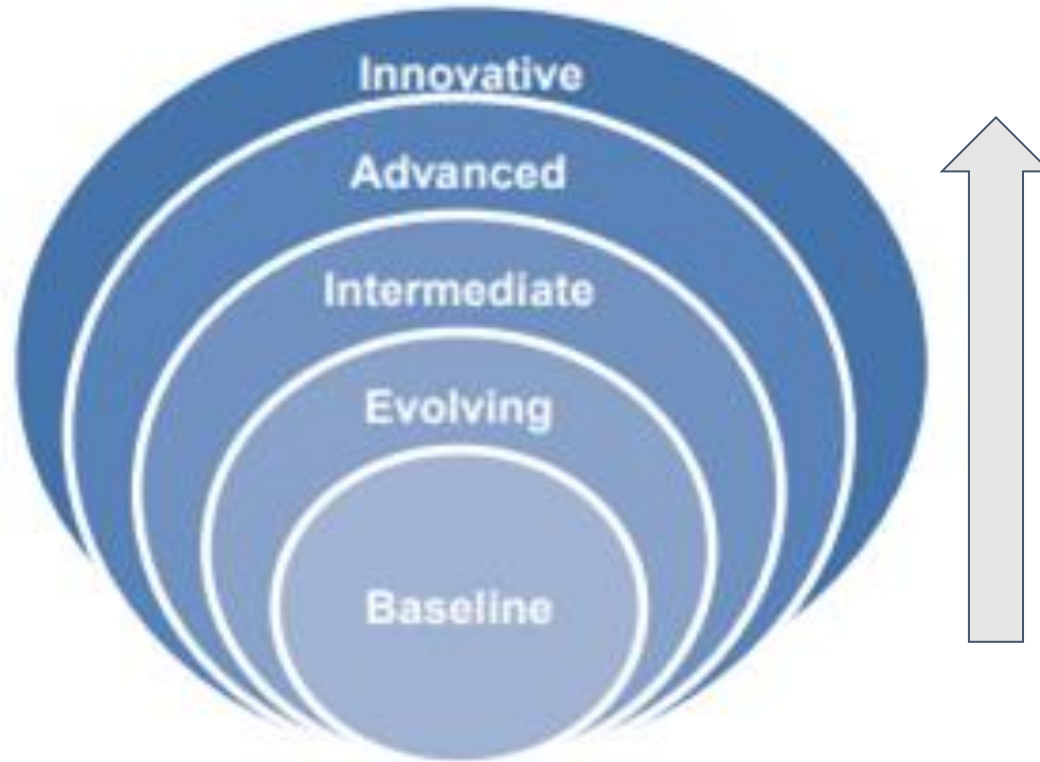
		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			

## Proceso continuo

- determining target maturity levels.
- conducting a gap analysis.
- prioritizing and planning actions.
- implementing changes.
- reevaluating over time.
- communicating the results.

# Niveles de Madurez Cybersecurity

---

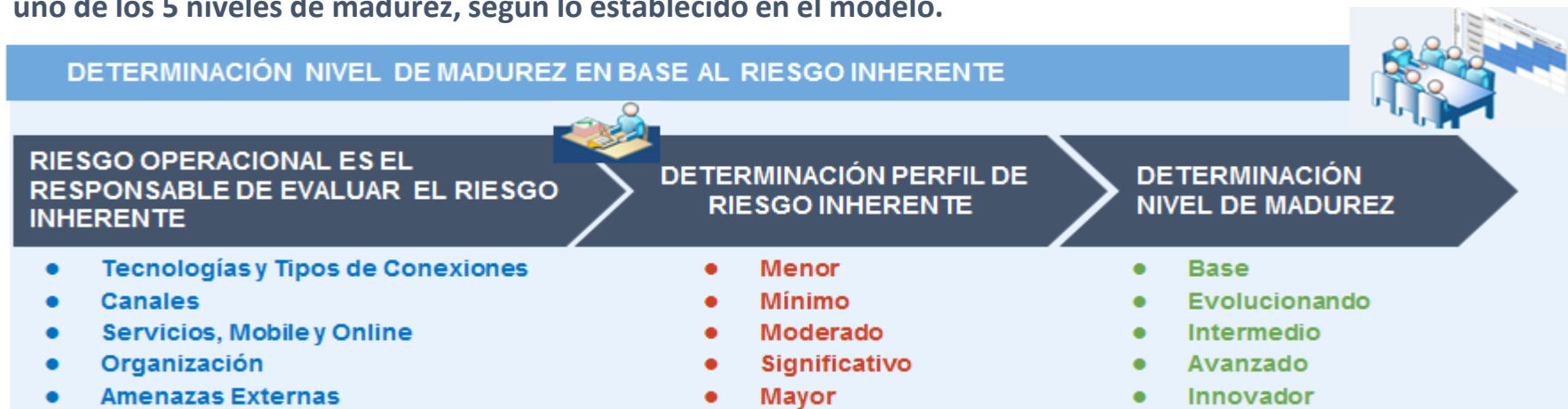


# Implementación del CAT-FFIEC en BCI

En el caso de BCI, se acuerda la aplicación del modelo CAT en los sistemas y plataformas considerados críticos para el negocio y que están reflejados en el BIA (Business Impact Analysis).

El modelo es transversal al banco, involucrando a todas las gerencias que dan continuidad al negocio. Es también aplicable a todas las filiales.

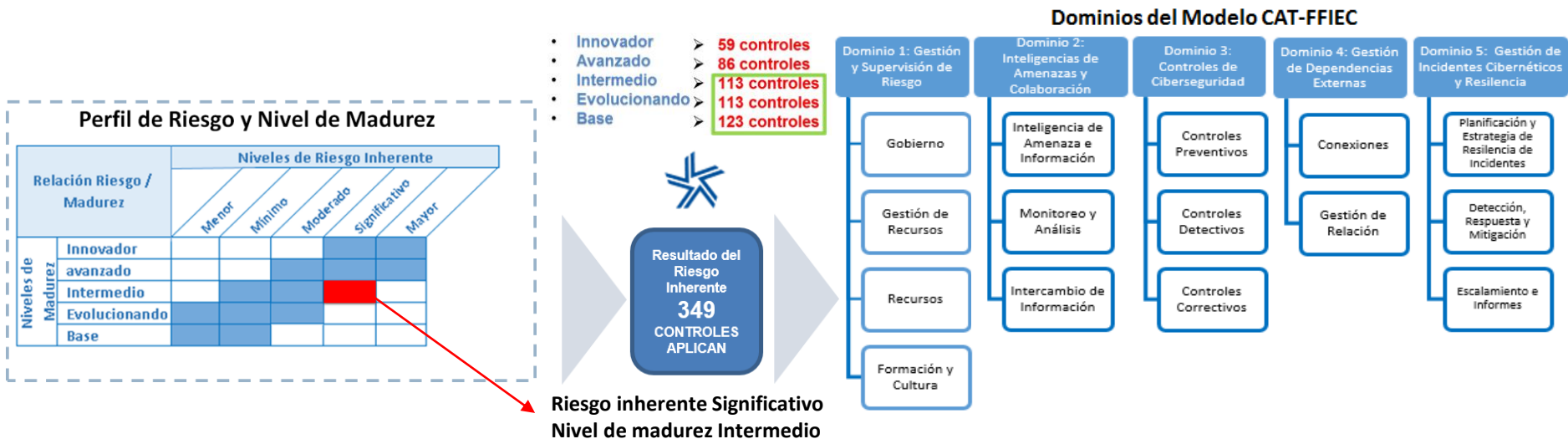
El punto inicial para la implementación del CAT, es el cálculo del riesgo inherente para luego situar al banco en uno de los 5 niveles de madurez, según lo establecido en el modelo.



# Determinación de cantidad de controles CAT-FFIEC en BCI

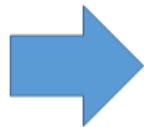
Una vez calculado el riesgo inherente de la organización, es posible definir en qué nivel de madurez trabajará la institución. Posteriormente, determinando el nivel de madurez, es posible asignar la cantidad de controles que se van aplicar en el banco.

Actualmente y en base al análisis realizado, BCI tiene un riesgo inherente significativo con un nivel de madurez intermedio lo que asigna 349 controles a revisar y que se enmarca en los 5 dominios del CAT.



# Alcance y Distribución del Modelo CAT-FFIEC en BCI

La integración de la herramienta CAT-FFIEC y sus 349 controles establecidos para el banco BCI, son aplicados transversalmente en la organización, permitiendo mantener controlada y monitoreada las distintas áreas del banco en busca de mejoras en la ciberseguridad, como también en la detección de brechas que podrían ser un posible foco de riesgo en el funcionamiento normal del banco.



ÁREAS DUEÑAS  
DE CONTROLES

- Seguridad Informática
- Continuidad de Negocios
- Op. Computacionales
- Riesgo Operacional
- Contraloría
- Fiscalía
- Compras
- Atracción de Talentos
- Capacitación
- Fiscalía
- RRHH
- Control de Acceso
- Desarrollo
- QA
- Telecanal
- Seguridad Física



Se establece un proceso de evaluación continua de ciberseguridad respecto del referente FFIEC-CAT Alineado con las 3 líneas de defensa.



# Evaluación de Riesgo Inherente de Ciberseguridad (CAT-FFIEC)



\* CAT - Cybersecurity Assessment Tools

\*FFIEC- Federal Financial Institutions Examination Council

Riesgo Operacional recalcula el riesgo inherente de la Corporación cada 3 meses

# Perfil de Riesgo Inherente, Abril 2016

**Riesgo Operacional, en el mes de Abril, identificó el siguiente Perfil de Riesgo Inherente**

Relación Riesgo / Madurez		Niveles de Riesgo Inherente				
		Menor	Mínimo	Moderado	Significativo	Mayor
Niveles de madurez	Innovador					
	Avanzado					
	Intermedio		X			
	Evolucionando		X			
	Inicial		X			

# Perfil de Riesgo Inherente esperado, Octubre 2016

**Contraloría, en el mes de Octubre, identificó el siguiente Perfil de Riesgo Inherente**

Relación Riesgo / Madurez		Niveles de Riesgo Inherente				
		Menor	Mínimo	Moderado	Significativo	Mayor
Niveles de madurez	Innovador					
	Avanzado					
	Intermedio					
	Evolucionando			X		
	Inicial					

# Comparativa Nivel de Madurez; Abril y Noviembre.

## *Dominio 1 : “Cyber Risk Management & Oversight”*

Dominio	Factor	Componente	Nivel de Madurez (Abril 2016)	Nivel de Madurez Propuesta (Noviembre 2016)	Gap Evolucionando	Cumplimiento x Nivel				
						Inicial	Evolucionando	Intermedio	Avanzado	Innovador
1: Cyber Risk Management & Oversight	1: Gobierno	1:Supervisión	Evolucionando	Evolucionando						
		2: Estrategia / Políticas	Inicial	Evolucionando						
		3: Gestión de activos de TI	Menos que Inicial	Inicial	3					
	2: Gestión del Riesgo	1: Programa de Gestión de Riesgo	Evolucionando	Evolucionando						
		2: Evaluación de Riesgos	Intermedio	Intermedio						
		3: Auditoría	Evolucionando	Evolucionando						
	3: Recursos	1: Dotación	Inicial	Evolucionando						
	4: Entrenamiento y Cultura	1: Entrenamiento	Menos que Inicial	Evolucionando						
		2: Cultura	Inicial	Evolucionando						

Para cumplir con el GAP, se deben realizar iniciativas relacionadas con el Ciclo de Vida del Activo.

# Estadística Comparativa del Análisis

Dominios	Revisión Abril 2016 *			Revisión Noviembre 2016 *		
	No	Yes	Total	No	Yes	Total
1: Cyber Risk Management & Oversight	75	66	141	79	56	135
2: Threat Intelligence & Collaboration	12	33	45	9	30	39
3: Cybersecurity Controls	33	141	174	29	121	150
4: External Dependency Management	19	32	51	19	30	49
5: Cyber Incident Management and Resilience	44	39	83	42	37	79
<b>Total general</b>	<b>316</b>	<b>178</b>	<b>494</b>	<b>178</b>	<b>274</b>	<b>452</b>
<b>Porcentaje</b>	<b>64%</b>	<b>36%</b>	<b>100%</b>	<b>40%</b>	<b>60%</b>	<b>100%</b>



- Se baja el total de controles de 494 a 452, se dejan fuera los controles objetados por la primera carta del FFIEC y los que no aplican a la regulación Chilena.
- Sobre un universo de controles actualizado, pasamos de un 36% de respuestas afirmativas a un 60%.

\*Datos son referenciales

## En Resumen...

---

1. **CAT-FFIEC es una herramienta y no es un estándar**
1. **Es una excelente herramienta para trazar un roadmap de seguridad**
1. **Permite priorizar inversiones y justificarlas frente a los directores y administración**
1. **Importante participación e involucramiento de todas las líneas de defensa**
1. **Importante generar un proceso de medición y control permanente.**
1. **Una de las mayores complejidades es determinar el alcance**

**Desafío, lograr aplicarlo a otras industrias....**

# Información en extenso en :

---

<https://www.ffiec.gov/cybersecurity.htm>



Cristian Guerra Bahamondes



---

# Proyecto implementación Cat FFIEC

Cristian Guerra Bahamondes

**Disclaimer:** El contenido y los datos mostrados del caso de implementación en esta presentación, han sido modificados por objeto de confidencialidad, las opiniones de esta presentación no representan a la Corporación BCI y están expresadas con un objeto de educación.



## Anexo: áreas de levantamiento de cuestionario de riesgo inherente

---

- **Technologies and Connection Types.** Certain types of connections and technologies may pose a higher inherent risk depending on the complexity and maturity, connections, and nature of the specific technology products or services. This category includes the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices.
- **Delivery Channels.** Various delivery channels for products and services may pose a higher inherent risk depending on the nature of the specific product or service offered. Inherent risk increases as the variety and number of delivery channels increases. This category addresses whether products and services are available through online and mobile delivery channels and the extent of automated teller machine (ATM) operations.
- **Online/Mobile Products and Technology Services.** Different products and technology services offered by institutions may pose a higher inherent risk depending on the nature of the specific product or service offered. This category includes various payment services, such as debit and credit cards, person-to-person payments, originating automated clearing house (ACH), retail wire transfers, wholesale payments, merchant remote deposit capture, treasury services and clients and trust services, global remittances, correspondent banking, and merchant acquiring activities. This category also includes consideration of whether the institution provides technology services to other organizations.
- **Organizational Characteristics.** This category considers organizational characteristics, such as mergers and acquisitions, number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information technology (IT) environment, locations of business presence, and locations of operations and data centers.
- **External Threats.** The volume and type of attacks (attempted or successful) affect an institution's inherent risk exposure. This category considers the volume and sophistication of the attacks targeting the institution.