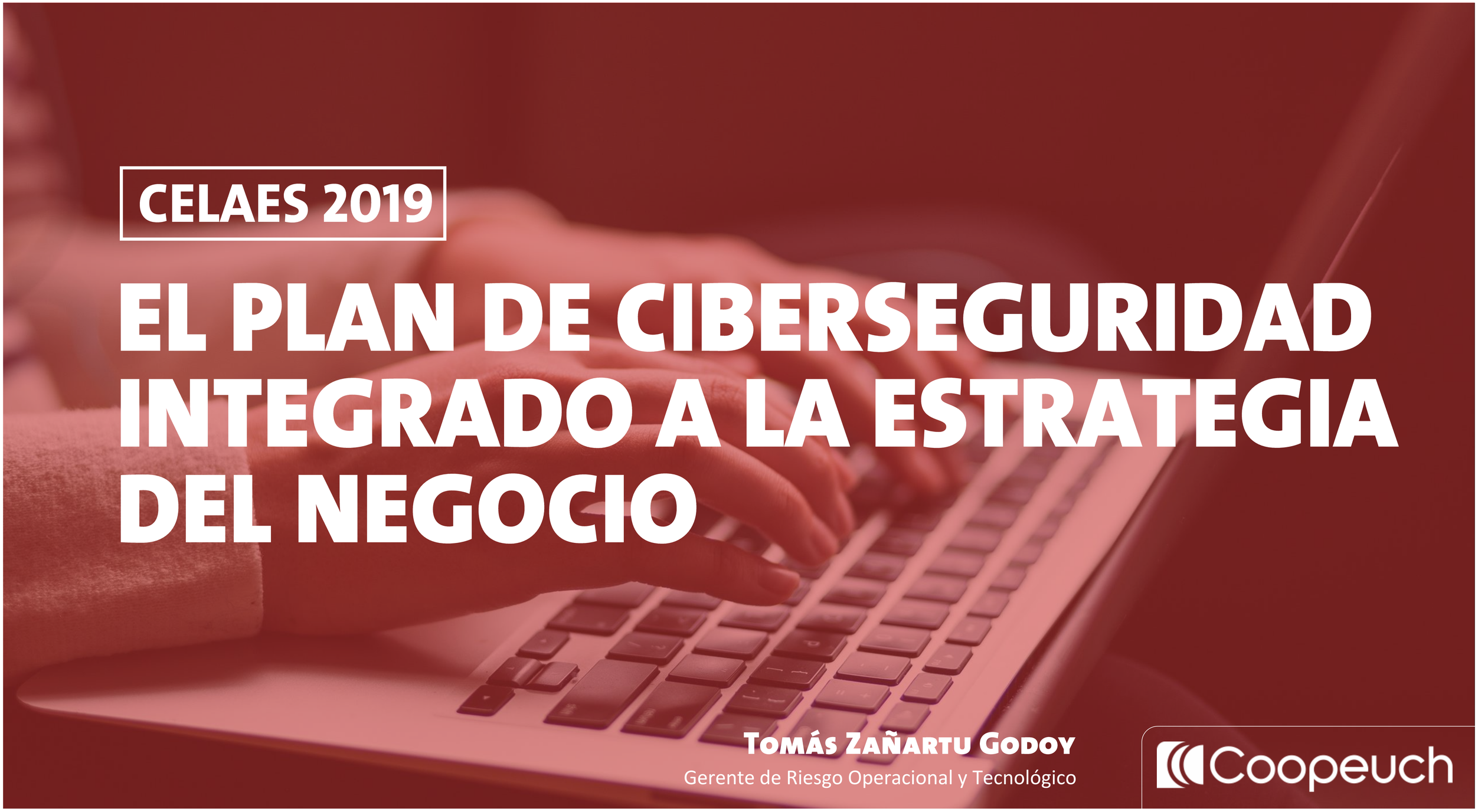


CELAES 2019

# EL PLAN DE CIBERSEGURIDAD INTEGRADO A LA ESTRATEGIA DEL NEGOCIO

**Tomás Zañartu Godoy**
Gerente de Riesgo Operacional y Tecnológico

Coopeuch

Coopeuch

# Quiénes Somos

# Somos la mayor Cooperativa de Ahorro y Crédito de Latinoamérica

Coopeuch fue fundada en el año 1967 y hoy es líder en Chile.

Institución financiera controlada democráticamente por sus socios.

Una Cooperativa altamente regulada por entidades bancarias, incluyendo mismos supervisores de banca (CMF, Banco Central).

Nuestros socios son en su mayoría personas naturales.

# Nuestro propósito es contribuir al desarrollo y progreso de nuestros socios y sus familias.

También la de clientes y la comunidad, contribuyendo a la sociedad y al país, a través de la facilitación de productos y servicios financieros inclusivos.

# Entregamos una oferta de valor integral de productos y servicios a nuestros socios y clientes

## Activo

- Créditos de Consumo en Cuotas
- Crédito Hipotecario
- Tarjeta de Crédito
- Créditos para Mipe

## Servicios

- Cuenta Vista
- Ahorro
- Depósitos a Plazo
- Cuotas de participación

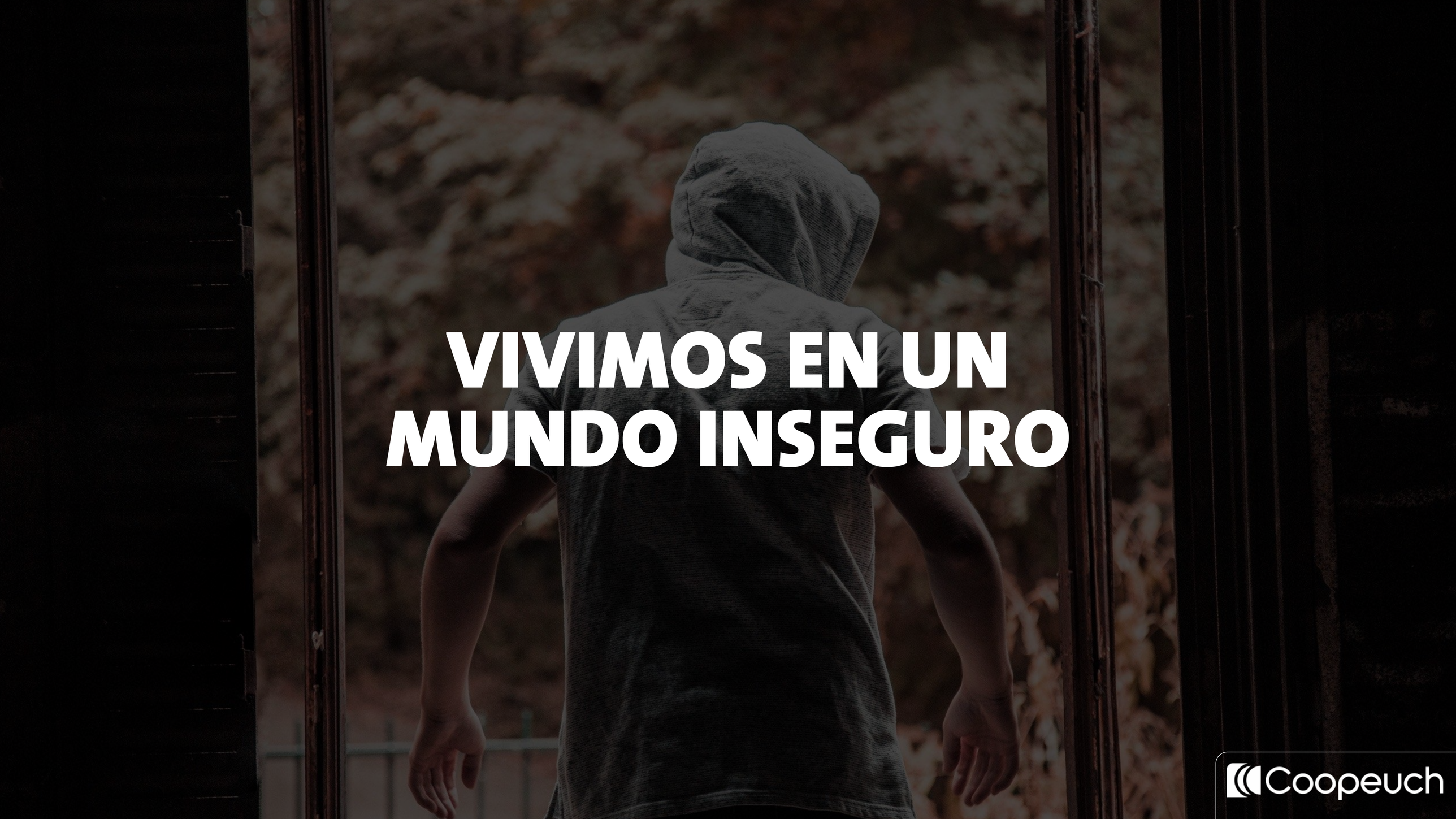
## Pasivo / Patrimonio

- Seguros
- Transferencia Electrónicas de Fondos

Coopeuch

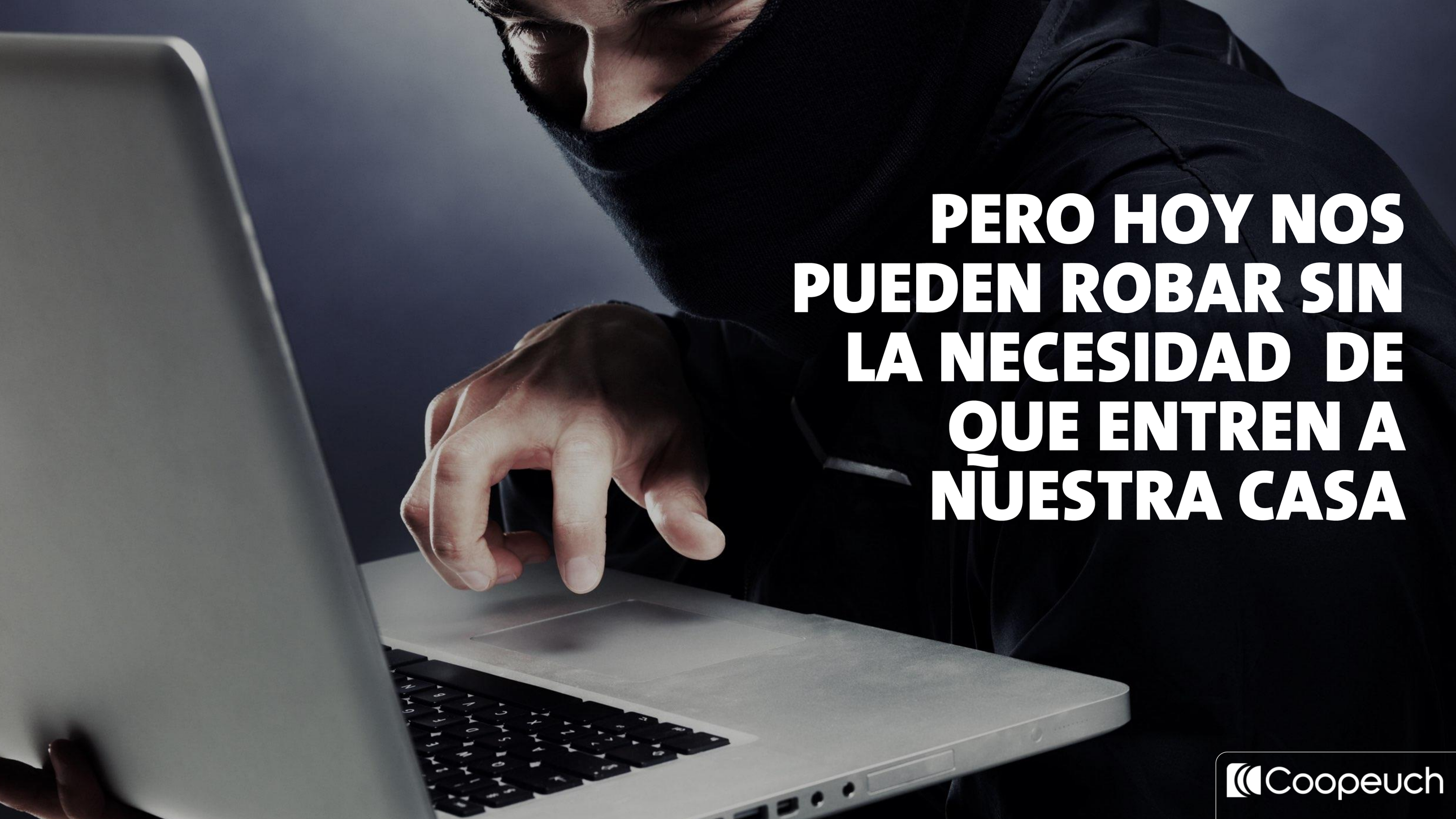
# ¿POR QUÉ ES IMPORTANTE LA CIBER SEGURIDAD?


NUESTRO PROPÓSITO ES MEJORAR LA CALIDAD DE VIDA LAS PERSONAS.
Y LA SEGURIDAD ES PARTE DE ESE PROPOSITO.
Coopeuch


VIVIMOS EN UN
MUNDO INSEGURO


CADA DÍA LAS PERSONAS SE
SIENTEN MÁS INSEGURAS
Coopeuch


LES ASUSTA QUE ENTREN
A ROBAR A SUS CASAS
Coopeuch

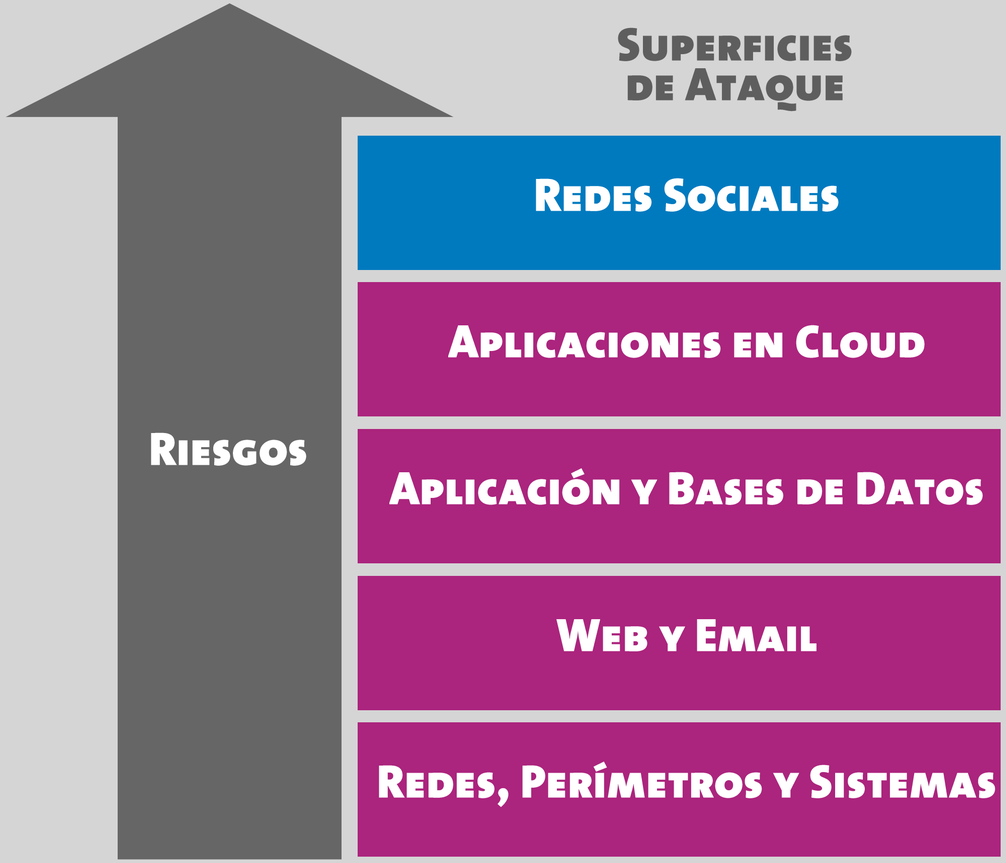

PERO HOY NOS
PUEDEN ROBAR SIN
LA NECESIDAD DE
QUE ENTREN A
NUESTRA CASA
Coopeuch


TODA NUESTRA
VIDA ESTÁ AQUÍ
Coopeuch


# AHÍ ES DONDE ENTRA EN JUEGO LA CIBER SEGURIDAD

Coopeuch

# NOS ENFRENTAMOS A NUEVAS SUPERFICIES DE ATAQUE

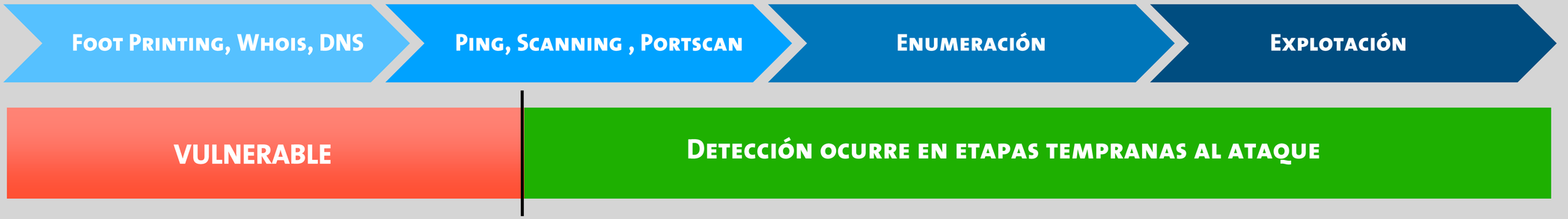



- La educación es clave, pero requiere tiempo. Las nuevas superficies de ataque mejoran Time to Market del Cibercrimen.
- Soluciones CASB para nuestras aplicaciones en la nube de terceros.
- Firewalls de nueva generación y herramientas avanzadas para el monitoreo de bases de datos.
- Web filtering y Gateway de correos
- Los virus logran avanzar con fuerza con infecciones masivas.

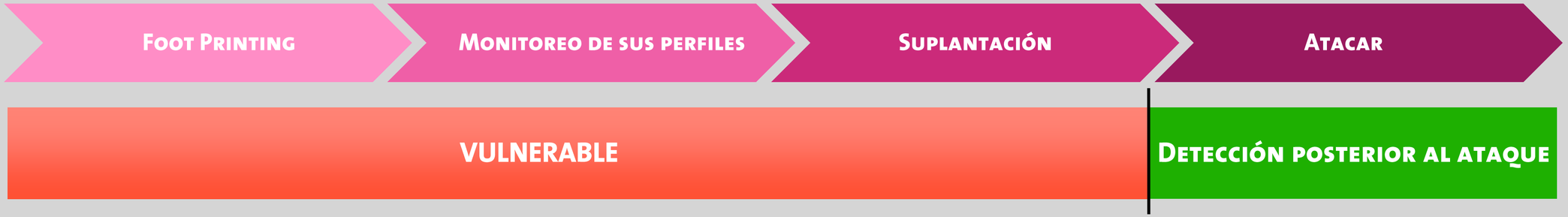
Coopeuch

# .....EN UN ENTORNO DE MAYOR COMPLEJIDAD

## Ataque Tradicional




## Ataque a un Red Social



# Nuevo entorno de interconexión total y delitos informáticos cada vez más frecuentes en la industria financiera

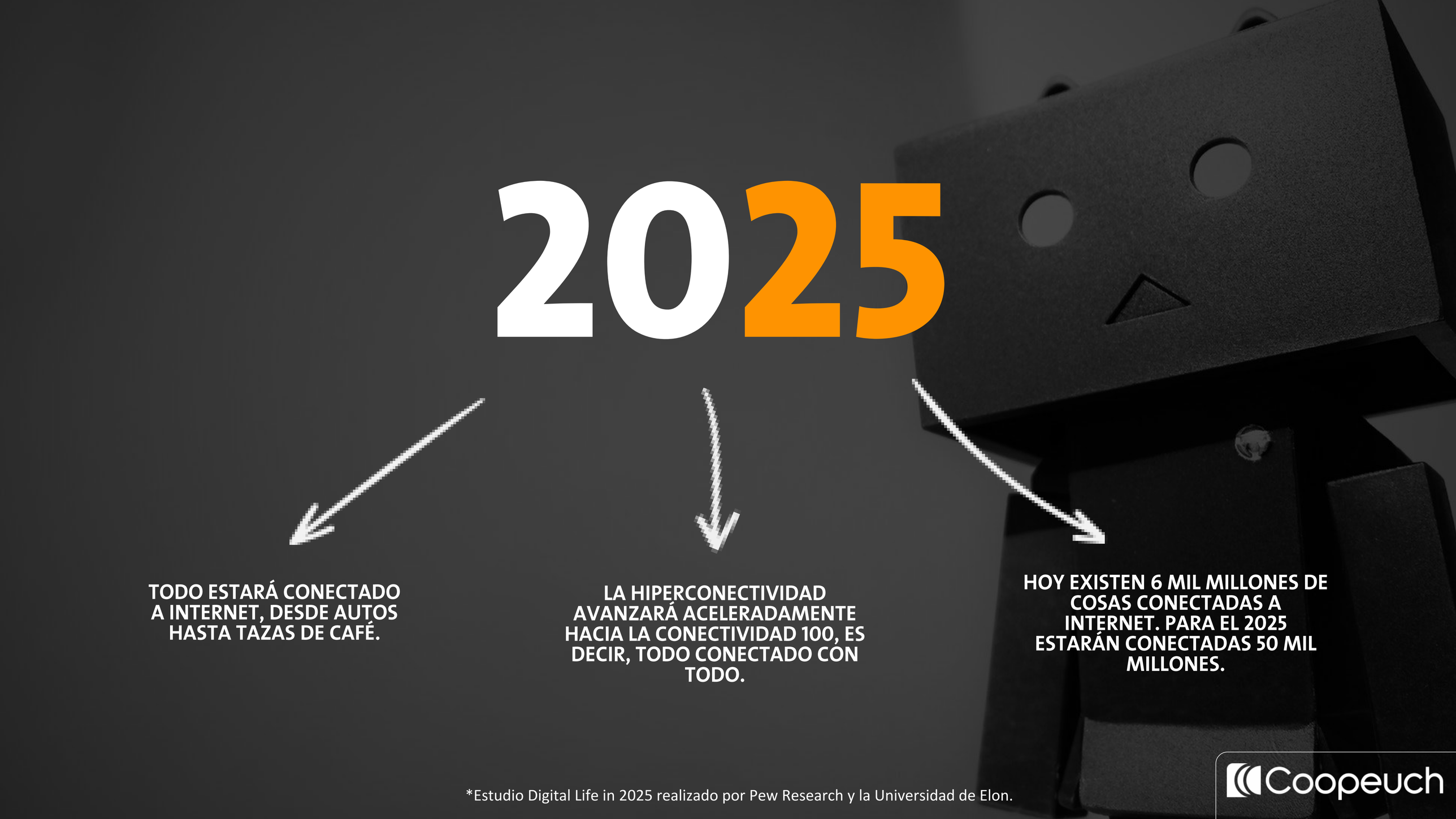
Coopeuch

# “LA GENTE CONFIARÁ MAS EN AMAZON QUE EN SU BANCO”.

## Erik Qualman


Coopeuch

# 2025



TODO ESTARÁ CONECTADO A INTERNET, DESDE AUTOS HASTA TAZAS DE CAFÉ.

LA HIPERCONECTIVIDAD AVANZARÁ ACELERADAMENTE HACIA LA CONECTIVIDAD 100, ES DECIR, TODO CONECTADO CON TODO.

HOY EXISTEN 6 MIL MILLONES DE COSAS CONECTADAS A INTERNET. PARA EL 2025 ESTARÁN CONECTADAS 50 MIL MILLONES.

*Estudio Digital Life in 2025 realizado por Pew Research y la Universidad de Elon.

Coopeuch

# El ciber crimen sabe donde están nuestras vulnerabilidades

**80%**

De los ataques se deben a errores humanos y no temas tecnológicos.

**41**

Años de edad es el promedio de las víctimas.

**90%**

De los correos recibidos es Spam o Virus.

**30%**

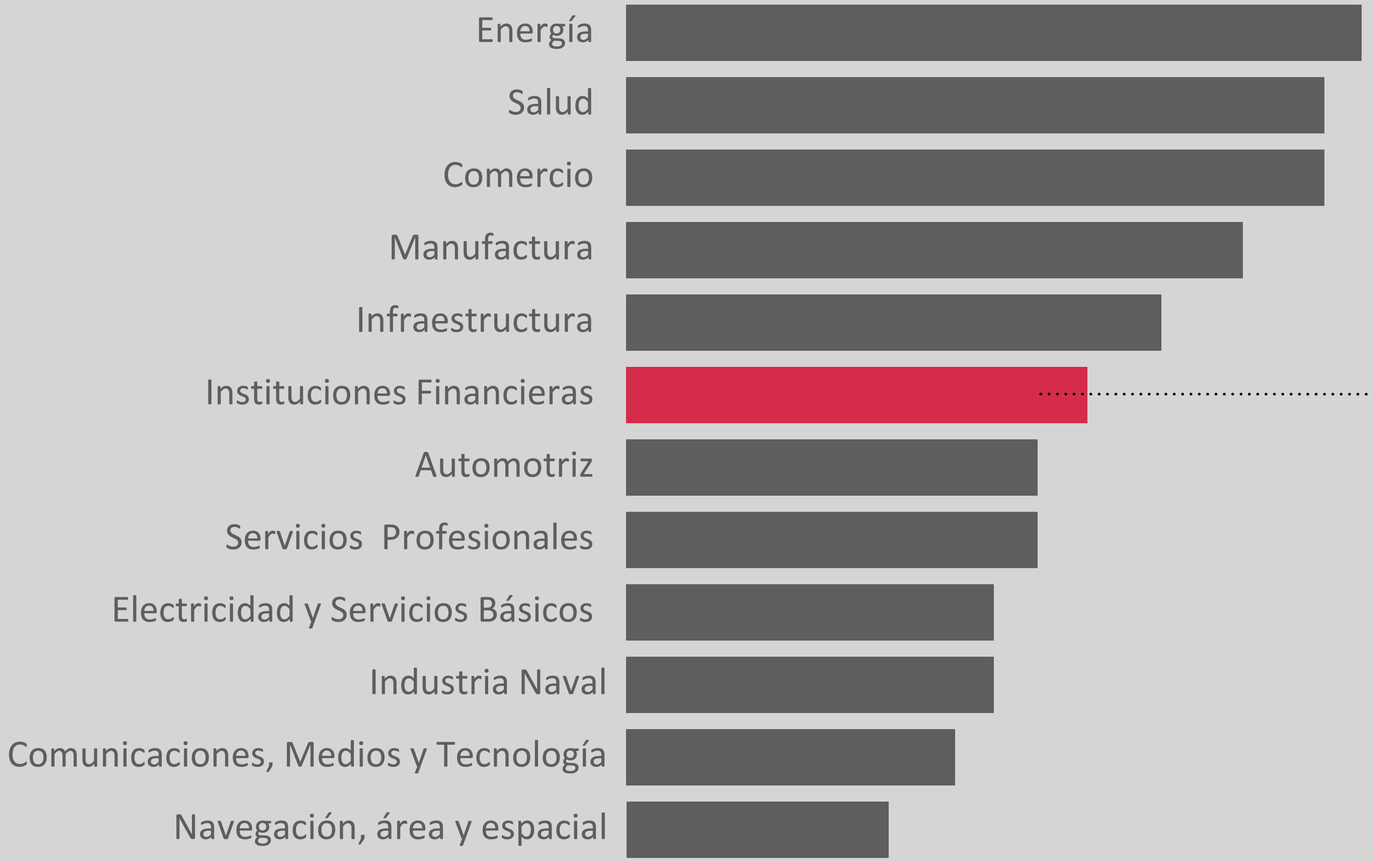
De las personas hace click en un email de Phishing

**77%**

De los ataques de ingeniería social son Phishing

Coopeuch

# LOS INDICADORES QUE HACEN QUE LA CIBERSEGURIDAD SEA UNA PREOCUPACIÓN A NIVEL GLOBAL




**La industria financiera es la más afectada por el Cibercrimen, con costos anuales que alcanzan los**

**US$18,28**

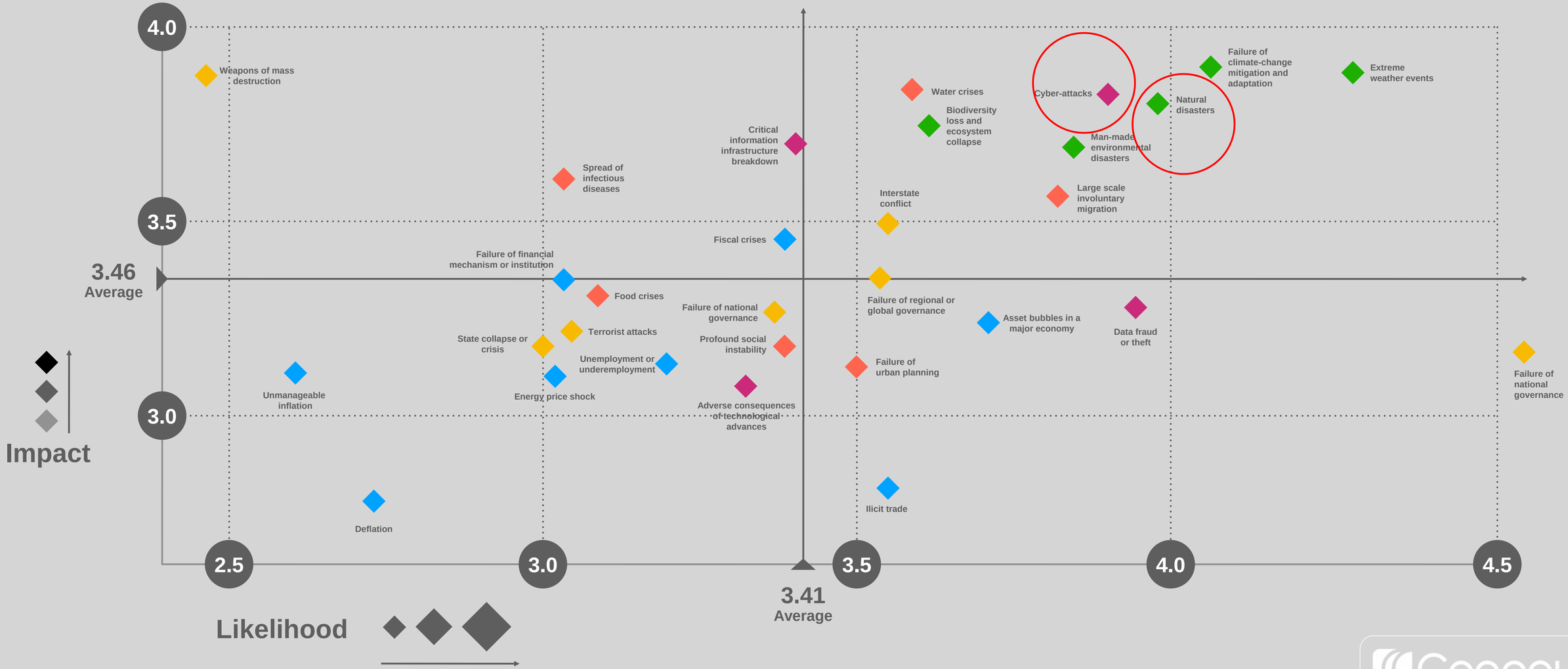
millones anuales

Fuente: Marsh&McLennan Companies, Global Risk Center (2018): MMC Cyber Handbook 2018.

Coopeuch

# EL MAPA DE RIESGOS 2019

## Impacto y Probabilidad de ocurrencia de riesgos en el mundo




Fuente: Adaptación WEF_Global_Risks_Report_2019

Coopeuch

# DESAFÍOS DE LA CIBERSEGURIDAD EN EL SECTOR FINANCIERO

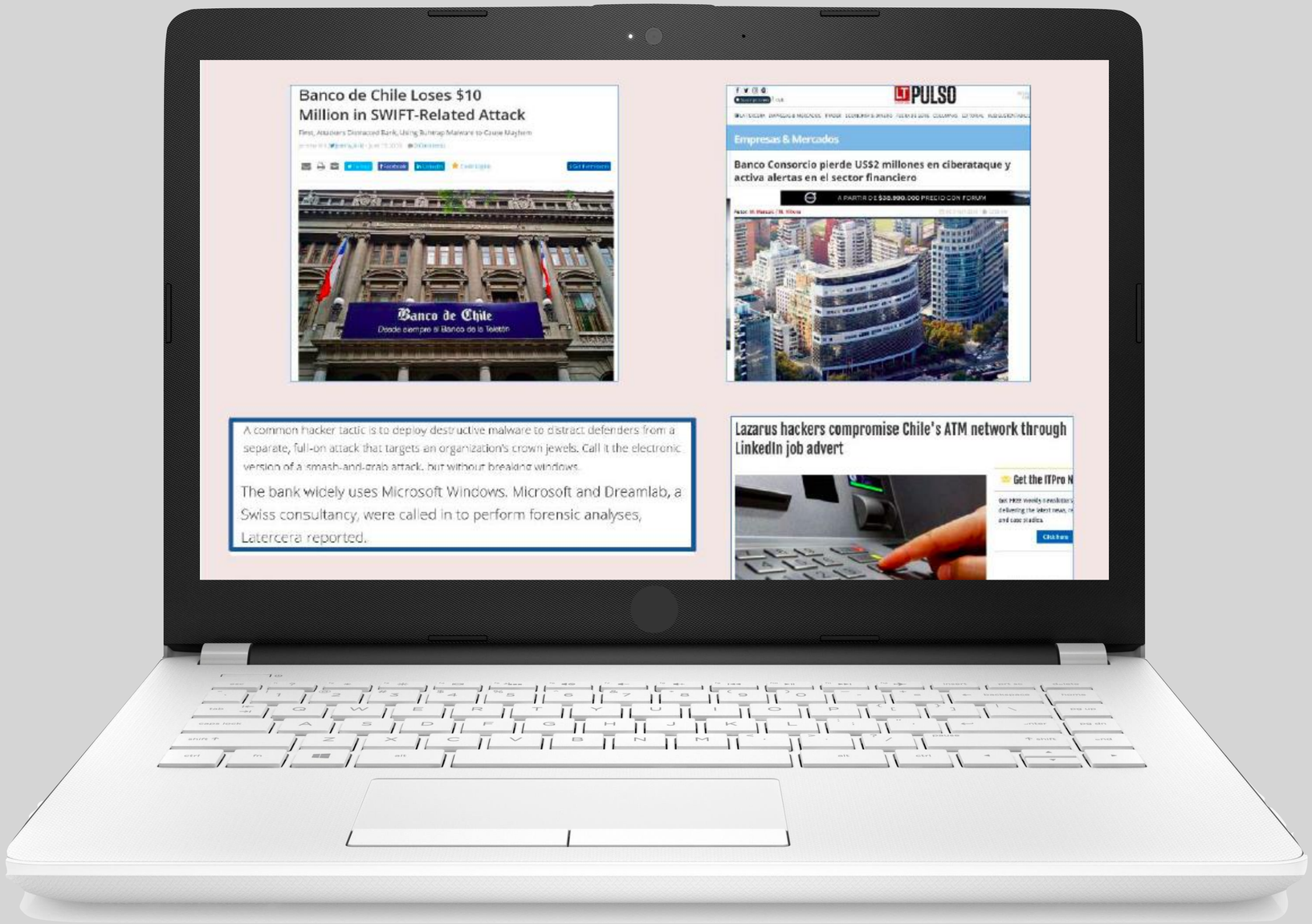
REGULACIONES CAMBIANTES

AMENAZAS QUE EVOLUCIONAN

TRANSFORMACION DIGITAL

Coopeuch

# ESTO ES UNA REALIDAD Y LLEGO PARA QUEDARSE




¿CÓMO DEBEMOS
ENFRENTAR LOS RIESGOS
EN LA ERA DIGITAL?
Coopeuch

# CONOCER A TU OPONENTE ES CLAVE


Coopeuch

# CONOCER A TU OPONENTE ES CLAVE


Coopeuch


CONOCER SUS HÁBITOS
CÓMO SE ALIMENTA
QUÉ ELEMENTOS UTILIZA
Coopeuch

# TRES PREGUNTAS CLAVE QUE NOS DEBEMOS HACER LAS INSTITUCIONES FINANCIERAS

¿Quién nos podría atacar?

¿Qué buscan y cuáles son nuestros Riesgos?

¿Qué estrategias podrían utilizar para atacarnos?

Coopeuch


Mexico
Nigeria
Ethiopia
Poland
Iraq
India
Bangladesh
Thailand
Vietnam
Taiwan
Indonesia
Malaysia
Costa Rica
Brazil
Uruguay
Chile
Kenya
Gabon
Targets:
Financial institutions
Casinos
Software developers for investment companies
Crypto-currency businesses
LAZARUS

# APT 38

## También conocido como

# Lazarus

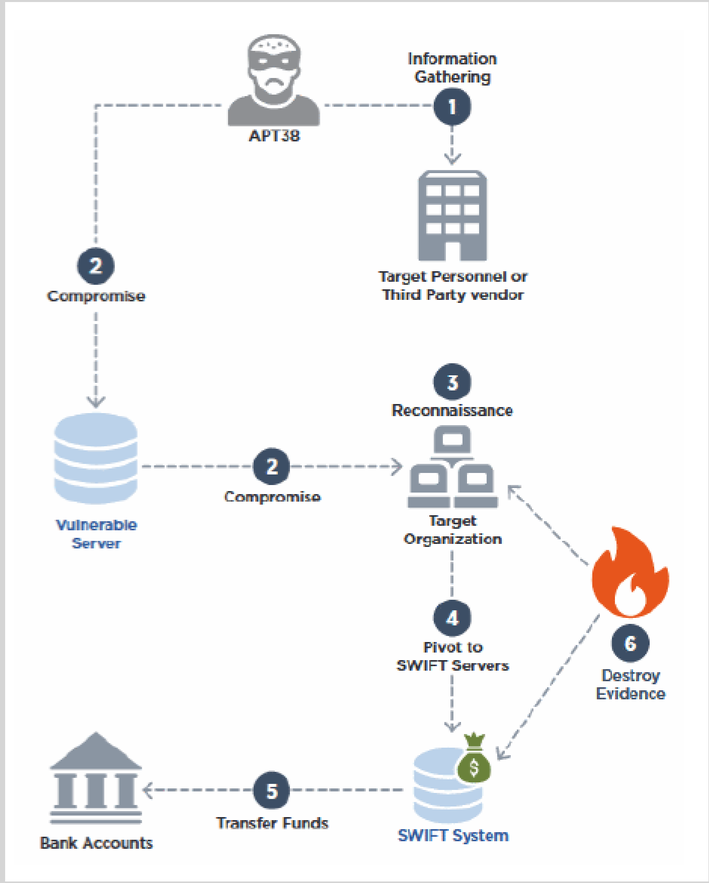
... o Hidden Cobra, Chollima, Guardians of Peace y otros. Es un grupo del tipo APT. Este es un tipo de ciberataques que son altamente sofisticado, prolongados a un blanco específico. Tienden a estar alineados con naciones/estados, y en el caso de Lazarus, exhibe comportamientos absolutamente alineados con los objetivos de ciber guerra norcoreanos.

Grupo con motivaciones financieras que ataca bancos e instituciones financieras de todos el mundo, tiene altas capacidades para crear y distribuir malware, ofuscar código, crear y encintar canales, para infiltrarse entre sus víctimas.

# APT 38 Swift Attack

| | | | |
|---|---|---|---|
| External reconnaissance | Initial Infection | Download Dropper | C&C Connection |
| Privileges Escalation | AD Compromised | Lateral Movement To gain understanding of critical systems | Critical system Infection |
| | Send Money Home | Last infection to Burn the place... Job Done | |

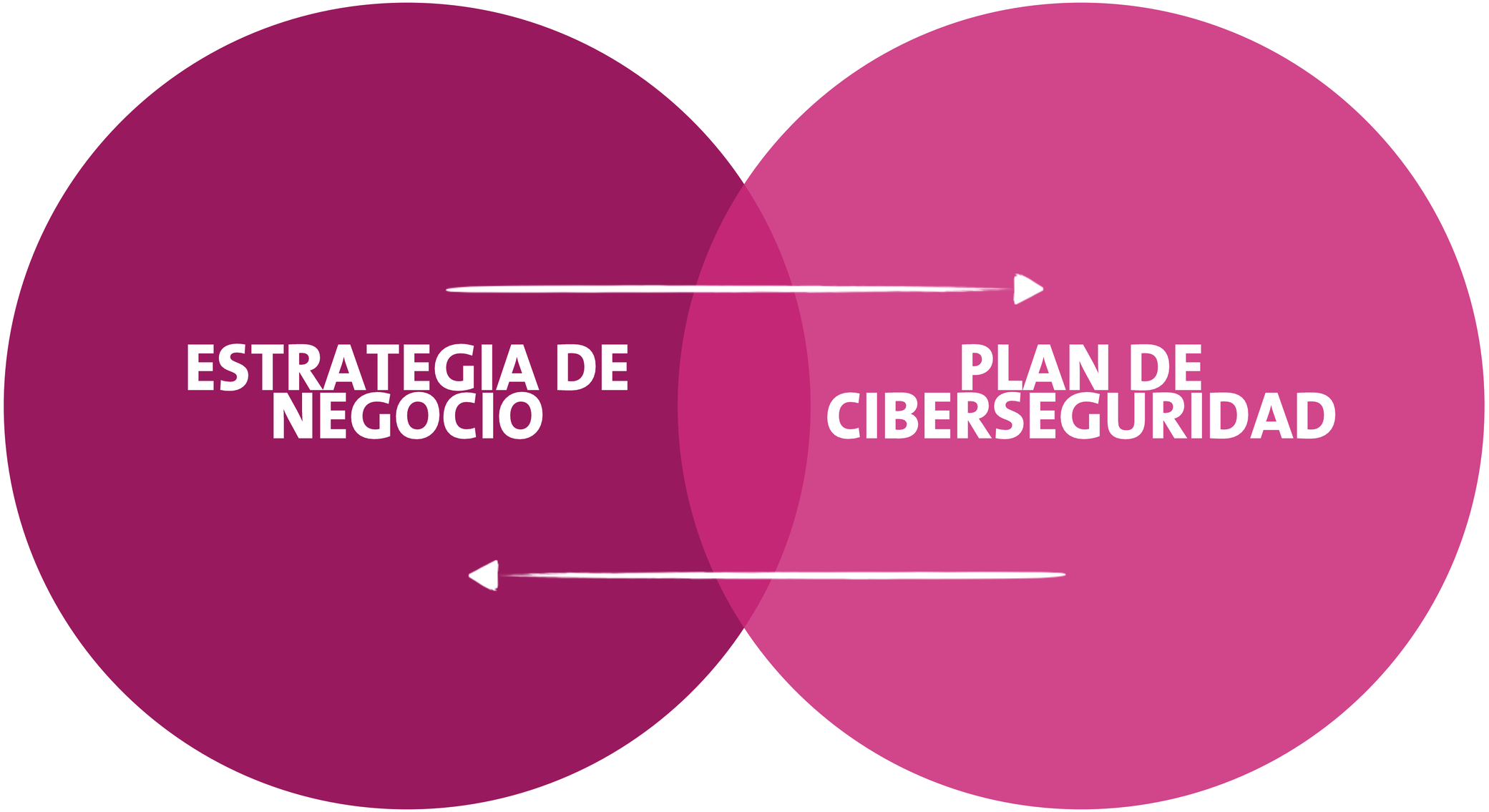
5 meses (150 días)




Coopeuch

Coopeuch

# LA CIBER SEGURIDAD DEBE SER PARTE DE LA ESTRATEGIA DEL NEGOCIO


ESTRATEGIA DE NEGOCIO
PLAN DE CIBERSEGURIDAD

# LA ESTRATEGIA DE CIBER SEGURIDAD SE DEBE POSICIONAR AL MÁS ALTO NIVEL DE GOBIERNO CORPORATIVO

Coopeuch

# CIBERSEGURIDAD Y MODELO DE CONTROL INTERNO

## Modelo de Control Interno y su conexión con la Ciberseguridad

**MARCO DEL GOBIERNO CORPORATIVO**

| 1ra. Línea de Defensa | 2da. Línea de Defensa | 3ra. Línea de Defensa |
|---|---|---|
| Responsables de asegurar las medidas de Ciberseguridad – Seguridad Tecnológica | Gestión del Riesgo de Ciberseguridad – Monitoreo, políticas, normas, indicadores. | Auditoría Interna– Evaluación efectividad de los controles |
| Grupo de Respuesta a Incidentes | **Control de Framework (FFIEC)** | **Auditoría Interna a Ciberseguridad** |
| Ejecución de Ciberseguridad | **Análisis de Amenazas** | |
| Proyectos de Ciberseguridad | **Inteligencia de Riesgo en Ciberseguridad** | |
| | **Monitoreo Externo e Independiente** | |

Auditor Externo

CMF y Otros Organismos Fiscalizadores

**1º LÍNEA DE DEFENSA**

Plan de Ciberseguridad Tecnológica

**2º LÍNEA DE DEFENSA**

Programa de Gestión de Ciber Riesgos

**3º LÍNEA DE DEFENSA**

Plan de Auditoria de Ciberseguridad

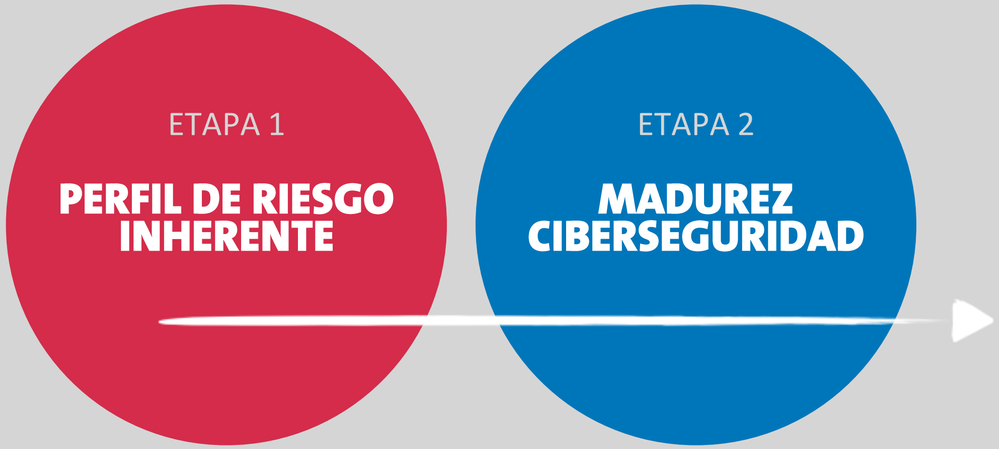
Coopeuch

# EL PUNTO DE PARTIDA DEL PLAN DE CIBER SEGURIDAD

## Riesgos y madurez en Ciber Seguridad

# EVALUACIÓN DE RIESGO Y MADUREZ DE CIBERSEGURIDAD

CONSTA DE DOS ETAPAS




Estas 2 etapas permiten evaluar si el riesgo inherente y la preparación de la institución están alineados.

COMO RESULTADO LOGRAMOS OBTENER

Un diagnóstico con el perfil de riesgo y análisis GAP en materias de Ciberseguridad.

Convergen los más altos estándares de ciberseguridad para la industria financiera (NIST , ISO 27.000, COBIT, SANS 20 Critical).

Fuente: CAT FFIEC

Coopeuch

# SIEMPRE ESTAMOS ATENTOS A LOS PERFILES DE RIESGO INHERENTE

EVALUANDO EL RIESGO DE:

- TECNOLOGÍAS Y TIPOS DE CONEXIÓN
- ORGANIZACIÓN DE TI
- CANALES DE ENTREGA
- AMENAZAS EXTERNAS
- PRODUCTOS ON LINE Y SERVICIOS MÓVILES Y TECNOLOGÍA.

En la evaluación se observa el tipo, volumen y complejidad de las operaciones y las amenazas dirigidas a Coopeuch

Se evalúan 39 factores para cada una de las actividades, servicios y productos. Evaluados a través de entrevistas con las diferentes áreas en relación a la Ciberseguridad, calificando diferentes niveles de riesgo.


Fuente: CAT FFIEC

Coopeuch

# REALIZAMOS EVALUACIONES CONSTANTES EN NUESTRA MADUREZ DE CIBERSEGURIDAD

La Madurez sirve para determinar si las conductas, prácticas y procesos de una institución puede apoyar la preparación para la ciberseguridad dentro de los cinco dominios.


**NIVELES DE MADUREZ**

Ámbitos de evaluación de madurez de ciberseguridad

---

Gestión de riesgos y Control de Ciberseguridad.

Amenaza de Riesgo y Colaboración.

Controles de Ciberseguridad.

Gestión de Proveedores TI.

Gestión de Incidentes y Resiliencia.

Fuente: CAT FFIEC

Coopeuch

# EVALUACIÓN DE RIESGO

| | NIVELES DE RIESGO INHERENTE → | | | | |
|---|---|---|---|---|---|
| CATEGORÍAS | MENOS | MÍNIMO | MODERADO | SIGNIFICATIVO | MÁS |
| TECNOLOGÍAS Y TIPOS DE CONEXIONES | | | | | |
| CANALES DE ENTREGA | | | | | |
| PRODUCTOS ONLINE / SERVICIOS MÓVILES Y TEC. | | | | | |
| CARACTERÍSTICAS DE LA ORGANIZACIÓN | | | | | |
| AMENAZAS EXTERNAS | | | | | |

Fuente: CAT FFIEC

# CATEGORÍA
# SERVICIOS ONLINE / MÓVILES Y SERVICIOS TECNOLÓGICOS

| | NIVELES DE RIESGO INHERENTE → | | | | |
|---|---|---|---|---|---|
| **CATEGORÍAS** | **MENOS** | **MÍNIMO** | **MODERADO** | **SIGNIFICATIVO** | **MÁS** |
| **TRANSFERENCIAS ELECTRÓNICAS** | No ofrecido | Solicitudes persona solamente. Canales Remotos Portal Web. Volumen Diario de Cable <3% del activo total. | Solicitudes personales, por teléfono y por fax; Volumen diario de alambre doméstico 3% -5% del activo total; Volumen de cable diario internacional <3% del activo total | Múltiples canales de solicitud (por ejemplo, en línea, texto, correo electrónico, fax y teléfono); Volumen diario de alambre doméstico 6% -25% del total de activos; Volumen diario de cable internacional 3% -10% del total de activos | Múltiples canales de solicitud (por ejemplo, en línea, texto, correo electrónico, fax y teléfono); Volumen diario de alambre doméstico> 25% del activo total; Volumen diario del cable internacional> 10% del activo total |
| **EMISIÓN DE TARJETAS DE DÉBITO Y CRÉDITO** | No emita tarjetas de débito o de crédito | Emitir tarjetas de débito y / o de crédito a través de un tercero; <10,000 tarjetas pendientes | Emitir tarjetas de débito o de crédito a través de un tercero; Entre 10,000-50,000 tarjetas pendientes | Emita tarjetas de débito o de crédito directamente; Entre 50.000 y 100.000 tarjetas pendientes | Emita tarjetas de débito o de crédito directamente; > 100.000 tarjetas pendientes; Emitir tarjetas en nombre de otras instituciones financiera |
| **TARJETAS DE PREPAGO** | No emite tarjetas de prepago | Emitir tarjetas prepago a través de un tercero; <5.000 tarjetas pendientes | Emitir tarjetas prepago a través de un tercero; 5.000-10.000 tarjetas pendientes | Emitir tarjetas prepago a través de un tercero; 10,001-20,000 tarjetas pendientes | Emitir tarjetas prepago internamente, a través de un tercero, o en nombre de otras instituciones financieras; > 20,000 tarjetas pendientes |
| **TECNOLOGÍAS DE PAGOS EMERGENTES (POR EJEMPLO, CARTERAS DIGITALES, CARTERAS MÓVILES) APP MÓVIL** | No acepte ni utiliza las tecnologías de pagos emergentes, | Admisión indirecta o uso de tecnologías de pagos emergentes (el uso del cliente puede afectar la cuenta de depósito o crédito) | La aceptación o el uso directo de las tecnologías de pagos emergentes; Socio o co-marca con proveedores no bancarios; Volumen de transacción limitado | La aceptación o el uso directo de las tecnologías de pagos emergentes; Pequeño volumen de transacciones; Sin pagos en el extranjero | La aceptación directa de las tecnologías de pagos emergentes; Volumen de transacción moderado y / o pagos en el extranjero |
| **PAGOS PERSONALES DE CLIENTES** | No ofrecido | Los clientes pueden originar pagos; Utilizado por <1.000 clientes o volumen de transacción mensual es <50.000 | Los clientes pueden originar pagos; Utilizado por 1.000-5.000 clientes o volumen de transacción mensual es entre 50.000-100.000 | Los clientes pueden originar pagos; Utilizado por 5,001-10,000 clientes o volumen de transacción mensual está entre 100,001-1 millones | Los clientes pueden solicitar el pago o dar origen al pago; Utilizado por> 10.000 clientes o volumen de transacción mensual> 1 millón |
| **PAGOS CÁMARA DE COMERCIO (ACH)** | Sin origen en ACH | Originar créditos ACH; Volumen diario <3% del activo total | Originar los débitos y créditos de ACH; Volumen diario es de 3% -5% del total de activos | Patrocinador procesador de pagos de terceros; Originan débitos y créditos de ACH con un volumen diario de 6% -25% del total de activos | Patrocinar procesadores de pagos de terceros anidados; Originan débitos y créditos con un volumen diario> 25% del activo total |

Fuente: CAT FFIEC

# MATRIZ DE EVALUACIÓN
# RELACIÓN RIESGO Y MADUREZ


Fuente: CAT FFIEC

Coopeuch

# MATRIZ DE EVALUACIÓN
# RELACIÓN RIESGO Y MADUREZ


Fuente: CAT FFIEC

Coopeuch

# MATRIZ DE EVALUACIÓN RELACIÓN RIESGO Y MADUREZ


Fuente: CAT FFIEC

Coopeuch

# DEFINIR EL ROADMAP DEL PLAN DE CIBER SEGURIDAD

Hemos diseñado un plan que se divide en 4 grandes etapas, observando en ellas, el desarrollo orgánico del negocio y el cumplimiento de los objetivos estratégicos, soportado en los tres pilares claves de la organización.

**ETAPA 1**

Seguridad Transaccional

**2013 / 2015**

**ETAPA 2**

Ciberseguridad en la Transacción Digital

**2016 / 2018**

**ETAPA 3**

Gestión de Ciber Seguridad Y Fraude Inteligente

**2019 / 2020**

**ETAPA 4**

Gestión de Ciber Seguridad Cognitiva

**2021**

**PERSONAS / PROCESOS / TECNOLOGÍA**

Coopeuch

**PERSONAS / PROCESOS / TECNOLOGÍA**

## Pilar 1
## Monitoreo y Control de Riesgo

Capacidades que faciliten un monitoreo y seguimiento oportuno de los riesgos y controles en materias de Ciberseguridad.

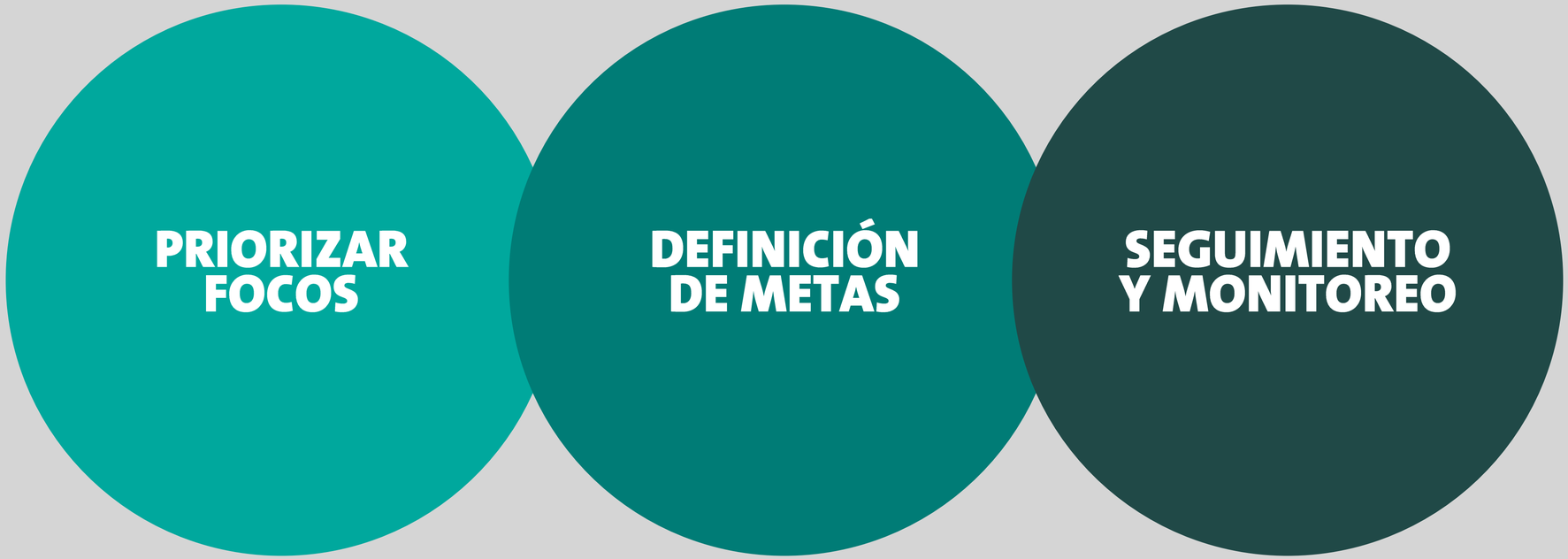
## Pilar 2
## Proyectos e Iniciativas de Seguridad Tecnológica

Nuevas capacidades tecnológicas necesarias para mitigar los riesgos inherentes a las nuevas tecnologías y amenazas.

## Pilar 3
## educación, Cultura y Monitoreo

Programas transversales (Educar, formar y sensibilizar), que contribuirán a sostener hábitos digitales que resguarden la ciberseguridad.

# ESTRATEGIA DE IMPLEMENTACIÓN




Coopeuch

# PRIORIZAR FOCOS


1
Nuevos controles preventivos, detectives y correctivos.

**GESTIÓN DE CONTROLES DE CIBER SEGURIDAD**

2
**GESTIÓN DE INTELIGENCIA DE NUEVAS AMENAZAS**

Inteligencia de Amenazas.
Monitoreo y Análisis Avanzado.
Programas de Intercambio de Información.

3
**GESTIÓN DE INCIDENCIAS DE CIBERATAQUES Y RESILIENCIA**

Planificación y Estrategia de Incidencias.
Plan de detección, Respuesta y Mitigación.
Modelo de Escalamiento y Monitoreo.

4
**GESTIÓN DE RIESGO Y CONTROL CIBERNÉTICO**

Modelo de Gestión de Riesgo.
Marco de Gobernabilidad.
Programa en Entrenamiento y Cultura.
Gestión de Recursos Humanos.

5
**GESTIÓN DE PROVEEDORES TI**

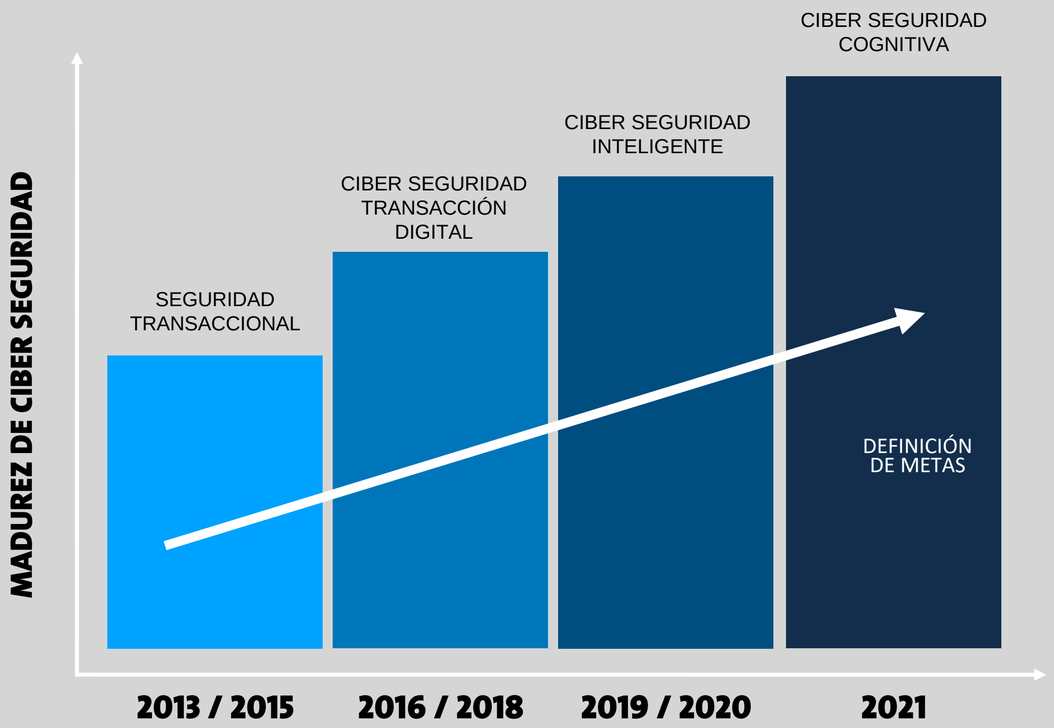
Modelo Conexiones.
Gestión de Relacionamiento.

Coopeuch

DEFINICIÓN DE METAS

# ESTRATEGIA DE IMPLEMENTACIÓN

## ETAPAS DEL PLAN




## METAS POR AÑO

| | |
|---|---|
| 2021 | INNOVADOR % |
| 2020 | AVANZADO % |
| 2019 | AVANZADO % |
| 2018 | INTERMEDIO % |

SEGUIMIENTO Y MONITOREO

# ESTRATEGIA DE IMPLEMENTACIÓN

| Foco de Gestión de Ciber Seguridad | Meta Definida 2018 | % Avance Madurez | Nivel de Madurez | Controles Implementados | Total de Controles | Menos | Mínimo | Moderado | Significativo | Mas |
|---|---|---|---|---|---|---|---|---|---|---|
| Gestión de Riesgo y Control Cibernético | Intermedio | 54,26% | Innovador | 4 | 15 | | | | 26,67% | 26,67% |
| | | | Avanzado | 14 | 32 | | | 43,75% | 43,75% | 43,75% |
| | | | Intermedio | 10 | 29 | | 34,48% | 34,48% | 34,48% | |
| | | | Evolucionado | 18 | 34 | 52,94% | 52,94% | 52,94% | | |
| | | | Base | 23 | 31 | 74,19% | 74,19% | | | |
| Inteligencia en las Amenazas y Colaboración | Intermedio | 42,31% | Innovador | 0 | 8 | | | | 0,00% | 0,00% |
| | | | Avanzado | 0 | 11 | | | 0,00% | 0,00% | 0,00% |
| | | | Intermedio | 0 | 11 | | 0,00% | 0,00% | 0,00% | |
| | | | Evolucionado | 4 | 7 | 57,14% | 57,14% | 57,14% | | |
| | | | Base | 7 | 8 | 87,50% | 87,50% | | | |
| Controles de Ciber Seguridad | Intermedio | 90,70% | Innovador | 16 | 20 | | | | 80,00% | 80,00% |
| | | | Avanzado | 19 | 25 | | | 76,00% | 76,00% | 76,00% |
| | | | Intermedio | 37 | 39 | | 94,87% | 94,87% | 94,87% | |
| | | | Evolucionado | 33 | 39 | 84,62% | 84,62% | 84,62% | | |
| | | | Base | 47 | 51 | 92,16% | 92,16% | | | |
| Gestión de Proveedores TI | Intermedio | 57,89% | Innovador | 3 | 6 | | | | 50,00% | 50,00% |
| | | | Avanzado | 2 | 7 | | | 28,57% | 28,57% | 28,57% |
| | | | Intermedio | 5 | 9 | | 55,56% | 55,56% | 55,56% | |
| | | | Evolucionado | 9 | 13 | 69,23% | 69,23% | 69,23% | | |
| | | | Base | 8 | 16 | 50,00% | 50,00% | | | |
| Gestión de Incidencias de Ciber Ataques y Resilencia | Intermedio | 37,93% | Innovador | 2 | 10 | | | | 20,00% | 20,00% |
| | | | Avanzado | 4 | 15 | | | 26,67% | 26,67% | 26,67% |
| | | | Intermedio | 5 | 21 | | 23,81% | 23,81% | 23,81% | |
| | | | Evolucionado | 8 | 20 | 40,00% | 40,00% | 40,00% | | |
| | | | Base | 9 | 17 | 52,94% | 52,94% | | | |

Coopeuch

# Principales Ventajas

Establece un proceso estratégico para gestionar riesgos y controles de ciberseguridad que son necesarios o que necesitan mejora y acciones a tomar para lograr el estado deseado.

Planificación de Inversiones y Gastos en Ciberseguridad alineados al perfil de Riesgo de la Institución.

Objetividad que facilita identificar los factores que contribuyen a determinar el riesgo global en ciberseguridad.

Evaluar si la preparación de ciberseguridad está alineada con el desarrollo de la estrategia presente y futura del negocio y sus riesgos inherentes.

Coopeuch

# PILARES DE LA ESTRATEGIA DE NUESTRO PLAN DE CIBER SEGURIDAD

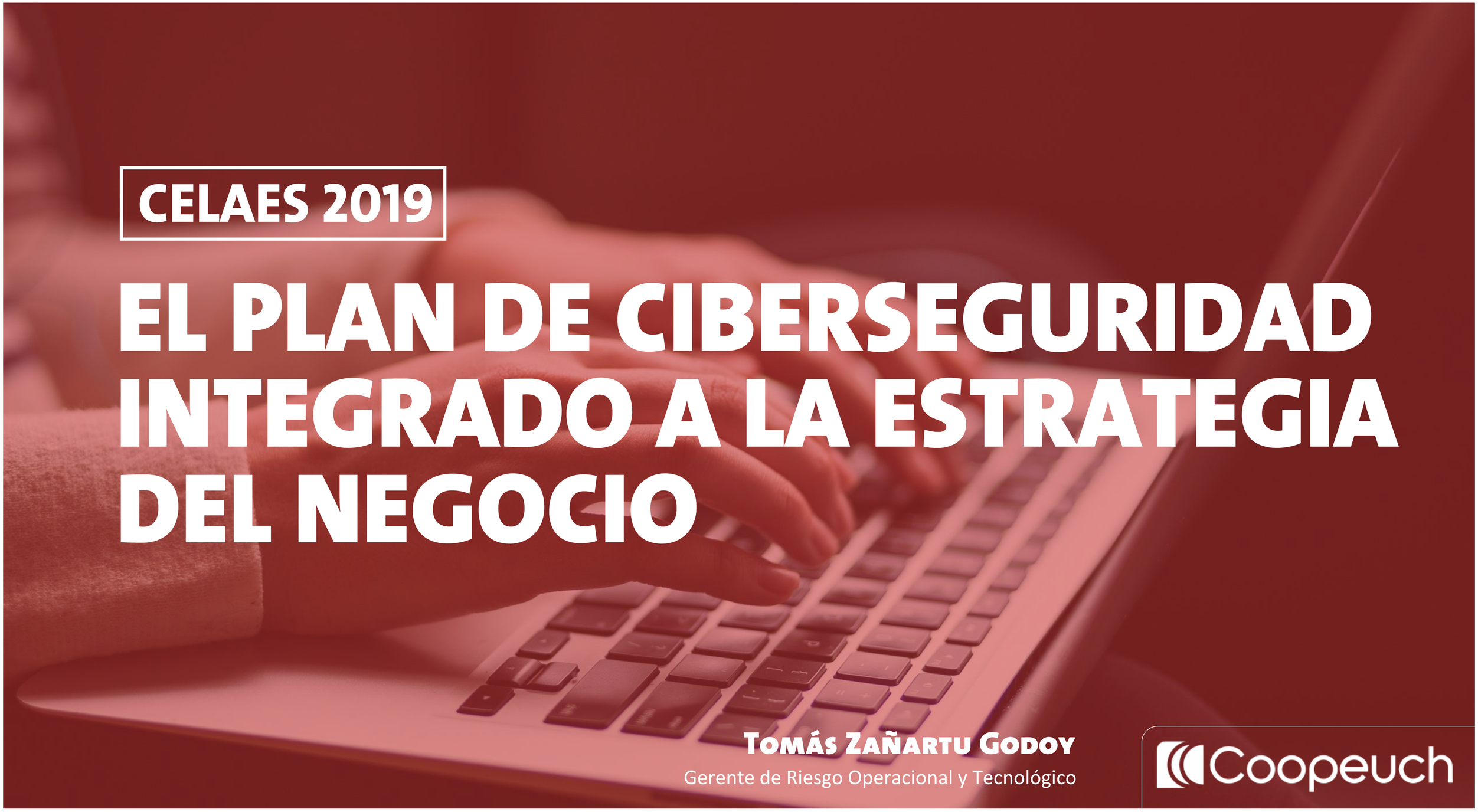

Coopeuch

# ES UN PROCESO CONTINUO


Coopeuch

Coopeuch

# GRACIAS



CELAES 2019

# EL PLAN DE CIBERSEGURIDAD INTEGRADO A LA ESTRATEGIA DEL NEGOCIO

**Tomás Zañartu Godoy**
Gerente de Riesgo Operacional y Tecnológico

Coopeuch