CASO CHALLENGERS 2026

Personas mayores, Ciberseguridad y Educación Financiera en Chile

(1) Contexto país

Chile está viviendo un proceso de envejecimiento poblacional acelerado. De acuerdo con los primeros resultados del Censo 2024, las personas de 65 años o más representan el 14,0% de la población del país, mientras que el índice de envejecimiento llegó a 79 personas de 65 años o más por cada 100 menores de 15 años. Esta tendencia confirma que el país ya no puede pensar en el envejecimiento como un desafío de largo plazo, sino como una realidad presente.

Al mismo tiempo, Chile ha avanzado de manera significativa en digitalización. Cada vez más personas realizan pagos, transferencias, compras, reservas de atención, consultas y trámites por medios electrónicos. En el sistema financiero, el acceso es muy alto: la Comisión para el Mercado Financiero (CMF) ha señalado que entre 97% y 98% de las personas mayores de 15 años tiene al menos un producto financiero, y BancoEstado informa que hay más de 15 millones de clientes con CuentaRUT, equivalentes al 87,2% de los habitantes de Chile mayores de 14 años.

Sin embargo, acceso no significa uso seguro ni comprensión suficiente. La CMF reporta que, aunque la conectividad digital del país es alta, el uso de herramientas financieras digitales cae con fuerza en los grupos de mayor edad. Solo 29% de los adultos mayores declara usar el celular para hacer o recibir pagos, y 54% señala que las transacciones financieras por internet pueden resultar difíciles o confusas.

Por otro lado, y con el rápido avance de la Inteligencia Artificial, hoy es más fácil crear mensajes, audios, imágenes o videos que parecen reales y confiables. Chile es uno de los países más avanzados de América Latina en este tema: el Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025 lo ubica entre los líderes regionales, y además registra 85 empresas de IA en el país. Al mismo tiempo, el uso de esta tecnología ya es cotidiano: en Chile, 60% de las personas dice usar inteligencia artificial en su vida diaria, y entre 2024 y 2025 ese uso aumentó en 12 puntos porcentuales.

En ese contexto, muchas personas mayores no cuentan con las herramientas necesarias para detectar un engaño, verificar si una solicitud es verdadera, proteger sus claves o comprender bien las consecuencias financieras de una acción digital.

Este escenario se vuelve más relevante porque Chile también ha fortalecido su institucionalidad en la materia. La Ley Marco de Ciberseguridad (Ley 21.663) fue promulgada el 26 de marzo de 2024 y publicada el 8 de abril de 2024, estableciendo una normativa general para enfrentar incidentes de ciberseguridad y proteger un ciberespacio más seguro. Además, desde enero de 2025 comenzó la actividad de la Agencia Nacional de Ciberseguridad. A ello se suma la Ley 21.719, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Esta ley distingue entre dato personal y dato personal sensible: el segundo incluye, entre otros, datos sobre salud, biometría, situación socioeconómica, creencias religiosas, afiliación política, orientación sexual e identidad de género. En este caso, esta definición es relevante porque muchas personas comparten datos que consideran inocuos, pero que legalmente son personales o sensibles, o que permiten ser identificadas y vulneradas.

En paralelo, el país ha comenzado a impulsar respuestas específicas para personas mayores. Al respecto, el Servicio Nacional del Adulto Mayor (SENAMA) publicó la Estrategia Nacional de Inclusión Digital para Personas Mayores 2025-2035, y la Subsecretaría de Telecomunicaciones (SUBTEL) junto a otras instituciones ha difundido campañas preventivas frente a fraudes digitales orientadas a este grupo.

(2) Problemática

En Chile, una parte importante de las personas mayores enfrenta una combinación compleja de riesgos asociados a la digitalización y la ciberseguridad (anexo 7 y 8). Por un lado, deben relacionarse con un entorno financiero cada vez más digitalizado: bancos, cuentas, transferencias, pagos, bonos, reservas médicas, plataformas públicas, comercio electrónico y comunicaciones institucionales se gestionan crecientemente mediante celulares, aplicaciones, páginas web y mensajería.

Por eso, la problemática no se limita a "usar tecnología". El problema central es el siguiente: Las personas mayores en Chile están expuestas a mayores riesgos de errores, estafas y engaños, en un mundo donde los servicios y trámites se digitalizan más rápido que el desarrollo de las capacidades de usarlas de forma segura.

La evidencia reciente sugiere que esta vulnerabilidad es real. En noviembre de 2025, la CMF alertó sobre un aumento de estafas de suplantación de identidad de instituciones y empresas, y de sus funcionarios, mediante llamadas telefónicas, correos electrónicos, documentos y

visitas a domicilio, señalando incluso un "incremento inusual" de consultas asociadas a este tipo de engaños.

Además, el problema no es solo de seguridad digital, sino también de educación. La inclusión financiera, según la CMF, no depende únicamente de tener acceso a un producto, sino también de su uso y calidad, junto con la capacidad de comprender sus beneficios y riesgos. En este sentido, la propia CMF destaca que la educación financiera ayuda a evitar fraudes, costos innecesarios y mal uso de productos financieros.

Dentro de las situaciones, aparecen las siguientes:

- Recepción de llamadas, mensajes o correos que solicitan datos personales, claves, códigos o acciones financieras inmediatas;
- Uso de aplicaciones, sitios web o enlaces falsos que imitan a instituciones legítimas;
- Decisiones de compartir información personal o financiera sin plena conciencia de sus consecuencias; y
- Transferencias o pagos realizados bajo presión, confusión o falsa validación institucional.

(3) Desafío y objetivos a resolver

¿Cuál es el desafío?

Como equipo participante, su misión es diseñar una propuesta concreta que ayude a las personas mayores en Chile a prevenir, identificar y enfrentar situaciones de riesgo digital y financiero en su vida cotidiana. Esto incluye situaciones como recibir llamadas, mensajes o correos que les solicitan datos personales o acciones financieras; encontrarse con aplicaciones, sitios web o enlaces falsos que imitan a instituciones reales; y tomar decisiones de compartir información personal o financiera sin comprender del todo las consecuencias que eso puede tener.

¿En qué situaciones pueden enfocarse?

No es necesario que su propuesta resuelva todos los riesgos al mismo tiempo. Pueden elegir uno o más de los siguientes focos (o buscar otros de su interés):

- Tipos de estafas y riesgos vigentes que afectan a personas mayores
- Decisiones de auto vulneración frecuentes que toman personas mayores

Existen un gran número de problemáticas a las que se enfrenta este segmento y puedes encontrar inspiración en los anexos 6 y 7 de este caso. La clave está en que su propuesta sea específica: mientras más claro sea el problema que están resolviendo y para quién lo están resolviendo, más sólida será su propuesta.

¿Qué se espera que logre su propuesta?

Su propuesta debe explicar claramente qué cambio concreto busca generar en las personas mayores. Al presentarla, deben ser capaces de responder estas preguntas:

• ¿Qué problema específico resuelve? Por ejemplo: reducir la probabilidad de que una persona mayor entregue su clave bancaria ante una llamada falsa.

• ¿Es posible de llevar a la práctica? (Viabilidad) Es decir, ¿puede implementarse con los recursos disponibles, sin depender de tecnología o condiciones inalcanzables?

• ¿Podría crecer o replicarse? (Escalabilidad) Por ejemplo, ¿funcionaría no solo en un barrio o ciudad, sino que podría aplicarse en otros lugares del país?

- ¿Cómo sabrían si está funcionando? (Medible) Deben proponer al menos una forma de medir si su solución está teniendo el efecto esperado. Por ejemplo: reducción de consultas por estafas, encuestas de confianza digital, entre otras.

¿Qué tipo de propuesta pueden presentar?

Su solución puede tomar distintas formas: un servicio, una herramienta digital, un programa educativo, una campaña de difusión, una intervención comunitaria u otro formato que estimen adecuado. No es obligatorio que el usuario de la solución sean las personas mayores, ni que sea una idea completamente nueva.

No se considerarán las propuestas que apunten a una política pública que requiera intervención estatal.

No hay una única respuesta correcta. Lo importante es que sea concreta, esté dirigida a mejorar la calidad de vida y disminuir los riesgos que la era digital puede implicar en personas mayores, y sea coherente con el presupuesto disponible (ver punto 4).

Para inspirarse, en los Anexos 8 y 9 encontrarán ejemplos de soluciones que ya existen en otros países y en Chile, junto con aprendizajes que pueden servirles como punto de partida. No se trata de copiarlas, sino de entenderlas y preguntarse: ¿cómo podríamos mejorarlas, adaptarlas o innovar a partir de ellas para el contexto chileno?

La propuesta no debe limitarse a la entrega de información general o consejos financieros aislados, sino que debe integrarse a situaciones concretas de uso digital y toma de decisiones.

Recuerden: una buena propuesta no tiene que ser perfecta ni tecnológicamente sofisticada. Tiene que ser clara, fundamentada y demostrar que entendieron el problema que están intentando resolver.

(4) Restricción presupuestaria del caso

Para este caso, se establece que los alumnos contarán con un presupuesto máximo de:

CLP 30.000.000

Con ese monto deberán financiar todas las acciones incluidas en su propuesta.

RÚBRICA

RÚBRICA DE EVALUACIÓN — CHALLENGERS 2026 *Personas mayores, Ciberseguridad y Educación Financiera en Chile*			
Criterio	**✓ Logrado** **(La propuesta cumple claramente con este criterio)**	**~ En desarrollo** **(La propuesta aborda el criterio, pero de forma parcial o poco precisa)**	**✗ Por desarrollar** **(La propuesta no aborda el criterio o lo hace de manera muy general)**
1. Comprensión del problema	El equipo identifica con claridad el problema central: las personas mayores enfrentan riesgos digitales y financieros en un entorno que se digitaliza más rápido que su capacidad de usarlo con seguridad. Explica a qué situación específica de riesgo se enfoca (por ej., llamadas fraudulentas, enlaces falsos o compartir datos sin conciencia) y fundamenta por qué ese problema es relevante.	El equipo menciona el problema general, pero no precisa en qué situación específica se enfoca o no justifica por qué la eligió. El problema se entiende, pero falta concreción.	El equipo describe el tema de forma muy amplia o confusa, sin distinguir claramente cuál es el problema que busca resolver ni para quién.
2. Propuesta concreta y pertinente	La propuesta describe con precisión qué es la solución, cómo funciona y cómo ayuda a personas mayores a prevenir, identificar o enfrentar el riesgo elegido. Es específica (no una idea general) y está claramente dirigida al grupo objetivo.	La propuesta existe y apunta en la dirección correcta, pero su descripción es vaga: no queda claro cómo funciona en la práctica o de qué manera concreta ayuda a las personas mayores.	La propuesta es demasiado genérica, no está dirigida a personas mayores, o no se distingue de soluciones ya existentes sin agregar ninguna mejora o adaptación al contexto chileno.
3. Viabilidad e implementación	El equipo demuestra que la propuesta puede llevarse a la práctica: explica cómo se implementaría, qué recursos requiere y cómo se ajusta al presupuesto disponible de $30.000.000. Considera además si la solución podría replicarse en otros lugares o escalarse en el tiempo.	La propuesta parece posible de implementar, pero el equipo no detalla cómo se llevaría a cabo ni verifica su coherencia con el presupuesto disponible. La escalabilidad no se aborda o se menciona solo de forma superficial.	La propuesta no considera su implementación práctica, excede claramente el presupuesto disponible o depende de condiciones que no son alcanzables en el contexto del concurso.
4. Resultados esperados y medición	El equipo explica qué cambio concreto busca generar en las personas mayores (por ej., reducir la entrega de claves ante llamadas falsas) y propone al menos una forma de saber si la solución está funcionando (por ej., , encuestas de confianza digital, reducción de consultas por estafas).	El equipo menciona que espera un impacto positivo, pero no lo precisa ni propone una forma concreta de medirlo. El resultado queda expresado de forma genérica (por ej., "las personas mayores estarán más seguras").	El equipo no define qué resultado espera lograr o no considera ninguna forma de evaluar si la propuesta tiene el efecto deseado.
Nota: Esta rúbrica tiene un propósito orientador. Los cuatro criterios tienen igual peso (25% cada uno). Su objetivo es ayudarte a entender qué se espera de tu propuesta, no servir como pauta rígida de corrección.			

ANEXOS

A continuación, se presentan una serie de Anexos estadísticos, como apoyo a la construcción de la propuesta, pero los alumnos pueden buscar más antecedentes para complementarlo, mientras provengan de fuentes respaldadas.

Anexo 1. Envejecimiento de la población en Chile

Indicador	Dato
Población censada en Chile (Censo 2024)	18.480.432
Personas de 65 años o más	14,0% de la población
Índice de envejecimiento 2024	79 personas de 65+ por cada 100 menores de 15
Regiones con mayor índice de envejecimiento	Valparaíso (98,6) y Ñuble (97,6)

Fuente: INE, primeros resultados Censo 2024.

Anexo 2. Inclusión financiera y acceso al sistema

Indicador	Dato
Personas mayores de 15 años con al menos un producto financiero	97%–98%
Clientes con CuentaRUT	más de 15 millones
Cobertura de CuentaRUT sobre población mayor de 14 años	87,2%

Fuente: CMF y BancoEstado.

Anexo 3. Brechas en uso digital financiero en personas mayores

Indicador	Dato
Personas mayores que usan celular para hacer o recibir pagos	29%
Personas mayores que consideran difíciles o confusas las transacciones financieras por internet	54%

Fuente: CMF, Oferta y demanda de servicios financieros digitales en Chile.

Anexo 4. Marco institucional y protección de datos

Elemento	Situación
Ley Marco de Ciberseguridad	Ley 21.663
Nueva ley de protección de datos personales	Ley 21.719
Agencia de Protección de Datos Personales	Creada por Ley 21.719
Estrategia Nacional de Inclusión Digital para Personas Mayores	2025-2035

Fuente: BCN y SENAMA.

Anexo 5. Qué entiende la ley chilena por dato personal y dato sensible

Concepto	Definición resumida
Dato personal	Información vinculada o referida a una persona natural identificada o identificable.
Dato personal sensible	Datos sobre salud, biometría, situación socioeconómica, creencias religiosas, afiliación política, orientación sexual, identidad de género, entre otros.
Implicancia para este caso	Información que parece cotidiana puede exponer identidad, patrimonio, intimidad o seguridad.

Fuente: Ley 21.719 y Biblioteca del Congreso Nacional.

Anexo 6. Tipos de estafas y riesgos vigentes relevantes para el caso

Tipo de estafa o riesgo	Cómo opera	Referencia
Phishing	Correo o mensaje que busca que la persona entregue datos o haga clic en enlaces maliciosos.	CSIRT
Smishing	Variante del phishing por SMS o mensajería móvil.	CSIRT
Vishing	Llamada telefónica destinada a extraer información o inducir acciones.	CSIRT
Créditos falsos	Entidades aparentan estar reguladas y exigen pagos previos por préstamos que no entregan.	CMF
Plataformas de inversión no reguladas	Ofrecen inversiones por internet o redes sociales sin supervisión.	CMF
Suplantación institucional	Delincuentes se hacen pasar por una entidad legítima mediante correos, llamados, documentos o visitas.	CMF

Fuente: CSIRT y CMF.

Anexo 7. Decisiones de auto vulneración frecuentes

Conducta	Dato o activo expuesto	Riesgo principal
Enviar foto de cédula por WhatsApp o redes a desconocidos	Identidad y dato personal	Suplantación o validación fraudulenta
Compartir cartolas, saldos o comprobantes con terceros no verificados	Datos financieros y patrimoniales	Exposición de cuentas y movimientos
Entregar claves, PIN o códigos SMS por teléfono	Credenciales críticas	Toma de control de cuentas y transferencias
Aceptar ayuda de terceros no confiables para usar apps o banca	Acceso indirecto a cuentas	Abuso o fraude sin trazabilidad
Hacer clic en enlaces urgentes sin verificar remitente	Dispositivo y credenciales	Robo de datos o instalación de malware
Reutilizar la misma clave en varios servicios	Múltiples cuentas	Compromiso en cadena ante una filtración

Fuente: Ley 21.719, CSIRT y alertas de la CMF.

Anexo 8. Benchmark de soluciones

Solución	Enfoque principal	Aprendizaje útil
Take Five to Stop Fraud	Pausa y verificación antes de enviar dinero o compartir información.	Diseño conductual para frenar decisiones impulsivas.
Confirmation of Payee	Validación del nombre del destinatario antes de transferir.	Rediseño del proceso para prevenir error o fraude.
SeniorShield.ai	Alertas, educación y revisión de mensajes sospechosos.	Apoyo continuo y prevención personalizada.
Campaña SUBTEL-SENAMA	Difusión y alfabetización digital para personas mayores.	Cobertura amplia, pero menor personalización.

Fuente: Take Five, Australian Payments Plus, SeniorShield.ai, SUBTEL y SENAMA.

Anexo 9. Benchmark para inspirar innovación

Los grupos deben revisar referencias existentes y luego proponer una mejora, adaptación o innovación sobre ellas.

Referencia	Cómo funciona	Aprendizaje para innovar
Take Five to Stop Fraud (Reino Unido)	Campaña nacional liderada por UK Finance que promueve una pausa deliberada ante solicitudes de dinero o información: Stop, Challenge, Protect.	Intervención conductual simple en el momento de riesgo; útil para pensar soluciones de pausa, verificación y autocontrol.
Confirmation of Payee (Australia)	Servicio interbancario que verifica si el nombre del destinatario coincide con los datos de la cuenta antes de transferir.	Rediseño del proceso para prevenir error o fraude antes del pago; útil para pensar validaciones y fricciones inteligentes.
SeniorShield.ai (Estados Unidos)	Aplicación orientada a personas mayores y cuidadores que ofrece alertas, educación y revisión de mensajes sospechosos.	Combina prevención, educación y apoyo en tiempo real; útil para pensar acompañamiento y protección continua.
Campaña SUBTEL-SENAMA (Chile)	Cápsulas y material educativo para disminuir estafas digitales a personas mayores.	Referencia local de difusión y alfabetización, útil como punto de partida, no como solución final.

Fuentes de referencia utilizadas para esta versión

- Biblioteca del Congreso Nacional (Ley 21.719 y Ley 21.663).
- CMF: inclusión financiera, servicios financieros digitales y alertas públicas.
- INE: Censo 2024.
- SENAMA: Estrategia Nacional de Inclusión Digital para Personas Mayores 2025-2035.
- CENIA/CEPAL (ILIA 2025), PwC Chile, Take Five to Stop Fraud, Australian Payments Plus y SeniorShield.ai.