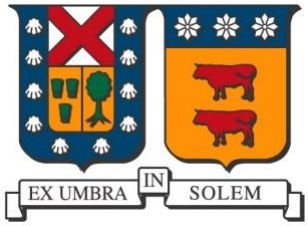
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



"GUÍA METODOLÓGICA DE GESTIÓN DEL CAMBIO PARA LA MEJORA CONTINUA EN LA AUTENTICACIÓN DE CANALES DE ATENCIÓN EN MESAS DE SERVICIO TI (GCAMTI)"

FELIPE ABARCA HUERTA

TESINA PARA OPTAR AL GRADO
DE MAGÍSTER EN TECNOLOGÍAS DE
LA INFORMACIÓN

Profesor Guía: JORGE OLIVARES

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☐ Memoria o trabajo de título X Tesis de Postgrado

Título del trabajo: Guía Metodológica de Gestión del Cambio para la mejora continua en la Autenticación de canales de atención en Mesas de servicio TI

(GCAMTI)

Nombre del candidato(a): Felipe Abarca Huerta

Carrera / Grado: Magister en Tecnologías de la Información

Campus: Vitacura **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Jorge Olivares, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

X El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por **(marcar una opción)**:

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 08-10-2026 **Firma:**

Estudiante o Candidato(a):

Fecha: 08-10-2026 **Firma:**

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Guía Metodológica de Gestión del Cambio para la mejora continua en la Autenticación de canales de atención en Mesas de servicio TI (GCAMTI)

Felipe Abarca Huerta
GTD
Calle Moneda 920, Santiago, Región Metropolitana

fabarcah@grupogtd.com

Resumen: La propuesta aborda la problemática de seguridad en la autenticación de canales de comunicación en mesas de servicio de tecnologías de la información (TI), a raíz de un incidente de ransomware que afectó una empresa de este rubro. El problema se contextualiza en el creciente riesgo de ciberataques y la necesidad de transformación cultural en la atención de tickets para garantizar la seguridad de los clientes y preservar la reputación de la empresa como proveedor confiable.
La solución propuesta se centra en la implementación de una guía metodológica de gestión del cambio basado en el ciclo PDCA con enfoque evolutivo y adaptabilidad a diferentes contextos, la que considera establecer niveles de desarrollo (modelo de madurez, de elaboración propia) que se aplicará a los distintos canales de comunicación que tienen los clientes para contactar. Se aborda inicialmente una autenticación multifactor manual por los agentes, focalizada en el correo electrónico y gestionando riesgos de los otros canales, con la visión de avanzar hacia la automatización total, preferiblemente a través del portal de autoatención. Se destaca la importancia de contar con un plan de gestión del cambio para abordar posibles resistencias.
La guía será evaluada mediante el juicio de expertos complementada con la observación cualitativa de los resultados obtenidos.
El objetivo es mejorar y fortalecer la seguridad en la atención de tickets, sin comprometer los tiempos de respuesta y preservando la reputación de la empresa, resultando en un cambio en el procedimiento de atención, ajustándose a las políticas internas de seguridad de la compañía y visibilizando la necesidad de seguir en constante evolución hasta lograr contar con un desarrollo totalmente automatizado y tecnológico. Además de mejorar la experiencia y satisfacción del cliente.

Palabras Clave: Ciberseguridad, PDCA (mejora continua), Gestión del Cambio, Mesa de servicio, Autenticación

1. Introducción

1.1. Contexto, motivación y problemática

En el contexto actual de creciente amenaza de los ciberataques, un reciente ataque de ransomware a una empresa de servicios TI ha puesto de relieve la necesidad de revisar y actualizar todos sus procesos y procedimientos de negocio. Este incidente, que provocó la pérdida de datos sensibles y la interrupción de los servicios, ha puesto en riesgo la confianza de los clientes y la reputación de la empresa.
Uno de los procesos que requiere una atención especial es el de creación de tickets. Este proceso, que permite a los clientes solicitar asistencia técnica, presenta vulnerabilidades que podrían ser explotadas por los atacantes. Dado que por este hecho se ha experimentado un aumento en las solicitudes de clientes relacionadas a la misma temática, seguridad, es necesario validar la identidad del solicitante para evitar suplantación de identidad y no volver a verse involucrado, directa o indirectamente, en un evento de esta envergadura. En la situación actual de la empresa, se hace necesario abordar las brechas de seguridad identificadas, siendo los canales de contacto fundamentales en la comunicación con los clientes es necesario mantenerlos con un nivel de seguridad adecuado.

1.2. Definición del problema

En concreto, el problema central en la empresa de estudio radica en la falta de control en la creación de tickets de requerimiento en la mesa de servicio, donde la ausencia de un código obligatorio y la accesibilidad a datos públicos como el RUT o la IP permiten que actores malintencionados soliciten modificaciones críticas, como accesos VPN sin superar una validación de identidad robusta, una vulnerabilidad agravada por un portal de clientes con baja seguridad y deficiente integración con el CRM. Cabe destacar que la decisión de robustecer estos canales no responde a una alta estadística de fraudes consumados en el registro histórico de la compañía, sino a un enfoque estrictamente proactivo y preventivo, bajo la premisa de que la baja incidencia de siniestros pasados no equivale a la ausencia de peligro. Por lo tanto, la implementación de esta guía metodológica de gestión del cambio para la autenticación se justifica como una acción estratégica indispensable para mitigar de raíz el riesgo latente de suplantación de identidad antes de que sea explotado por agentes maliciosos, garantizando que la operación diaria se alinee de forma rigurosa con los nuevos estándares de cumplimiento y gobernanza corporativa de la organización.

1.3. Resumen de la propuesta de solución

La propuesta de solución se fundamenta en la metodología PDCA (Plan-Do-Check-Act) aplicada a la gestión del cambio en la mesa de servicio TI, considerando como eje central la triada de personas, procesos y tecnologías. El enfoque busca fortalecer los canales de atención bajo criterios de autenticación y seguridad, de manera que los usuarios dispongan de mecanismos confiables para la generación y gestión de solicitudes, reduciendo riesgos asociados a brechas de control e incrementando la eficiencia operativa.

La guía se estructura como un proceso iterativo estructurado en las fases del ciclo PDCA, donde en cada etapa se abordan acciones específicas sobre las personas (capacitación, concientización y cultura organizacional), los procesos (estandarización, documentación y mejora continua) y las tecnologías (herramientas de ticketing, autenticación, seguridad y monitoreo). Esta integración permite no solo implementar controles técnicos, sino también consolidar una cultura organizacional enfocada en la mejora continua.

Los objetivos que persigue la propuesta son proporcionar un marco de gestión del cambio que permita fortalecer la autenticación y seguridad en los canales de atención de la mesa de servicio TI, alineando a las personas, procesos y tecnologías bajo un modelo unificado, asegurando trazabilidad y confianza en la operación, implementando un esquema de mejora continua que permita la evolución progresiva del modelo hacia mayores niveles de madurez.

Además, el proyecto tiene como objetivo optimizar los procesos internos. Se busca implementar una guía de gestión del cambio que permita adaptar el proceso a las políticas internas de seguridad que promueve la organización de manera gradual y efectiva. Esto implica una comunicación clara y transparente con todos los involucrados, así como la capacitación del personal en los nuevos procedimientos.

A largo plazo, se vislumbra un escenario donde la gestión de solicitudes sea completamente automatizada. La implementación de tecnologías avanzadas permitirá agilizar los procesos, reducir errores y mejorar la satisfacción del cliente. Sin embargo, es importante destacar que la automatización no sustituirá la interacción humana por completo, sino que complementará el trabajo de los agentes, permitiéndoles enfocarse en tareas de mayor complejidad y valor para la organización.

El marco teórico adoptado se basa en tres aspectos principales:

- Gestión del cambio organizacional, entendida como la capacidad de movilizar a las personas y los procesos hacia nuevas prácticas sostenibles en el tiempo, con énfasis en los pilares de la triada persona–proceso–tecnología como elementos inseparables.
- Ciclo PDCA o ciclo de Deming, utilizado como metodología de mejora continua que asegura la implementación ordenada, la verificación de resultados y la aplicación sistemática de mejoras.

- Ciberseguridad, entendida como el conjunto de principios, prácticas y controles destinados a proteger la confidencialidad, integridad y disponibilidad de la información. En esta guía se vincula directamente con la necesidad de contar con canales de atención seguros, autenticación confiable y trazabilidad de las solicitudes, garantizando que los procesos tecnológicos estén alineados con estándares y normativas de seguridad.

Complementariamente, se incorpora la noción de niveles de madurez (básico, intermedio y avanzado), que permite ubicar a la organización en un punto de referencia inicial y proyectar su evolución en función de la aplicación de la guía.

1.4. Hipótesis

La aplicación de una guía metodológica de gestión del cambio basada en el ciclo PDCA sobre la tríada de Personas, Procesos y Tecnología, permite estructurar un modelo de autenticación para mesas de servicio TI de carácter holístico, evolutivo, flexible y escalable.

1.4.1. Variables independientes

Aplicación del ciclo PDCA sobre la tríada Personas, Procesos y Tecnología (Marco GCAMTI): Representa la intervención metodológica del estudio. Constituye la causa o mecanismo estructurado mediante el cual se orquestan las capacitaciones y la cultura organizacional (Personas), la estandarización y gobernanza de flujos (Procesos), y el despliegue de herramientas de autenticación (Tecnología) a lo largo de las fases de Planificación, Ejecución, Revisión y Mejora.

1.4.2. Variables dependientes

Las variables dependientes corresponden a los cuatro atributos metodológicos que se comprueban cualitativamente mediante la aplicación de la guía y la validación por juicio de expertos:

- Carácter Holístico: Grado de cobertura sistémica y articulación simultánea entre la cultura humana, los protocolos de atención y las herramientas tecnológicas, garantizando la ausencia de "puntos ciegos" en la gestión del cambio.
- Carácter Flexible: Capacidad de la guía para graduar los controles de autenticación según el nivel de riesgo de la solicitud y adaptarse a la realidad operativa de los distintos canales de atención sin generar fricción inaceptable en el usuario.
- Carácter Escalable: Capacidad del diseño modular de la guía para desplegarse desde un entorno piloto controlado hacia volúmenes masivos de atención sin degradar la disponibilidad ni la latencia del servicio.
- Carácter Evolutivo: Capacidad del modelo para aprender de los hallazgos operativos e incidentes de cada ciclo PDCA, incorporando ajustes dinámicos y madurando progresivamente hacia niveles superiores en la postura de ciberseguridad.

1.5. Metodología de prueba

Para la validación de la hipótesis de esta investigación, se ha optado por la metodología de "Juicio de Experto" complementada con la observación cualitativa de los resultados obtenidos.

Dado que el modelo es una propuesta de gestión del cambio en un entorno vivo, no solo la validación requiere complementar métricas cuantitativas con evaluación cualitativa, sino que requiere la evaluación de profesionales con autoridad y conocimiento técnico en las áreas críticas.

1.6. Estructura del informe

El documento se organiza secuencialmente en seis capítulos principales. El Capítulo 2 (Marco Teórico) y el Capítulo 3 (Estado de la Industria) establecen las bases conceptuales, los riesgos de suplantación en la nube, las soluciones de autenticación y su alineación con la Ley N° 21.663 de Chile y la gestión del cambio. El Capítulo 4 (Modelo Propuesto) y el Capítulo 5 (Aplicación de la Guía Metodológica) detallan el diseño holístico y la metodología operativa del modelo basado en el ciclo PDCA y la tríada personas, procesos y tecnología. Finalmente, el Capítulo 6 (Validación de la Guía Metodológica) evalúa el modelo mediante juicio de expertos, mientras que el Capítulo 7 (Conclusiones) sintetiza los hallazgos y valida la efectividad de la doble iteración.

2. Marco Teórico

Para entender técnicamente el tema sobre el modelo propuesto, es fundamental contar con varios conceptos del ámbito de tecnologías de la información, seguridad de la información y ciberseguridad, como los que se presentan a continuación:

- Ciberseguridad: Es la práctica de proteger equipos, redes, aplicaciones, sistemas críticos y datos de la organización ante posibles amenazas digitales, donde se utilizan medidas y herramientas con el fin de resguardar la información de acceso no autorizado e incluso evitar interrupción de las operaciones empresariales producto de una actividad de red no deseada [1]
- Zero Trust (Confianza Cero): Modelo de seguridad guiado por el principio "nunca confiar, siempre verificar". Elimina la confianza implícita asociada a estar dentro del perímetro de la red corporativa o usar un dispositivo de la empresa. Exige autenticación y autorización independientes para cada sujeto, dispositivo y sesión antes de conceder acceso a los recursos. [2]
- Mesa de servicio: Ente estratégico que actúa como punto de contacto e intermediario entre los usuarios, la organización y sus socios, gestionando y supervisando los servicios de TI. [3]
- Spoofing: De acuerdo con el glosario del Computer Security Resource Center del NIST (CSRC - NIST), el spoofing se define como la falsificación deliberada de identidad, direcciones de origen o datos digitales para acceder sin autorización o inducir a error a un usuario/sistema. Comprende modalidades como impersonating, masquerading, mimicking y piggybacking, agrupadas en dos vertientes: Measurement spoofing (Alteración/retardo de señales físicas) y Data spoofing (Inyección de datos falsos. [4]
- Autenticación: Proceso de verificación de la identidad de un usuario o dispositivo mediante credenciales (contraseñas, tokens de hardware, etc.) [5]
- Autenticación multifactor basada en riesgo: Evalúa el riesgo de cada intento de acceso en tiempo real y calcula una puntuación. A mayor probabilidad de compromiso, el sistema aplica un nivel de autenticación más estricto y restrictivo. [6]
- Ciclo Deming (PDCA): Metodología sistemática de planificación, ejecución, verificación y acción orientada a la calidad y la mejora continua institucional. [7]
- Portal de autoatención: Punto único de acceso (SPOA - Single Point of Access) que centraliza, organiza y distribuye información y conocimiento personalizado para facilitar la toma de decisiones rápida por parte del usuario. [8]
- Gestión del cambio: Enfoque integral, cíclico y estructurado diseñado para acompañar la transición de personas, equipos y organizaciones desde un estado actual hacia un estado futuro objetivo, garantizando los beneficios del negocio. [9]
- Modelo de madurez: El modelo de madurez en gestión de proyectos (Pennypacker & Grant, 2002) se define como un marco estructurado de mejora progresiva que permite evaluar el nivel actual de los procesos de una organización y trazar una ruta hacia su perfeccionamiento. Conceptualmente, opera bajo un enfoque bidimensional que integra áreas clave de conocimiento con los cinco niveles del Capability Maturity Model (CMM). Comienza en un Nivel 1 (Proceso inicial), caracterizado por la informalidad y la improvisación ad hoc; avanza hacia un Nivel 2 (Proceso estructurado), donde existen metodologías repetibles y documentadas pero de aplicación inconsistente; se consolida en un Nivel 3 (Normas organizativas), al formalizar e institucionalizar los estándares en toda la empresa; escala a un Nivel 4 (Proceso gestionado), apoyado en métricas de desempeño y valor ganado para tomar decisiones

estratégicas; y culmina en un Nivel 5 (Optimización del proceso), enfocado en la mejora continua y el aprendizaje sistémico mediante el análisis constante de datos. Este diagnóstico actúa como un punto de referencia (benchmark) frente a la industria. Sin embargo, su adopción presenta dos dinamismos críticos: por un lado, los procesos progresan a velocidades disímiles dentro de una misma organización, permitiendo la coexistencia de diferentes grados de madurez entre áreas; por otro lado, la madurez no es irreversible, por lo que, ante la falta de supervisión y mejora sostenida, los procesos corren el riesgo de degradarse y retroceder hacia niveles inferiores. [10][11]

3. Estado de la industria (estado del arte)

La evolución de los servicios de atención al cliente evidencia una transición hacia modelos CCaaS en la nube con funciones avanzadas de inteligencia artificial, análisis de datos y automatización, mercado dominado por proveedores clave evaluados en el Cuadrante Mágico de Gartner [12]. No obstante, la securitización de estos canales telemáticos es crítica; según el Digital Trust Survey 2023 de PwC, solo el 40% de las empresas se percibe totalmente protegida frente a ciberataques, identificando la suplantación de identidad como una amenaza directa [13]. Históricamente catalogados como el eslabón más débil, se proyectaba que el 75% de las organizaciones sufriría fraudes en sus Contact Centers [14]; vulnerabilidad que se ha sofisticado rápidamente, como confirma una encuesta global de Gartner (2025) donde el 62% de las empresas reportó ataques de deepfake por ingeniería social, además de incidentes en IA generativa (29%) y manipulación de peticiones (prompt injection) en asistentes virtuales (32%) [15].

Para contrarrestar estas brechas, el ámbito técnico se respalda en la publicación NIST SP 800-63B para la validación de identidades mediante niveles de confianza (AAL1 a AAL3) [16]. En el contexto local chileno, la promulgación de la Ley 21.663 (Ley Marco de Ciberseguridad) exige a los Operadores de Importancia Vital implementar Sistemas de Gestión de Seguridad de la Información (SGSI), notificar incidentes a la ANCI y asegurar la continuidad operacional, convirtiendo la auditabilidad de la mesa de servicio en un requisito legal imperativo [17]. Asimismo, el Cloud Native Maturity Model (CNMM v4.0) de la CNCF demuestra que la madurez tecnológica trasciende la acumulación de herramientas y radica en una capacidad adaptativa articulada en cinco pilares (negocio, personas, procesos, políticas y tecnología), promoviendo la seguridad desde etapas tempranas (shift-left) y la sostenibilidad operativa [18].

En conclusión, la literatura confirma que la ciberseguridad requiere integrar la tecnología con el factor humano y los procesos mediante el ciclo PDCA. A pesar de los avances en soluciones CCaaS, estándares como NIST, exigencias legales como la Ley 21.663 y marcos de madurez como el CNMM v4.0, persiste una brecha metodológica entre el fortalecimiento técnico y la gestión del cambio. Debido a que los puntos de contacto siguen siendo altamente vulnerables por su dependencia del factor humano, esta investigación propone un modelo integrador para alinear la rigurosidad técnica con la adopción cultural y la mejora continua en la mesa de servicio.

4. Propuesta de solución

La solución propuesta se materializa en la Guía Metodológica de Gestión del Cambio para la mejora continua en la Autenticación de canales de atención en Mesas de servicio TI (GCAMTI), un marco integral que articula la tríada personas, procesos y tecnología con el ciclo de mejora continua PDCA y la gestión estratégica de los canales de atención. Su propósito fundamental es guiar a la organización en la transición desde una ciberseguridad reactiva hacia un estado de resiliencia operativa eficiente, sostenible y plenamente alineada con los objetivos del negocio a través de una serie de características metodológicas clave. La guía metodológica se caracteriza por las siguientes características fundamentales:

- **Holístico:** Considera de manera sistémica los pilares de personas, procesos y tecnologías. Esta visión asegura que la transformación no se limite a una implementación técnica, sino que se sea incorporada

de forma sostenible en la cultura organizacional, garantizando la coherencia entre las herramientas utilizadas y el comportamiento humano.

- **Evolutivo:** Incorpora el ciclo PDCA (Plan-Do-Check-Act) para fomentar una cultura de mejora continua. Este enfoque permite que el modelo no sea estático, sino que aprenda de los incidentes y métricas de desempeño para adaptarse de forma dinámica a un panorama de amenazas en constante cambio.
- **Flexible:** Permite graduar la intensidad de los controles de autenticación en función del nivel de riesgo de cada solicitud y adaptarse a la realidad operativa de los diversos canales de atención. Esta cualidad facilita una transición gradual que minimiza la fricción con los usuarios, reduce la resistencia al cambio y ajusta los protocolos a las particularidades de la organización.
- **Escalable:** Posee una estructura modular diseñada para crecer de forma sostenida, permitiendo que el modelo sea desplegado progresivamente desde un entorno piloto controlado hacia operaciones transaccionales masivas, o adoptado por organizaciones de diversos tamaños y sectores sin comprometer la latencia, los acuerdos de nivel de servicio (SLA) ni la disponibilidad del sistema.

A continuación, se listan los componentes de la propuesta metodológica de la guía:

- Gestión del cambio
- Triada de pilares de aplicación del cambio
- Ciclo PDCA como metodología de mejora continua
- Canales de atención
- Niveles de desarrollo o niveles de madurez
- Roles participantes

Estos componentes se explican en las siguientes secciones.

4.1. Gestión del cambio

En el marco de la guía GCAMTI, la gestión del cambio se define como el conjunto estructurado de estrategias, metodologías y herramientas diseñado para guiar y acompañar a la organización y fundamentalmente a las personas, en la transición desde los métodos de autenticación tradicionales y vulnerables hacia un ecosistema de ciberseguridad robusto y resiliente.

Lejos de entenderse como un proceso puramente administrativo, en este modelo la gestión del cambio actúa como el puente indispensable entre la innovación técnica y la realidad operativa. Su propósito central es abordar el factor humano de manera proactiva, mitigando la resistencia natural ante nuevos controles, sensibilizando sobre los riesgos de ingeniería social y facilitando la adopción cultural de los nuevos protocolos. En definitiva, es la disciplina que garantiza que las soluciones tecnológicas no queden en la precariedad de un "parche técnico", sino que sean asimiladas de forma sostenible, convirtiendo la seguridad en un hábito operativo compartido y coordinado.

4.2. Triada de pilares de aplicación del cambio

La propuesta reconoce que la seguridad de la información es un esfuerzo multidisciplinario que debe equilibrar tres dimensiones:

- Personas Constituyen la "primera línea de defensa". Se enfoca en el desarrollo de competencias, la sensibilización sobre la ingeniería social y la claridad en roles y responsabilidades para asegurar el compromiso con los nuevos protocolos de autenticación.
- Procesos: Definen el "cómo" de la operación. Garantizan la estandarización, la gobernanza y la eficiencia en la atención de tickets, asegurando que cada interacción siga un flujo de trabajo validado y auditable.
- Tecnologías: Actúan como habilitadores estratégicos. Facilitan la automatización, la robustez en la autenticación (MFA) y proporcionan la trazabilidad necesaria para garantizar el no repudio y la integridad de la atención.

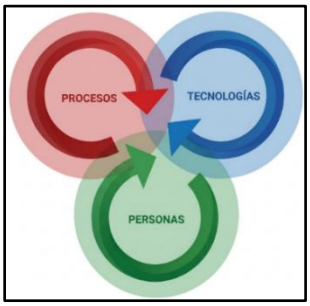


Figura 1: Triada gestión del cambio

La interacción coordinada de estas tres dimensiones es el fundamento para que el modelo propuesto se mantenga en el tiempo y pueda adaptarse a nuevas exigencias.

4.3. El ciclo PDCA como metodología de mejora continua

Para operativizar el modelo, se utiliza el ciclo de Deming, estructurando el cambio en fases iterativas:

- Planificar: definir los objetivos, alcances y lineamientos estratégicos.
- Hacer: ejecutar lo planificado en cada dimensión de la triada.
- Revisar: auditar, monitorear y evaluar los resultados obtenidos.
- Mejorar: Introducción de ajustes correctivos basados en los hallazgos de la fase anterior, preparando la organización para un nuevo ciclo de madurez superior.

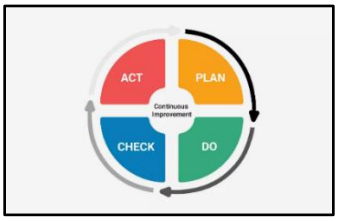


Figura 2: Ciclo PDCA

Es fundamental destacar que en la arquitectura de la guía GCAMTI, el ciclo PDCA no se concibe como una herramienta lineal o de aplicación única, sino bajo un enfoque de doble iteración estructural:

- PDCA de Diseño (Nivel Metodológico): Representa el ciclo iterativo aplicado durante la concepción y formulación de la guía. En esta fase, la propuesta teórica se somete a revisiones continuas frente a la realidad operativa de la empresa, permitiendo refinar y adaptar sus componentes antes de su versión final.
- PDCA de Aplicación (Nivel Operativo): Constituye el motor de ejecución continua una vez implementada la guía en la mesa de servicio. Es la dinámica que permite a la organización aprender de los incidentes, evaluar el desempeño de los canales de atención y adaptar los controles de autenticación de forma proactiva ante la evolución de las amenazas.

Este enfoque garantiza que el modelo no sea estático, sino que evolucione en función de la retroalimentación, los hallazgos y las necesidades emergentes.

4.4. Los canales de atención

Un eje central de la solución es la securitización de los vectores de entrada (correo, portal, teléfono, chat). La propuesta establece que cada canal debe estar sujeto a controles de gestión de identidad y acceso. El

fortalecimiento de estos canales reduce drásticamente la superficie de ataque frente a incidentes de identidad, convirtiendo la gestión de canales en un factor decisivo para la reputación de la empresa



Figura 3: Ejemplo de canales de atención

4.5. Los niveles de desarrollo o niveles de madurez

Inspirado en los modelos de madurez de capacidades (CMM), esta propuesta establece tres estados incrementales que permiten medir el progreso de la organización en la securitización de sus mesas de servicio:

- Nivel 1 – Inicial (Básico)
- Nivel 2 – Gestionado (Intermedio)
- Nivel 3 – Optimizado (Avanzado)

Cada uno de estos estados o niveles de desarrollo consideran los 3 pilares de la triada de gestión del cambio, con detalles específicos para la securitización de los canales de ingresos que ofrece la compañía a los clientes y cuyo punto de contacto es el call center.

Nivel 1 - Inicial (Básico): Se caracteriza por un enfoque reactivo y controles de seguridad ad-hoc.

- Personas: Nivel de concientización bajo; la seguridad depende de la voluntad individual del agente. Alta resistencia percibida ante nuevos controles.
- Procesos: Flujos manuales, poco documentados y no estandarizados. La gestión de identidades es informal.
- Tecnologías: Herramientas aisladas con funcionalidades limitadas; ausencia de una plataforma centralizada de autenticación.

Nivel 2 - Gestionado (Intermedio): Representa una transición hacia la estandarización y el compromiso organizacional.

- Personas: Programas de capacitación formal en marcha. Los empleados comprenden el riesgo y el valor de los nuevos procedimientos.
- Procesos: Procesos documentados y repetibles. Se establecen métricas básicas para medir el cumplimiento de los protocolos de seguridad.
- Tecnologías: Automatización parcial e integración de herramientas. Implementación de políticas de inversión tecnológica alineadas con la seguridad de la información.

Nivel 3 - Optimizado (Avanzado): Estado de madurez donde la seguridad y la mejora continua están institucionalizadas.

- Personas: Cultura de seguridad arraigada; el personal actúa proactivamente para identificar brechas (Cultura de "Firewall humano").
- Procesos: Flujos de trabajo altamente eficientes, adaptativos y basados en el riesgo, integrados totalmente con el ciclo PDCA.

- Tecnologías: Automatización integral bajo un enfoque de Zero Trust (Nunca confiar, siempre verificar). Uso de autenticación robusta y analítica de datos para la mejora del servicio.

4.6. Roles participantes

Adicionalmente a los componentes metodológicos y tecnológicos descritos, la correcta gobernanza de la guía GCAMTI requiere delimitar con precisión las responsabilidades de los actores clave que intervienen en el ciclo de vida de los requerimientos. En el proceso integral de atención y gestión de tickets, destacan de manera fundamental los siguientes roles:

- **Cliente (Usuario Solicitante):** Es el actor que gatilla el flujo operativo al manifestar una necesidad de soporte o modificación técnica. Su participación es activa tanto al definir los parámetros de su solicitud como al someterse a los controles de identidad. De acuerdo con el diseño flexible de la guía, el cliente posee la autonomía de canalizar su requerimiento interactuando con la primera línea de atención o, de forma óptima, autogestionar la creación de sus tickets de manera directa y centralizada a través del Portal de Clientes, omitiendo la intermediación humana.
- **Agente de Contact Center:** Constituye el primer punto de contacto y la línea de defensa inicial en la cadena de atención. Su función principal consiste en recibir de manera telemática la solicitud del cliente, aplicar rigurosamente los factores de autenticación dictados por la matriz dinámica según el nivel de riesgo, y registrar de forma estructurada el caso en la plataforma de mesa de servicio para su posterior escalamiento.
- **Ingeniero de Atención al Cliente (Resolutor):** Es el especialista encargado de asumir la propiedad técnica del ticket para su procesamiento final. Su labor comprende la ejecución y resolución definitiva de la solicitud siguiendo estrictos protocolos de seguridad y continuidad operativa. El ciclo concluye con un cierre formal del proceso, el cual se ejecuta obligatoriamente tras realizar una validación final con el usuario solicitante para garantizar el no repudio y resguardar la integridad del servicio entregado.

5. Explicación de la guía metodológica propuesta

El presente capítulo aborda la instrumentación práctica y el despliegue operativo de la guía metodológica GCAMTI, transformando los lineamientos teóricos y conceptuales previamente definidos en un marco de acción completamente ejecutable. Con el propósito de conducir a la organización hacia una autenticación robusta, segura y resiliente en sus canales de atención de mesas de servicio TI, a continuación, se describe la interacción de los componentes clave del modelo y su desarrollo estructurado bajo el enfoque de la mejora continua.

El desarrollo de la solución se basa en la metodología PDCA. Inicialmente, se realizará una planificación detallada para asegurar una implementación óptima del modelo propuesto. Esta planificación se centrará en los elementos clave que sustentan el modelo, como son los componentes mencionados en el capítulo anterior (Capítulo 4).

A partir de este punto, se iniciará un recorrido por cada una de las fases del ciclo PDCA: Plan, Do, Check y Act. En cada fase se abordarán sus componentes de manera sistemática, mostrando cómo se planifica, se ejecuta, se verifica y finalmente se mejoran los elementos críticos.

La estructura funciona como una guía: primero se presenta lo que se debe planificar, luego cómo se lleva a la práctica, posteriormente cómo se evalúan los resultados y finalmente cómo se aplican las mejoras. De esta manera, se asegura una comprensión clara del lugar en el que se encuentra el lector dentro del documento y de lo que viene a continuación: el desarrollo completo del modelo PDCA aplicado a la gestión de cambios en la mesa de servicios TI.



Figura 4: Niveles de madurez

La figura expone de manera macro la progresión secuencial que propone la guía GCAMTI para robustecer de forma sostenible la seguridad en los canales de atención de las mesas de servicio. A través de un eje ascendente marcado por el vector de "EVOLUCIÓN", el diagrama ilustra visualmente cómo una organización transita desde un estado de vulnerabilidad y control reactivo (Bajo Madurez – color rojo) hacia un ecosistema de alta resiliencia y proactividad (Alto Madurez – color verde), transformando simultáneamente las dimensiones de personas, procesos y tecnologías, que se puede corroborar en la figura de a continuación:

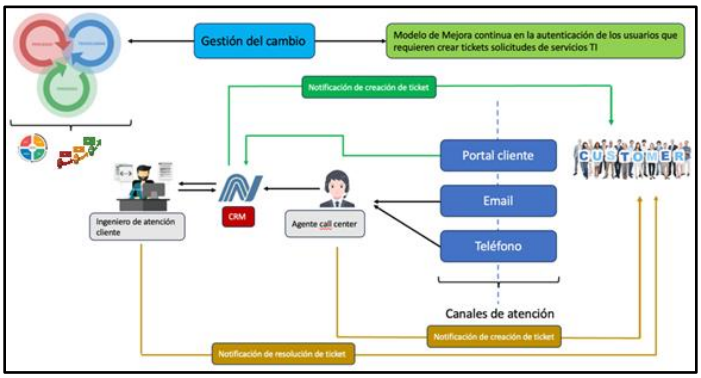


Figura 5: Propuesta de solución

La figura 5 ilustra la síntesis visual del modelo propuesto por la guía GCAMTI, representando gráficamente cómo se interconectan de manera sistémica y armónica todos los componentes descritos en los apartados anteriores.

El modelo se enmarca firmemente dentro del entorno operativo de las mesas de ayuda TI, cuyo dinamismo diario está definido por la interacción de roles claramente delimitados. En este ecosistema, el flujo transaccional se activa cuando el Cliente inicia el proceso solicitando un ticket de modificación a través de los canales habilitados; esta solicitud es recibida inmediatamente por el Agente de Contact Center, quien asume el rol de primera línea de defensa, atiende el requerimiento y lo registra formalmente en los sistemas de la organización. Finalmente, el caso es derivado al Ingeniero de Atención al Cliente, el especialista encargado de procesar, ejecutar y dar resolución definitiva al ticket técnico.

Lo que la guía GCAMTI busca es, precisamente, integrar este flujo operativo tradicional dentro de un modelo formal de gestión del cambio enfocado en la mejora continua. Para transformar esta operación, frecuentemente expuesta a vulnerabilidades de identidad, la guía no se limita a implementar soluciones técnicas aisladas, sino que potencia de forma simultánea e interconectada la tríada fundamental de Personas, Procesos y Tecnologías. Como se aprecia en el diagrama, esta integración no se produce de forma abrupta, sino a través de un proceso estrictamente evolutivo guiado por el ciclo de mejora continua (PDCA), el cual conduce de forma progresiva a la organización desde un estado de Bajo Madurez hasta el nivel más alto de resiliencia operativa (Alto Madurez) Es importante destacar que, dependiendo de la organización donde se aplique esta guía, cada aspecto sugerido puede variar, ya que las necesidades de cada entidad son diferentes. lo propuesto corresponde a una referencia metodológica adaptable al contexto organizacional.

5.1. PLANIFICAR (P de PLAN del PDCA)

El objetivo de la fase de "planificación" (PLAN del modelo PDCA o ciclo Deming) es diseñar y estructurar las acciones necesarias para implementar un modelo de gestión del cambio enfocado en la triada personas, procesos y tecnología. Esta fase contempla la identificación de los actores clave (personas), el levantamiento y análisis de los procesos actuales, así como la evaluación de las tecnologías existentes, especialmente aquellas relacionadas con la autenticación y seguridad en los canales de atención de la mesa de servicio TI.

5.1.1. Planificación respecto de las personas

Dentro de la guía GCAMTI, la dimensión de personas es el eje transversal que determina la efectividad de los controles técnicos y procedimentales. La planificación en esta etapa busca diagnosticar el estado actual del capital humano y diseñar las intervenciones necesarias para transitar hacia un esquema de seguridad proactiva.

5.1.1.1. Identificación y selección de stakeholders

La identificación de las partes interesadas es un proceso crítico para garantizar la adopción del modelo. Para asegurar que el modelo GCAMTI cubra todas las necesidades de seguridad y operatividad, la identificación de los interesados se puede realizar de la siguiente manera:

- Mapeo de la cadena de valor (Flujo del Ticket): Se identifican los actores que intervienen en el ciclo de vida de una solicitud, desde el Emisor (Cliente/Usuario), el Gestor (Agente de Mesa de Ayuda N1/N2), hasta el Aprobador (Supervisor o Dueño del Activo Crítico).
- Clasificación mediante matriz de poder: Se categoriza a los actores según su capacidad de influir en el proyecto y su nivel de interés en los resultados. Esto permite priorizar a los Stakeholders Clave (como el CISO y Gerentes de Operaciones) que requieren una gestión directa, de los Stakeholders Operativos que requieren formación y comunicación constante.
- Entrevistas de Diagnóstico: Se realizan consultas con los líderes de las áreas de Redes, Seguridad e Infraestructura para identificar dependencias técnicas y requisitos legales (ej. cumplimiento de PCI DSS o ISO 27001) que deban integrarse en el diseño de los controles.

Las partes interesadas identificadas, junto con sus roles en el modelo GCAMTI, niveles de poder e interés, y la correspondiente estrategia de gestión se detallan en el ANEXO 1.

5.1.1.2. Diagnóstico de competencias

Para establecer una línea base de capacidades, se planifican tipos de evaluaciones de diagnóstico que permiten identificar brechas de seguridad humana:

- Evaluación técnica: Evaluación del conocimiento y destreza en el uso de herramientas de gestión (ITSM) y mecanismos de seguridad (MFA, VPN). Se aplican pruebas de entorno controlado donde el técnico debe realizar un proceso de autenticación multifactor completo en un tiempo determinado, validando la correlación entre la identidad solicitada y el registro en el CRM.
- Evaluación psicológica: Análisis de la susceptibilidad ante vectores de ataque basados en la manipulación psicológica o urgencia fingida. Mediante el uso de test psicométricos y análisis de respuesta ante disparadores emocionales, se mide la probabilidad de que un agente ceda ante un cliente que simula una emergencia crítica para saltar protocolos de validación.
- Evaluación de riesgo conductual: Observación de la tendencia a utilizar "atajos" procedimentales en favor de la agilidad operativa o el cumplimiento de KPIs de tiempo. Se utiliza el método de "observación presencial o remota en tiempo real" para registrar cuántas veces el agente omite pasos obligatorios de seguridad con el fin de reducir el tiempo promedio de atención.

La pauta metodológica detallada, las rúbricas de evaluación técnica y la matriz de ponderación del riesgo conductual del personal de la Mesa de Ayuda se presentan en el ANEXO 2

5.1.1.3. Diseño del Programa de Formación y Entrenamiento Técnico

La planificación del entrenamiento se aleja de la capacitación genérica para enfocarse en el desarrollo de habilidades críticas de seguridad. El objetivo es garantizar que cada integrante de la Mesa de Ayuda sea capaz de operar el modelo GCAMTI con precisión técnica y conciencia del riesgo.

La metodología se puede definir de la siguiente forma:

- Técnica (Herramientas): Entrenamiento en el uso de plataformas MFA, motores de biometría de voz y flujos de validación en el ITSM (Jira/ServiceNow).
- Capacitación de Ciberseguridad Humana (Defensa): Técnicas de detección de ingeniería social, como phishing, vishing y manipulación psicológica.
- Normativa (Compliance): Alineación con estándares PCI DSS v4.0, ISO 27001 y la Ley de Ciberseguridad vigente.

A su vez, se considera segmentarla por roles:

- Agentes N1/N2: Enfoque en la ejecución operativa y protocolos de identidad.
- Supervisores/Líderes: Enfoque en la gestión de excepciones, auditoría de tickets "condicionales" y toma de decisiones ante crisis.
- Stakeholders Comerciales: Sesiones informativas sobre cómo comunicar los nuevos controles a los clientes para reducir la fricción.

En el ámbito pedagógico, las sesiones de entrenamiento pueden considerar diversas fórmulas, tales como:

- Ejercicios de simulación de roles: Simulaciones de llamadas reales donde un "atacante" intenta extraer información, obligando al agente a aplicar el protocolo de biometría.
- Laboratorios de herramientas: Sesiones prácticas en ambientes de prueba para dominar el uso del segundo factor de autenticación (OTP/App).
- Cápsulas de “Micro-learning”: Píldoras de video de 3 minutos para refuerzo semanal sobre vulnerabilidades críticas.

La malla curricular detallada, la carga horaria por módulo y la matriz de capacitación diferenciada por rol operacional se presentan en el ANEXO 3

5.1.1.4. Estrategia de comunicación transversal y plan de concientización

La planificación de la comunicación interna busca que el personal de la Mesa de Ayuda y las áreas de soporte, los gestores de cuentas de clientes y equipos comerciales compartan un mismo lenguaje de confianza y seguridad. Para lograrlo, se proyecta una estructura de mensajería segmentada que evite la saturación y garantice la relevancia de la información según el rol del receptor:

- Alineación operativa por niveles: Se definen mensajes diferenciados donde el nivel operativo se enfoca en el "cómo" a través de manuales de guiones y flujos de escalamiento; el nivel táctico se centra en el "control" mediante reportes de cumplimiento y gestión de excepciones; y el nivel estratégico prioriza el "valor", destacando la reducción de riesgos legales y el cumplimiento de normativas como ISO 27001.
- Canales de retroalimentación: Se planifica la creación de espacios de escucha técnica, como "Círculos de Seguridad", donde los agentes puedan reportar si un proceso es excesivamente lento o confuso antes del despliegue masivo, permitiendo ajustes ágiles en el diseño.

En cuanto a la dimensión externa, el éxito del modelo depende de que el cliente no perciba la autenticación reforzada como un obstáculo, sino como un beneficio directo para la protección de sus activos críticos. La estrategia externa se enfoca en educar al usuario antes de que ocurra la interacción:

- Campaña de seguridad compartida: Diseño de comunicados oficiales dirigidos a las contrapartes técnicas de los clientes, explicando que la implementación de biometría y MFA responde a estándares internacionales diseñados para prevenir el secuestro de información (Ransomware).
- Preparación del punto de contacto: Configuración de mensajes preventivos en el IVR de la central telefónica para advertir al usuario que se le solicitará validar su identidad, junto con la creación de plantillas de notificación que instruyan al cliente sobre cómo completar su validación de forma autónoma al abrir un ticket.

Finalmente, el plan de concientización busca transformar el entrenamiento técnico en un cambio de hábito organizacional, institucionalizando la verificación continua como un pilar cultural:

- Cápsulas de sensibilización y “storytelling”: Creación de contenidos breves que narren casos reales de suplantación de identidad en la industria y cómo el modelo GCAMTI los habría evitado, generando empatía y sentido de urgencia en el equipo.
- Refuerzo positivo: Establecimiento de un sistema de reconocimiento para aquellos agentes que detecten intentos de fraude o suplantación, incentivando el cumplimiento del protocolo por convicción profesional y no por temor a la sanción.
- Institucionalización en el “Onboarding”: Integración de la filosofía de seguridad desde el proceso de bienvenida de cualquier nuevo colaborador, asegurando que la cultura de "cero subjetividad" sea el estándar desde su primer día en la organización.

5.1.2. Planificación respecto de los procesos (procesos de atención de la mesa de ayuda TI)

La planificación de procesos en el modelo GCAMTI no se limita a la creación de manuales estáticos, sino que proyecta una reingeniería profunda del flujo de atención. El objetivo es garantizar que cada interacción, especialmente aquellas de alta criticidad, cuente con una validación de identidad técnica, automatizada y rastreable, minimizando la intervención del criterio humano en puntos críticos de control.

5.1.2.1. Diagnóstico Inicial de Procesos

Para que la planificación de la seguridad sea efectiva, es imperativo realizar un análisis sistemático de los flujos de trabajo vigentes. Este diagnóstico permite identificar vulnerabilidades operativas, ineficiencias en los tiempos de respuesta y brechas de cumplimiento normativo antes de la implementación de cualquier mejora técnica. El objetivo es establecer el estado actual (AS-IS) de la organización para contrastarlo con el estado deseado tras la ejecución del modelo

5.1.2.2. Diseño de la Matriz de Control

La pieza fundamental de la planificación es la creación de una matriz dinámica que vincule la criticidad de la solicitud con el factor de autenticación requerido. Esto evita el agotamiento operativo al no sobre-exigir controles en consultas de bajo riesgo, pero bloquea el paso en acciones que comprometan la infraestructura. La sugerencia de parámetros para la confección de la matriz es la siguiente:

- Definición de niveles de riesgo: Se categorizan las solicitudes en Riesgo Bajo (Consultas de estado), Riesgo Medio (Desbloqueo de cuentas estándar) y Riesgo Alto (Cambios de privilegios o acceso a servidores críticos).

- Asignación de factores de autenticación: Para riesgos bajos se planifica el uso de factores de conocimiento; para riesgos medios y altos se exige obligatoriamente factores de posesión (OTP) e inherencia (Biometría de voz), eliminando el uso de preguntas de seguridad manuales.
- Protocolo de excepciones: Se define un flujo formal para casos donde la tecnología de validación falle, obligando a una doble aprobación por parte de un supervisor y el registro de una justificación grabada en el ticket.
- Prioridad de Preferencia de Uso de Canales: Escala numérica estandarizada (de 1 a n) que indica la posición relativa del canal en orden de importancia y nivel de confianza institucional, donde 1 representa la máxima prioridad de atención.
- Aplicabilidad: Atributo binario (Sí o No) que valida si el canal y sus controles están técnicamente habilitados para su uso en la organización.
- Estado: Indicador de la condición operativa actual del canal y sus controles, clasificado en: "Operativo", "Por desarrollar" o "No Aplica".
- Controles de Autenticación: Listado de herramientas y metodologías de validación de identidad desplegadas en los canales (Autenticación Normal, Segundo Factor/OTP, Llamada Reversa, Palabra Clave, Correo Autorizado, N° Teléfono Autorizado, Cita Teams/Meet/Otro).
- Acción / Autorización: La consecuencia o tipo de requerimiento permitido que se habilita de forma estricta tras superar los controles de autenticación asociados.

La estructura integral de la Matriz de Control junto con la parametrización detallada de sus campos operacionales, canales de atención y reglas de decisión por nivel de riesgo, se presenta en el ANEXO 4

5.1.2.3. Reingeniería del Ciclo de Vida del Ticket (Workflow Seguros)

Esta etapa define el esquema de atención estructurado que guía el ciclo de vida de una solicitud. Se busca homogeneizar la atención y asegurar que la seguridad esté embebida en cada paso del flujo:

- Primer contacto y validación de Origen: Establecimiento de controles mínimos desde el ingreso de la solicitud para asegurar que el canal de origen es confiable.
- Generación de ticket y clasificación automática: Conversión de la solicitud en un registro formal donde, según su categoría, se aplican políticas de SLA y prioridad de forma inmediata.
- Ejecución del protocolo de identidad: Desarrollo de los pasos técnicos de resolución donde el sistema dispara las validaciones definidas en la MCA (OTP, Biometría) antes de permitir acciones en el sistema.
- Escalamiento y cierre con trazabilidad: Definición de rutas hacia personal especializado si el primer nivel no resuelve, finalizando con una comunicación formal al usuario y el registro inalterable de todo el proceso de validación en el expediente del ticket.

5.1.2.4. Priorización de canales y gestión de datos

La planificación establece una jerarquía de canales para incentivar el uso de aquellos que poseen controles de identidad nativos, protegiendo la integridad del ecosistema TI:

- Canal preferente y autoservicio: Se planifica el portal web como canal primario debido a su capacidad de integrar MFA desde el inicio de la sesión, reduciendo la carga de trabajo de los agentes humanos.
- Tecnificación del canal de Voz: Se proyecta un flujo de validación previo (IVR Seguro) donde el usuario sea autenticado antes de ser transferido al agente, eliminando la validación manual subjetiva.
- Saneamiento y calidad de datos en CRM: Para asegurar la efectividad de los procesos automáticos, se planifica una campaña de actualización de datos de contacto (teléfonos y correos de respaldo), evitando que información obsoleta bloquee el servicio al usuario legítimo.

5.1.2.5. Homologación y documentación de procesos

Para garantizar la continuidad operacional y la mejora continua, se planifica el registro formal de todo el conocimiento generado en las etapas anteriores:

- Manual de procedimientos Operativos de Identidad: Documentación detallada de los flujos, roles, tiempos, condiciones y excepciones, asegurando que el conocimiento esté disponible para todos los involucrados.
- Definición de roles y responsabilidades (Matriz RACI): Clarificación de quién ejecuta, quién aprueba y quién es consultado en cada etapa de los nuevos flujos de seguridad.
- Establecimiento de métricas de desempeño: Definición de indicadores asociados a la seguridad y la eficiencia que permitirán auditar el cumplimiento del modelo en fases posteriores.

5.1.3. Planificación referente a las tecnologías

La dimensión tecnológica en el modelo GCAMTI actúa como el habilitador estratégico que sustenta los procesos y empodera a las personas. La planificación en esta área no se limita a la adquisición de herramientas, sino a su orquestación para que actúen como el validador primario de la identidad. El objetivo es transitar hacia una arquitectura donde la tecnología automatice la seguridad y elimine el error humano mediante el uso de estándares de autenticación avanzados.

5.1.3.1. Tecnologías para la Recepción de Solicitudes (Punto de Contacto)

Son las plataformas técnicas que permiten la interacción inicial entre el usuario y la mesa de servicio. La planificación busca habilitar canales diversificados que capturen datos de identidad desde el primer contacto, reduciendo la carga operativa de validación manual:

- Portal de autoservicio y Apps móviles: Implementar interfaces donde el ingreso de solicitudes esté condicionado a una sesión activa y validada mediante Single Sign-On (SSO), garantizando que el origen del ticket sea siempre confiable.
- Central telefónica IP (VoIP) con CTI: Configurar la telefonía para que reconozca automáticamente el número de origen (ANI) y lo contraste con el CRM, preparando al sistema para la validación biométrica posterior.
- Asistentes virtuales (Bots) con validación: Desplegar chatbots integrados con los sistemas de tickets que realicen una autenticación básica antes de permitir que la solicitud sea transferida a un agente humano.

5.1.3.2. Tecnologías para la Autenticación de Identidad (Inherencia y Posesión)

Representan el núcleo de seguridad del modelo, encargándose de verificar que el solicitante es quien dice ser mediante factores de autenticación reforzada que eliminan la subjetividad del agente:

- Motores de biometría de voz: Integrar soluciones de huella vocal en el canal telefónico que analicen rasgos fisiológicos únicos, permitiendo una autenticación inmune a la ingeniería social y los deepfakes.
- Ecosistema de autenticación multifactor (MFA): Planificar el envío de códigos OTP (One-Time Password) a dispositivos móviles registrados y el uso de aplicaciones autenticadoras para validar solicitudes de riesgo medio y alto.
- Single Sign-On (SSO) Federado: Implementar protocolos como SAML o OpenID Connect para que la identidad validada en la red corporativa se extienda de forma transparente y segura a todas las herramientas de soporte.

5.1.3.3. Tecnologías para la Gestión de Tickets (ITSM)

Son las plataformas que centralizan el ciclo de vida de las solicitudes. La planificación se enfoca en configurar reglas de negocio estrictas que conviertan a la herramienta en un bloqueador proactivo de riesgos:

- Configuración de workflows seguros: Programar herramientas como Jira, ServiceNow o Freshservice para que hereden los datos de autenticación y bloqueen la resolución de tickets si no existe una evidencia digital de validación exitosa.
- Integración con herramientas de colaboración: Habilitar Microsoft Teams o Slack para sesiones de autorización crítica, asegurando que las aprobaciones de privilegios elevados queden grabadas y vinculadas al ticket.
- Motores de aprobación automatizados: Configurar disparadores (triggers) que envíen notificaciones push a los dueños de procesos para autorizaciones en tiempo real, garantizando la trazabilidad de cada permiso concedido.

5.1.3.4. Tecnologías para el Monitoreo y Análisis (Business Intelligence)

Herramientas analíticas encargadas de procesar los datos generados para medir el desempeño de la seguridad y detectar anomalías en el comportamiento de los usuarios:

- Cuadros de mando (Power BI / Tableau): Diseñar visualizaciones que muestren en tiempo real la tasa de fallos de autenticación por canal, permitiendo identificar intentos de fraude masivos de forma temprana.
- Análisis de comportamiento (UEBA): Utilizar algoritmos de aprendizaje para detectar solicitudes inusuales (horarios extraños o volumen excesivo de cambios de clave) que no correspondan al perfil histórico del usuario.
- Monitoreo de disponibilidad de canales: Implementar sondas que aseguren que los métodos de autenticación (servidores de OTP y Biometría) operen con una disponibilidad del 99.9%.

5.1.3.5. Tecnologías para la Seguridad y Cumplimiento (Arquitectura Zero Trust)

Conjunto de capas de protección destinadas a garantizar que el modelo cumpla con normativas internacionales bajo la filosofía de "Nunca confiar, siempre verificar":

- Alineamiento con PCI DSS v4.0 e ISO 27001: Planificar el uso de contraseñas de alta complejidad, cifrado de extremo a extremo (TLS/SSL) y registros de eventos críticos (Logs) para auditorías forenses.
- Gestión de secretos y bóvedas de contraseñas: Implementar herramientas que eviten que los agentes conozcan las claves de los clientes, gestionando accesos mediante tokens temporales de un solo uso.
- Consolidación de logs en SIEM: Automatizar el envío de todos los eventos de identidad hacia un monitor central de seguridad para garantizar el cumplimiento de los estándares de no repudio y trazabilidad.

5.2. HACER (D de DO del PDCA)

El objetivo de la fase de “hacer” (DO del modelo PDCA o ciclo Deming) es llevar a cabo lo definido en la fase de planificación para la implementación del modelo de gestión del cambio sobre la triada personas, procesos y tecnología. En particular aplicando lo planificado sobre los actores clave (personas), los procesos actuales y las tecnologías involucradas en la autenticación y seguridad de los canales de atención en la mesa de servicio TI.

5.2.1. Hacer referente a las personas

5.2.1.1. Identificar y clasificar stakeholders

En esta etapa se ejecuta el levantamiento de información de los actores clave identificados en la planificación. La recopilación de datos (necesidades, niveles de autoridad y expectativas de seguridad) se realiza mediante

entrevistas o talleres de trabajo adaptados a la estructura de cada organización, tomando como marco de referencia la categorización y estrategia de gestión mencionada en ANEXO 1.

5.2.1.2. Diagnosticar competencias

Aplicar las herramientas de diagnóstico propuestas (evaluaciones técnicas, psicométricas y de riesgo conductual) para detectar brechas de seguridad. Se deben levantar indicadores cuantitativos y cualitativos que establezcan la línea base de habilidades del personal frente a vectores de ataque como la ingeniería social.

5.2.1.3. Ejecutar el programa de formación y entrenamiento técnico

Realizar los talleres y laboratorios prácticos diseñados para desarrollar competencias en el uso de herramientas de identidad (MFA, Biometría) y detección de fraude (vishing - phishing). Se deben aplicar simulacros de entorno controlado y certificar las competencias técnicas de los agentes antes de otorgarles permisos definitivos en los sistemas productivos.

5.2.1.4. Desplegar la estrategia de comunicación y concientización

Publicar contenidos segmentados por canales internos y externos para generar alineación organizacional. Esto implica difundir cápsulas de sensibilización, manuales de resolución para equipos comerciales y configurar mensajes preventivos en los puntos de contacto (IVR/Portal) para educar al usuario sobre los nuevos protocolos de seguridad.

5.2.2. Hacer referente a los procesos

5.2.2.1. Realizar diagnóstico inicial de procesos

Ejecutar el levantamiento de flujos vigentes mediante observación directa y revisión de registros. Se deben validar tiempos de atención, rutas de escalamiento y niveles de trazabilidad para consolidar un informe de diagnóstico que identifique las brechas críticas entre el estado actual y el modelo diseñado.

5.2.2.2. Operativizar la Matriz de Controles

Implementar sistemáticamente los niveles de autenticación reforzada según la criticidad de la solicitud. Esto requiere integrar técnicamente los desafíos de identidad (OTP, Biometría) en el flujo de trabajo del agente y establecer responsables para la gestión de excepciones bajo aprobación jerárquica documentada.

5.2.2.3. Ejecutar la reingeniería del ciclo de vida del ticket (Workflows Seguros)

Aplicar los nuevos flujos de atención estructurados desde el primer contacto hasta el cierre. Se deben configurar reglas de negocio en la plataforma de gestión que bloqueen el progreso de una solicitud si no existe una evidencia técnica de identidad verificada, asegurando la trazabilidad en cada transición de estado.

5.2.2.4. Priorizar canales y gestionar datos críticos (Gobernanza de Datos)

Incentivar el uso de canales con controles nativos (Portal/Autoservicio) y ejecutar protocolos de actualización de emergencia en el CRM. Se debe asegurar la higiene de la información de contacto en tiempo real para evitar que datos erróneos impidan la ejecución de la autenticación multifactor.

5.2.2.5. Homologar y documentar procesos

Elaborar, revisar y publicar formalmente el Manual de Procedimientos Operativos de Identidad (MPOI) y la matriz RACI. Se debe garantizar el acceso a esta documentación para todos los involucrados y validar su comprensión mediante ejercicios prácticos, asegurando la continuidad operacional.

5.2.3. Hacer referente a la tecnología

5.2.3.1. Configurar tecnologías para la recepción de solicitudes (Punto de Contacto):

Corroborar que el portal de autoservicio, la telefonía IP (VoIP) y los asistentes virtuales estén operativos y correctamente integrados. Se deben establecer métricas iniciales de disponibilidad para asegurar que los canales de entrada capturen datos de identidad desde el inicio de la sesión.

5.2.3.2. Implementar tecnologías para la autenticación de identidad (Inherencia y Posesión):

Realizar el despliegue técnico de los motores de biometría de voz y ecosistemas MFA. Se deben configurar las APIs necesarias para que la validación de rasgos fisiológicos y factores de posesión (OTP) sea un requisito técnico infranqueable para solicitudes de riesgo medio y alto.

5.2.3.3. Parametrizar tecnologías para la gestión de tickets (ITSM):

Ajustar la herramienta de gestión de tickets para reflejar los flujos y reglas de negocio planificadas. Se deben activar disparadores (triggers) automáticos para aprobaciones y notificaciones en tiempo real, asegurando que la plataforma actúe como el orquestador central de la seguridad.

5.2.3.4. Poner en marcha tecnologías para el monitoreo y análisis (Business Intelligence):

Implementar tableros de control y reportes automáticos que permitan visualizar el desempeño del modelo. Se deben configurar alertas de umbrales para detectar anomalías en la autenticación, proporcionando información periódica a los stakeholders clave para la toma de decisiones.

5.2.3.5. Validar tecnologías para la seguridad y cumplimiento (Arquitectura Zero Trust)

Revisar que todas las capas tecnológicas cumplan con las políticas de cifrado (TLS/SSL), control de accesos y registros de auditoría. Se deben consolidar los logs de identidad en un sistema centralizado (SIEM) para garantizar la trazabilidad forense y el cumplimiento de normativas internacionales.

5.3. REVISAR (C de CHECK del PDCA)

El objetivo de la fase de “revisar” (CHECK del modelo PDCA o ciclo Deming) es realizar una revisión, monitoreo o auditoría de lo realizado en la fase DO para la implementación del modelo de gestión del cambio sobre la triada personas, procesos y tecnología. En particular revisando lo ejecutado sobre los actores clave (personas), los procesos actuales y las tecnologías involucradas en la autenticación y seguridad de los canales de atención en la mesa de servicio TI.

5.3.1. Revisar referente a las personas

5.3.1.1. Evaluar aprendizaje y retención de competencias

Verificar si las capacitaciones y simulacros han transferido efectivamente las habilidades técnicas necesarias. Se deben realizar auditorías de vishing- phishing ético post-entrenamiento para medir la mejora en la detección de engaños y aplicar métricas de "Residuo de Subjetividad" mediante la escucha de grabaciones, comprobando si el agente prioriza los factores de identidad técnicos sobre su criterio personal.

5.3.1.2. Analizar compromiso y comprensión organizacional

Auditar la alineación de los stakeholders mediante encuestas de percepción y grupos focales. Se debe validar si el personal operativo comprende el propósito de los controles (ej. prevención de ransomware) y verificar la consistencia del discurso en el soporte comercial, asegurando que no existan silos informativos que generen fricción ante quejas de clientes por bloqueos de seguridad.

5.3.2. Revisar referente a los procesos

5.3.2.1. Auditar cumplimiento de flujos operacionales

Realizar muestreos aleatorios de tickets para verificar la trazabilidad completa desde el ingreso hasta el cierre. Se debe confirmar el uso correcto de categorías y prioridades, validando que los pasos de escalamiento se cumplan estrictamente según el modelo y detectando saltos de procesos no justificados.

5.3.2.2. Evaluar el uso de canales de atención y matriz de autenticación

Comprobar si los canales están siendo utilizados según la priorización establecida. Se debe ejecutar un análisis estadístico para detectar "canales no autorizados" o informales y auditar que cada ticket crítico cuente con el respaldo de identidad exigido (OTP, biometría), prestando especial atención a los tickets en estado "condicional".

5.3.2.3. Verificar la trazabilidad de extremo a extremo (E2E) y calidad de datos

Realizar una reconstrucción forense de casos cerrados para asegurar la correlación transcanal (ID de llamada vs. log de biometría vs. ticket). Asimismo, auditar la higiene del CRM midiendo la tasa de fallos en la autenticación causados por datos obsoletos, validando que los protocolos de actualización de emergencia se ejecuten sin comprometer la seguridad.

5.3.3. Revisar referente a las tecnologías

5.3.3.1. Monitorear funcionamiento de tecnologías críticas

Evaluar la disponibilidad y estabilidad de los canales habilitados y las herramientas de autenticación (SSO, MFA, Biometría). Se deben revisar los logs de errores de integración entre las plataformas de contacto y el ITSM, asegurando que la automatización de los registros de seguridad sea íntegra y oportuna.

5.3.3.2. Analizar indicadores operativos y de seguridad (BI Avanzado)

Utilizar cuadros de mando para detectar anomalías de acceso, como intentos fallidos iterativos desde geolocalizaciones inusuales. Se deben identificar "puntos ciegos" en la reportabilidad operativa (AHT, SLAs) que impidan visualizar desviaciones críticas en la validación de identidad o subutilización de las herramientas de biometría.

Se definirán indicadores de desempeño tales como: (i) tasa de autenticación multifactor aplicada, (ii) tiempo promedio de atención, y (iii) número de incidentes de validación incorrecta. Estos indicadores serán comparados antes y después de la implementación de la guía.

5.3.3.3. Evaluar cumplimiento normativo técnico

Corroborar que las tecnologías aplicadas mantengan los estándares de cifrado (TLS/SSL), control de accesos y perfiles definidos. Se deben realizar escaneos de integridad de los logs de auditoría para asegurar que no puedan ser modificados, garantizando el cumplimiento de marcos regulatorios como ISO 27001 o PCI DSS v4.0.

5.3.4. Consolidar hallazgos de verificación

5.3.4.1. Registrar desviaciones y cumplimientos

Documentar de forma estructurada las brechas detectadas en personas (resistencia), procesos (datos sucios) y tecnología (latencias).

5.3.4.2. Priorizar acciones para la fase ACT

Generar una Matriz de Hallazgos Críticos que clasifique los riesgos emergentes y las sugerencias de los equipos técnicos, estableciendo la hoja de ruta para las acciones correctivas y de mejora continua.

5.4. MEJORAR (A de ACT del PDCA)

El objetivo de la fase de “mejorar” (ACT del modelo PDCA o ciclo Deming) es llevar a cabo las mejoras y actualizaciones identificadas en la fase anterior para la implementación del modelo de gestión del cambio sobre la triada personas, procesos y tecnología. En particular aplicando mejoras sobre los actores clave (personas), los procesos actuales y las tecnologías involucradas en la autenticación y seguridad de los canales de atención en la mesa de servicio TI.

5.4.1. Mejorar referente a las personas

5.4.1.1. Fortalecer la alineación estratégica y colaboración de stakeholders

Establecer Comités de Gobernanza de Identidad entre el CISO, Gerentes de Operaciones y KAM para resolver bloqueos operativos. Se deben formalizar Acuerdos de Niveles Operativos (OLA) que garanticen que el área comercial respalde los rechazos de atención por fallos de identidad, eliminando la presión sobre el agente técnico.

5.4.1.2. Ajustar la efectividad del plan de formación y concientización

Optimizar los programas de capacitación incorporando casos reales de fraude detectados durante la ejecución. Se deben implementar sesiones de refuerzo para temas con baja retención y desplegar cápsulas de concientización basadas en incidentes reales que refuercen el sentido de vigilancia y el propósito de los controles.

5.4.1.3. Institucionalizar el conocimiento y las buenas prácticas

Incorporar formalmente el módulo de identidad en el proceso de Onboarding para nuevos colaboradores. Se deben reconocer públicamente a los "Embajadores de Seguridad" que apliquen con éxito las metodologías, asegurando que el aprendizaje se integre en el ADN organizacional y no se pierda con la rotación de personal.

5.4.2. Mejorar referente a los procesos

5.4.2.1. Optimizar el desempeño y rediseñar flujos operativos

Actualizar los diagramas de proceso (BPMN) para diferenciar flujos de "Consulta" de "Cambios Críticos", eliminando pasos redundantes en casos de bajo riesgo para optimizar el AHT. Se deben redistribuir cargas de trabajo basadas en los cuellos de botella identificados en la fase de verificación.

5.4.2.2. Implementar protocolos de higiene de datos en vivo

Establecer como política mandatoria la actualización de datos de contacto en el CRM durante cada interacción exitosa. Esto garantiza que la base de datos se mantenga saneada, evitando que información obsoleta bloquee los flujos de autenticación multifactor (MFA) en el futuro.

5.4.2.3. Actualizar e institucionalizar la documentación operativa

Publicar y distribuir la Versión 2.0 de los manuales y protocolos (MPOI), incluyendo el manejo de excepciones técnicas y flujos de escalamiento ante caídas de sistemas. Se deben unificar los repositorios digitales para asegurar que el personal consulte exclusivamente las versiones vigentes, eliminando manuales informales.

5.4.3. Mejorar referente a las tecnologías

5.4.3.1. Integrar controles de seguridad en el workflow de ITSM

Aplicar "Seguridad por Diseño" configurando bloqueos automáticos de transiciones en herramientas como Jira o ServiceNow. El sistema debe impedir el progreso o cierre de un ticket si no existe un registro de validación exitosa (MFA/Biometría), eliminando la posibilidad de omisión manual por parte del agente.

5.4.3.2. Tecnificar el canal de voz y automatizar el IVR

Implementar soluciones de IVR Seguro que permitan al cliente realizar la autenticación multifactor durante el tiempo de espera. El objetivo es que el agente reciba la llamada con la identidad ya validada técnicamente, desplazando la responsabilidad desde el humano hacia sistemas automáticos de alta precisión.

5.4.3.3. Estandarizar configuraciones y trazabilidad continua

Robustecer los parámetros de Single Sign-On (SSO) y asegurar el cifrado extremo a extremo en todos los canales. Se deben automatizar las exportaciones de eventos de identidad hacia un monitor centralizado (SIEM) para detectar anomalías transcanales de forma proactiva y garantizar el cumplimiento normativo permanente.

5.4.4. Cerrar el ciclo e iniciar una nueva iteración

Al finalizar la fase ACT, el modelo GCAMTI deja de ser un proyecto de implementación para convertirse en el estándar operativo de la organización.

5.4.4.1. Elaborar el Informe Final de Resultados

Documentar la reducción del riesgo residual de suplantación, la mejora en tiempos de respuesta por automatización y el nivel de adopción cultural alcanzado.

5.4.4.2. Reiniciar el Ciclo PDCA

Utilizar los aprendizajes y nuevos desafíos detectados para alimentar la planificación del siguiente ciclo, asegurando que el modelo evolucione dinámicamente frente al panorama de amenazas.

6. Verificación de la Guía Metodológica GCAMTI en aplicación práctica

El presente capítulo tiene como objetivo validar la efectividad del modelo de Gestión del Cambio para la Autenticación en Mesas de Servicio TI (GCAMTI). Para ello, se analiza la aplicación práctica de la guía desarrollada en el Capítulo 5, evaluando el desempeño de la tríada Personas, Procesos y Tecnología y su impacto directo en la seguridad de los canales, la confianza del cliente y la adopción interna del proceso.

6.1. Validación del modelo en su fase de "Planificación"

La validación del modelo GCAMTI mediante su aplicación en un entorno controlado permitió contrastar las directrices de planificación con la realidad operativa de la organización. En la dimensión de personas, la identificación de partes interesadas mediante el mapeo de la cadena de valor integró a jefaturas de soporte, centro de contacto, administración de cuentas y ciberseguridad, lo que otorgó un sólido respaldo institucional y alineación con las políticas internas; no obstante, se identificó como oportunidad de mejora incorporar tempranamente a la primera línea de atención para evitar la percepción de una imposición gerencial. En formación y diagnóstico, se adoptó un enfoque delegado en los líderes de equipo que aportó agilidad y adaptabilidad psicológica, aunque asumiendo el riesgo de heterogeneidad en los criterios de evaluación, el cual fue mitigado mediante cursos transversales corporativos. Asimismo, la comunicación basada en la guía redujo la fricción operativa, mientras que el saneamiento preventivo de datos aseguró la consistencia requerida por los sistemas.

En la dimensión de procesos, se postergó el diagnóstico definitivo para el siguiente ciclo PDCA con el fin de priorizar el fortalecimiento de la seguridad en un entorno controlado. La planificación articuló una matriz de controles y validación que, si bien preveía un incremento en los tiempos de gestión, fue determinante para resguardar la integridad de las solicitudes. Este diseño demostró que el flujo de atención de tickets actual no requiere una reingeniería profunda, sino la integración estratégica y documental de controles de contacto para asegurar la replicabilidad del modelo.

Respecto a la dimensión de tecnología, se optó por aprovechar la infraestructura instalada (portal, correo y teléfono) para minimizar la curva de aprendizaje y preservar la estabilidad operativa. La estrategia se focalizó en desplazar la validación hacia sistemas automatizados mediante la integración de IVR y MFA con OTP dinámico, atacando directamente la suplantación de identidad. Se mantuvieron las plataformas de tickets existentes por su compatibilidad con "Active Directory", identificando como limitación la falta de licenciamiento integral en el centro de contacto para explotación analítica avanzada en herramientas como BI y "Tableau".

Al contrastar la planificación con la hipótesis del estudio, se confirma que el enfoque holístico del modelo elimina puntos ciegos al articular la tríada Personas, Procesos y Tecnología (PPT). Su diseño flexible facilita la adopción adaptándose a la realidad operativa de la primera línea, la estructura técnica escalable permite una expansión masiva sin pérdida de eficiencia, y la naturaleza evolutiva del ciclo PDCA asegura la mejora continua. En conjunto, esta rigurosidad técnica y procedimental fortalece la confianza del cliente, consolidando a GCAMTI como una propuesta integral, adaptable y alineada con los requerimientos de ciberseguridad institucional.

6.2. Validación de la Guía Metodológica en su fase de "Ejecución"

La fase de ejecución (DO) puso a prueba la operatividad del modelo GCAMTI en un entorno de atención real, arrojando hallazgos determinantes sobre la tríada PPT. En la dimensión de personas, aunque la selección por

cadena de valor identificó con precisión a los actores críticos, la fase de entrenamiento reveló una brecha estructural: la guía definía el "cómo" formar, pero no "quién" debía liderarlo. Delegar la instrucción al criterio de cada jefatura generó heterogeneidad en la asimilación de contenidos, evidenciando la necesidad de centralizar la formación bajo un estándar unificado de calidad.

En la dimensión de procesos, la aplicación de la matriz de controles blindó los accesos, pero generó una ralentización operativa inicial. Esta fricción se intensificó por un fallo de difusión que omitió notificar al equipo comercial sobre la entrada en vigencia del MFA, provocando respuestas no coordinadas ante consultas de clientes. Asimismo, la ejecución confirmó que el saneamiento de datos es una labor transversal y prioritaria, cuya falta de actualización impactó la fluidez de los flujos y la experiencia del usuario. El comportamiento temporal de los tiempos promedios de atención evidenciando el incremento inicial por curva de adopción y la posterior regularización del servicio, se ilustra en el ANEXO 5.

En la dimensión de tecnología, se maximizó la infraestructura instalada para reducir la curva de aprendizaje, desplegando con éxito OTP en el portal de clientes e implementando un IVR en el canal telefónico como capa persuasiva y disuasoria ante la ingeniería social. La gestión se apoyó en los sistemas de ticketing e inteligencia de negocios existentes (BI y Tableau) en estricta observancia de las políticas corporativas.

Al contrastar la ejecución con la hipótesis, se confirma la efectividad del enfoque holístico para elevar la ciberseguridad. La implementación de MFA e IVR validó la escalabilidad del modelo, mientras que la capacidad de detectar brechas comunicacionales y formativas demostró su flexibilidad adaptativa. En términos de impacto técnico sobre los vectores de entrada, la combinación de controles procedimentales en el correo electrónico, capas disuasivas en el canal telefónico y validaciones automatizadas mediante OTP en el portal institucional evidencia una transición progresiva en la postura de ciberseguridad. Esta evolución confirma empíricamente la capacidad del modelo para elevar de manera gradual la resiliencia de los puntos de interacción empresa-cliente sin interrumpir la continuidad operacional del negocio. Para visualizar con precisión este impacto técnico y la evolución de los canales de entrada, refiérase al ANEXO 6.

6.3. Validación de la Guía Metodológica en su fase de “Revisión y Mejora”

Las fases de Revisión (CHECK) y Mejora (ACT) confirman la funcionalidad de la guía y la adecuada interacción de la tríada PPT, ubicándose en un proceso de maduración operativa. Dado el carácter evolutivo del modelo GCAMTI, los hallazgos del piloto representan un diagnóstico preliminar que requiere extender el periodo de observación para diluir la curva de aprendizaje inicial. En consecuencia, la organización determinó mantener una etapa de iteración reforzada, donde las mejoras identificadas, como el saneamiento profundo de datos maestros y la centralización formativa, se reevaluarán en nuevos ciclos PDCA antes de emitir un juicio definitivo sobre su eficacia de largo plazo. Respecto a la confianza del cliente, evaluada cualitativamente mediante juicio de expertos y métricas operativas, se constató una contención satisfactoria evidenciada en la estabilización de los SLA, la ausencia de reclamos formales y la nula ocurrencia de suplantaciones de identidad; estableciéndose la medición empírica directa (encuestas NPS/CSAT) para la siguiente iteración.

La validación del modelo se enriqueció mediante un proceso de contraste cualitativo con tres expertos sectoriales (Banca, Previsional y Telecomunicaciones), quienes evaluaron la aplicabilidad de la guía y emitieron juicios técnicos respecto a su solidez, usabilidad y escalabilidad. La convergencia entre estas tres visiones confirma que la resiliencia no surge de barreras infranqueables, sino de una gestión del cambio equilibrada. El detalle de la evaluación por juicio de expertos, el análisis sectorial comparativo y la Matriz Consolidada de Validación de la Hipótesis se presentan en el ANEXO 7.

7. Conclusiones

La investigación y el desarrollo de la guía metodológica GCAMTI respaldan la hipótesis planteada al evidenciar que la inseguridad en los canales de atención no responde a fallos aislados, sino a un desfase sistémico entre la

sofisticación de las amenazas (como el ransomware experimentado previamente) y la precariedad de la autenticación tradicional. Se concluye que tratar la ciberseguridad como un parche tecnológico aislado es ineficaz; solo una visión holística que equilibre la tríada Personas, Procesos y Tecnología (PPT) logra cerrar las brechas que el factor humano y la obsolescencia procedimental dejan abiertas. Esta implementación transforma la mesa de servicio de un punto débil a una barrera disuasoria, protegiendo a la organización de brechas de datos y daños reputacionales. Asimismo, se demuestra que la seguridad no es enemiga de la operación: aunque se introducen capas de control (MFA, matrices), la fricción inicial se mitiga mediante comunicación efectiva y adopción gradual, redefiniendo la usabilidad y la "buena atención" a partir de la tranquilidad del usuario.

Desde la perspectiva del ejercicio profesional en ingeniería y el aporte académico, el trabajo demuestra que la solución tecnológica resulta insuficiente por sí sola. El desafío contemporáneo trasciende el despliegue técnico de herramientas (MFA, IVR) y exige la gestión de la resistencia humana y el diseño de procesos viables en la realidad operativa. El principal aporte metodológico radica en la aplicación dual del ciclo PDCA: un PDCA de Diseño, que contrastó la teoría con la realidad empresarial en tiempo real para refinar la guía, y un PDCA de Aplicación, que actuó como motor de ejecución del piloto operativo. Esta metodología de "doble vuelta" asegura que la propuesta no sea un constructo teórico inerte, sino un modelo intrínsecamente evolutivo, flexible y escalable, con el potencial de extender esta cultura de seguridad a otras unidades de negocio como un activo intangible diferenciador.

En cuanto a los alcances y limitaciones de la investigación, los resultados cualitativos del piloto proporcionan evidencia empírica suficiente para confirmar la viabilidad de la propuesta. Se reconoce que el modelo se encuentra en una fase de maduración incremental; por lo tanto, la ausencia de métricas cuantitativas consolidadas no representa una debilidad, sino la ratificación de un sistema "vivo" y dinámico. Como recomendación y trabajo derivado, se proyecta someter la guía a futuras iteraciones del ciclo PDCA, lo que permitirá ajustar los controles de acuerdo con la evolución del panorama de amenazas y la maduración cultural de la organización. En definitiva, esta tesina consolida la seguridad de la información como un compromiso cultural e institucional coordinado, situándola como el pilar estratégico fundamental de la confianza en la era digital.

8. Referencias

[1] Amazon Web Services, Inc., "¿Qué es la ciberseguridad? - Explicación de la ciberseguridad - AWS," AWS, 2024. [En línea]. Disponible: https://aws.amazon.com/es/what-is/cybersecurity/. [Accedido: 06-ene-2024].

[2] S. Rose, O. Borchert, S. Mitchell y S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, ago. 2020. [En línea]. Disponible: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf. [Accedido: 02-abr-2026].

[3] Zendesk, "Service desk: ¿Qué es? Sus características y ventajas," Zendesk, 2024. [En línea]. Disponible: https://www.zendesk.com.mx/blog/mesa-de-servicio-que-es/. [Accedido: 07-ene-2024].

[4] National Institute of Standards and Technology (NIST), "Spoofing," Computer Security Resource Center (CSRC) Glossary. [En línea]. Disponible: https://csrc.nist.gov/glossary/term/spoofing. [Accedido: 27-jul-2026].

[5] Cloudflare, "¿Qué es la autenticación?," Cloudflare, 2024. [En línea]. Disponible: https://www.cloudflare.com/es-es/learning/access-management/what-is-authentication/. [Accedido: 07-ene-2024].

[6] Mitek, "Aumente la seguridad: autenticación multifactor frente a basada en riesgos," Mitek Systems, 2024. [En línea]. Disponible: https://www.miteksystems.com/es/blog/que-es-la-autenticacion-multifactor-y-basada-en-el-riesgo. [Accedido: 07-ene-2024].

[7] Universidad de Concepción, "Aplicación del ciclo Deming o PDCA para la gestión de la calidad en la educación superior," Concepción, Chile, Informe técnico, 2020. [En línea]. Disponible: https://desarrolloestrategico.udec.cl/wp-content/uploads/2021/01/DDD-N-4-Ciclo-Deming.pdf. [Accedido: 23-abr-2026].

[8] C. Toth y K. E. Toth, "Face recognition and authentication in mobile environments," arXiv, preprint arXiv:1208.0892, 2012. [En línea]. Disponible: https://arxiv.org/abs/1208.0892. [Accedido: 27-jul-2026].

[9] Project Management Institute (PMI), A Guide to the Project Management Body of Knowledge (PMBOK Guide), 7ma ed. Pensilvania, EE. UU.: PMI, 2021.
[10] Project Management Institute (PMI), "Project Management Maturity: An Industry-Wide Assessment," PMI, 2004. [En línea]. Disponible: https://www.pmi.org/learning/library/pm-maturity-industry-wide-assessment-9000. [Accedido: 27-jul-2026].
[11] Smartsheet, "Guía para los modelos de madurez de procesos," Smartsheet, 2024. [En línea]. Disponible: https://es.smartsheet.com/content/process-maturity. [Accedido: 27-sep-2024].
[12] Genesys, "Líder 2023 en el Cuadrante Mágico de CCaaS – Gartner," Genesys, 2024. [En línea]. Disponible: https://www.genesys.com/es-mx/resources/gartner-magic-quadrant-for-contact-center-as-a-service. [Accedido: 07-ene-2024].
[13] PwC España, "Pocas empresas se consideran totalmente protegidas frente a ciberataques en sus áreas más críticas," PwC, 2022. [En línea]. Disponible: https://www.pwc.es/es/sala-prensa/notas-prensa/2022/pocas-empresas-protegidas-areas-criticas-contra-ciberataques.html. [Accedido: 27-jul-2026].
[14] Nuance, "Prevención de Fraude en el Contact Center de Nuance," TechTalk Summits, 2024. [En línea]. Disponible: https://techtalksummits.com/MediaLibraries/Files/Prevencion-de-Fraude-en-el-Contact-Center-de-Nuance.pdf. [Accedido: 16-mar-2024].
[15] Gartner, "Gartner Survey Reveals Generative Artificial Intelligence Attacks Are on the Rise," Gartner Press Release, 2025. [En línea]. Disponible: https://www.gartner.com/en/newsroom/press-releases/2025-09-22-gartner-survey-reveals-generative-artificial-intelligence-attacks-are-on-the-rise. [Accedido: 27-jul-2026].
[16] National Institute of Standards and Technology (NIST), "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B. [En línea]. Disponible: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accedido: 07-ene-2024].
[17] Agencia Nacional de Ciberseguridad (ANCI), "Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información," ANCI, 2024. [En línea]. Disponible: https://anci.gob.cl/normativa/ley-marco-ciberseguridad/. [Accedido: 02-abr-2026].
[18] Cloud Native Computing Foundation (CNCF), "Cloud Native Maturity Model," Cartografos Working Group, v4.0. [En línea]. Disponible: https://maturitymodel.cncf.io/. [Accedido: 27-jul-2026].

9. Anexos

La presente sección complementa el desarrollo teórico y metodológico expuesto en el cuerpo principal de esta tesina. Para su correcta interpretación y aplicación, los anexos incorporados deben ser comprendidos bajo dos categorías funcionales diferenciadas según su origen y propósito:

- Anexos 1 al 4 (Instrumentos metodológicos del capítulo 5): Corresponden a los artefactos, plantillas y herramientas diseñadas en el marco de la Guía Metodológica GCAMTI (fase PLAN). Dichos instrumentos no deben ser considerados como procedimientos rígidos o esquemas estáticos, sino como referencias y guías operativas adaptables. Su propósito es servir de base flexible para que cada organización los parametrice e instancie según su nivel de madurez técnica, estructura organizacional y contexto particular.
- Anexos 5 al 7 (Resultados y evidencias de validación del apítulo 6): Reúnen los datos empíricos, protocolos de gobernanza, evaluaciones cualitativas y matrices de trazabilidad derivados de la aplicación práctica y verificación de la guía (fases DO, CHECK y ACT). Estos anexos documentan la viabilidad del modelo en un entorno controlado, consolidando las evidencias operativas y el juicio de expertos que respaldan la validez de la hipótesis planteada.

ANEXO 1: Ejemplo de categorización stakeholders (Fase PLAN – Personas)

El éxito de la guía GCAMTI radica en abordar la dimensión de Personas como el pilar determinante de la efectividad de los controles de ciberseguridad. La identificación de los stakeholders en la fase de Planificación (PLAN) combina la matriz de poder e interés con la asignación de roles RACI (Responsible, Accountable, Consulted, Informed). Esta integración permite diseñar estrategias de gestión del cambio diferenciadas que mitiguen la resistencia operativa, alineen las políticas corporativas y aseguren la continuidad del negocio.

Tabla 1 : Ejemplo categorización stakeholders

Stakeholder	Rol en GCAMTI	Poder	Interés	Estrategia/RACI
CISO / Gerente Seguridad.	Definir políticas y niveles de riesgo.	Alto	Alto	Gestionar de cerca / Aprobador (Accountable - A)
Agentes Mesa Ayuda	Ejecutar validación de identidad.	Bajo	Alto	Mantener informados y capacitados / Ejecutor (Responsible - R)
Clientes	Usuarios de servicios críticos.	Medio	Alto	Comunicación proactiva de beneficios / Consultado-Informado (Consulted/Informed - C/I)

Stakeholder	Rol en GCAMTI	Poder	Interés	Estrategia/RACI
Área Legal/Compliance	Validar trazabilidad y no repudio.	Alto	Medio	Mantener satisfechos / Auditor-Consultado (Consulted - C)

ANEXO 2: Instrumento de Diagnóstico de Competencias Técnicas, Psicológicas y Riesgo Conductual (Fase PLAN - Personas)

Dentro de la guía GCAMTI, el diagnóstico de competencias en la dimensión de Personas constituye el punto de partida para transformar al personal operativo de un vector de riesgo pasivo a una línea defensiva activa. Este instrumento permite calcular el Índice de Vulnerabilidad Humana (IVH) mediante la ponderación de tres dimensiones fundamentales: destreza técnica en herramientas, resistencia psicotrópica a la ingeniería social y propensión al incumplimiento por presión operativa.

Tabla 2: Rúbrica de evaluación y matriz de ponderación del riesgo conductual

Dimensión Evaluada	Criterio de Medición	Ponderación (%)	Nivel Crítico (Riesgo Alto)	Nivel Aceptable (Riesgo Bajo)
Técnica	Tiempo de ejecución y precisión en la validación	35	Tiempos de validación mayores a 180 segundos	Ejecución fluida. Tiempos menores o iguales a 60 segundos con registro en ticket
Psicológica	Resistencia ante disparadores emocionales de urgencia, autoridad o amenaza comercial.	40	Cede ante la presión del usuario y omite el protocolo de autenticación.	Mantiene la calma, aplica el guion formal y exige la validación MFA.
Riesgo conductual	Frecuencia de uso de "atajos" procedimentales para reducir indicadores	25	Omisión sistemática de pasos de seguridad en horas de alta demanda (Mayor o igual a 10%)	Adherencia al protocolo del 100% independientemente del volumen de llamadas.

Para evaluar el aspecto técnico se le presentan al agente tres escenarios de requerimientos técnicos de distinta criticidad. El evaluador mide el manejo técnico del ecosistema de. Se califica la capacidad de detectar discrepancias de datos entre el canal de origen y el registro del cliente, otorgando puntaje máximo al agente que completa la validación sin incurrir en registros erróneos ni duplicidad de identidades.

En la dimensión psicológica se evalúa la susceptibilidad del individuo frente a disparadores de manipulación: Urgencia Simulada (simulación de caída de servidor crítico de un cliente VIP), Invocación de Autoridad (suplantación de un ejecutivo de alta gerencia), Coerción Comercial (amenaza de cancelación de contrato) y Empatía/Lástima. La prueba determina el perfil de riesgo del agente, identificando si su patrón conductual tiende a la complacencia reactiva para priorizar el diseño de capacitaciones focalizadas.

Y en cuanto al riesgo conductual, a través del monitoreo discrecional de interacciones reales (escucha remota en vivo y revisión de logs), se audita una muestra de interacciones por agente. El evaluador registra cada caso en que el operador utiliza atajos (tales como validar la identidad mediante preguntas informales o asumir la identidad por reconociendo de voz no automatizado) con el fin de cumplir los límites de tiempo medio de atención, calculando la tasa de desviación procedimental individual.

ANEXO 3: Malla Curricular y Programa de Formación (Fase PLAN - Personas)

El Programa de Formación GCAMTI está estructurado bajo un enfoque teórico-práctico de tres niveles. Su propósito es garantizar la transferencia efectiva de competencias sobre los procesos de autenticación de identidad, minimizando la curva de aprendizaje y reforzando la toma de decisiones del personal operativo bajo escenarios de alta presión.

Tabla 3: Malla curricular del programa de entrenamiento GCAMTI

Módulo	**Contenidos principales**	**Carga horaria (horas)**	**Audiencia objetiva**	**Formato**
1.- Conceptos, Herramientas y Autenticación	Principios de autenticación segura, factores MFA y lógica de OTP dinámico.	8	Agentes mesa de ayuda, ingenieros de soporte	Marco teórico y laboratorio práctico
2.- Ciberseguridad Humana y Vishing	Protocolos de detección de engaño, vectores de ingeniería social, manejo de objeciones y desactivación de manipulaciones.	6	Agentes mesa de ayuda, ingenieros de soporte, supervisores mesa de ayuda y de mesa de soporte	Simulación de roles
3.- Gobernanza, Excepciones y Compliance	Ley N° 21.663, ISO 27001, trazabilidad E2E, gestión de tickets "condicionales" y flujo de excepciones jerárquicas.	4	Supervisores, jefaturas y equipo comercial	Taller de casos de estudio y análisis regulatorio

Módulo	Contenidos principales	Carga horaria (horas)	Audiencia objetiva	Formato
4.- Refuerzo Continuo y Concientización	Microcápsulas de 3 minutos, lecciones aprendidas de incidentes reales y novedades en amenazas de identidad.	1 (cada mes)	Toda la organización	Microcápsulas asíncronas y boletines

El primero módulo está enfocado en los principios de autenticación segura, factores MFA y la lógica del OTP dinámico. Capacita al operador en ambientes simulados para lograr verificación de credenciales, aplicación de controles y el registro en el CRM.

El segundo módulo se enfoca en desarrollar el sentido crítico del agente. Mediante llamadas simuladas con actores que interpretan a usuarios hostiles, apurados o con perfil ejecutivo, el entrenamiento adiestra al personal en la aplicación inflexible del protocolo de verificación, enseñándoles a canalizar la atención sin romper la cortesía comercial ni comprometer la seguridad.

El tercer módulo está dirigido a las líneas de supervisión y gestión comercial, este módulo aborda los aspectos legales de la trazabilidad y el no repudio. Se instruye en el protocolo formal para autorizar bypasses de seguridad en contingencias, el registro de evidencias de auditoría y la forma correcta de comunicar las políticas de ciberseguridad a las contrapartes comerciales del cliente.

El cuarto y último módulo está orientado al refuerzo continuo y concientización. Su objetivo es consolidar el aprendizaje y mantener una vigilancia activa sobre la ciberseguridad y la protección de datos en la cultura organizacional.

ANEXO 4: Ejemplo de matriz de control para canales de autenticación (Fase PLAN – Procesos)

La Matriz de Control constituye la pieza operativa central del pilar de Procesos dentro de la guía GCAMTI. Su propósito técnico es erradicar la subjetividad en la primera línea de atención, sustituyendo el criterio del agente por una gobernanza determinista basada en el nivel de riesgo de la transacción. Al correlacionar los canales de entrada con mecanismos específicos de autenticación de identidad, la matriz asegura que ningún requerimiento con potencial impacto en la infraestructura o en la confidencialidad de los datos pueda ser ejecutado sin la correspondiente validación y autorización.

Tabla 4 Ejemplo matriz de control

					CONTROLES								ACCIÓN/AUTORIZACIÓN	RIESGO
MATRIZ	CANALES	APLICABILIDAD	ESTADO	PRIORIDAD	SEGUNDO FACTOR	LLAMADA REVERSA	PALABRA CLAVE	AUTENTICACIÓN NORMAL	CORREO AUTORIZADO	N°TELÉFONO AUTORIZADO	CITA TEAMS/MEET/OTRO	OTROS		
	Voz (normal)	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Voz (normal)	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Voz (normal)	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Voz (contingencia)	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Correo corporativo	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Correo corporativo	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Correo corporativo	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Correo contingencia	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Portal de autoatención	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Portal de autoatención	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Whatsapp	SI/NO	Operativo/Por desarrollar/No aplica	1 a "n"										
	Otros													

La primera sección de la matriz establece los puntos de contacto entre el cliente y la mesa de servicio. La columna Canales diferencia entre vías transaccionales normales y de contingencia para modalidades de voz, correo corporativo, portal de autoatención y mensajería instantánea como WhatsApp. El atributo Aplicabilidad actúa como una llave de paso binaria que certifica si un canal cumple con los requisitos técnicos de

ciberseguridad corporativos para estar habilitado. Complementariamente, la columna Estado gestiona el ciclo de vida tecnológico del canal, discriminando si está plenamente Operativo, en estado Por desarrollar o si No aplica su utilización. Finalmente, la Prioridad define una jerarquía numérica del 1 al n que promueve la migración progresiva hacia canales con controles nativos automatizados.

El bloque de Controles estructura las pruebas de identidad en función de factores de conocimiento, posesión e inherencia. La columna Segundo Factor contempla el despliegue de códigos de un solo uso (OTP) o notificaciones push enviadas a dispositivos registrados; la Llamada Reversa y la confirmación por N° Teléfono Autorizado o Correo Autorizado verifican el origen de la solicitud contra la base de datos maestra del CRM. La Palabra Clave y la Autenticación Normal proveen factores de conocimiento tradicionales para interacciones de baja criticidad, mientras que la opción de Cita Teams/Meet/Otro introduce un mecanismo de validación presencial remota para casos excepcionales de muy alto riesgo. La matriz contempla la casilla Otros para permitir la incorporación evolutiva de futuras tecnologías, tales como biometría de voz pasiva o análisis de comportamiento contextual.

Las últimas dos columnas de la matriz articulan la lógica de decisión que gobierna la operación de la mesa de ayuda. La columna Riesgo clasifica la transacción en niveles Bajo, Medio o Alto según la matriz de impacto del negocio, evaluando variables como la elevación de privilegios, el acceso a datos sensibles o la modificación de configuraciones de red. La columna Acción / Autorización establece el alcance operativo preciso que se le otorga al agente o al sistema una vez que los controles de la fila han sido superados satisfactoriamente.

Los anexos presentados a continuación corresponden a lo detallado en el capítulo 6 con respecto a la validación de la guía GCAMTI

ANEXO 5: Visualización tiempos promedios de atención (Validación de la guía)

A continuación, se presenta y analiza la curva de comportamiento de los tiempos de atención registrada desde la puesta en marcha de la matriz de control para el fortalecimiento de la seguridad en la gestión de tickets de requerimientos:



Figura 6: Evolución timepos promedios de atención

La figura 6 ilustra la evolución de los tiempos promedio de atención. En el Punto A (mayo de 2026), se inició la aplicación obligatoria de la matriz de controles de identidad en la Mesa de Servicios TI.

Durante el periodo de adaptación (mayo – julio de 2026), los tiempos de respuesta y SLAs aumentaron temporalmente debido a la curva de aprendizaje de los agentes, la asimilación del MFA/OTP y las fricciones iniciales con los usuarios. Finalmente, a partir de agosto de 2026 (fase de estabilización), los tiempos descendieron hasta alcanzar los umbrales operativos deseados, confirmando la correcta adopción del procedimiento.

ANEXO 6: Matriz de evolución y madurez de los canales de atención en su fase de ejecución del PDCA (D) relacionado al capítulo de validación de la guía.

Con el propósito de complementar el análisis cualitativo de la fase de ejecución y evaluar la efectividad de las medidas introducidas en los vectores de entrada de la Mesa de Servicios TI, la siguiente matriz sintetiza el cambio en la postura de ciberseguridad antes y después de aplicar la guía GCAMTI:

Tabla 5 Matriz de evolución y madurez de los canales de atención en su fase de implementación (DO)

Canal de Atención	**Estado de Seguridad Inicial**	**Control / Mejora Implementada**	**Estado de Seguridad Post-Ejecución**	**Descripción y Alcance Operativo**
Correo Electrónico	Bajo	Protocolos manuales de validación de identidad del remitente.	Medio	Se estandarizó la verificación humana mediante flujos rigurosos que obligan al agente a confirmar la autenticidad del remitente antes de procesar tickets críticos.
Teléfono (Call Center)	Bajo	Integración de un sistema IVR persuasivo y disuasivo.	Bajo (Con capa de seguridad adicional)	Aunque la tecnología basal mantiene limitaciones estructurales, el IVR actúa como un filtro inicial crítico, mitigando y desalentando los ataques directos de ingeniería social.
Portal de Clientes	Bajo	Implementación de segundo factor de autenticación (MFA mediante OTP).	Medio	Se robusteció el acceso digital a través de la automatización del envío de códigos dinámicos y únicos, reduciendo drásticamente el riesgo de suplantación de identidad.

El rediseño operativo de los canales de atención evidencia una transición progresiva y medible en la postura de ciberseguridad de la organización. Si bien el canal telefónico conserva una clasificación técnica base debido a la naturaleza de su medio físico, la adición del IVR cumple con éxito el propósito estratégico de disuasión.

Por su parte, la combinación de controles procedimentales estrictos en el correo electrónico y la automatización tecnológica del OTP en el portal institucional consolidan un estado intermedio (gestionado) de protección. Esta evolución valida empíricamente que la guía GCAMTI es capaz de elevar de manera gradual la resiliencia de los puntos de interacción empresa-cliente sin interrumpir la continuidad operacional del negocio.

ANEXO 7: Juicio extendido de expertos sobre la guía GCAMTI

Para validar la aplicabilidad, solidez y versatilidad de la guía GCAMTI más allá del entorno controlado del piloto, se diseñó un protocolo de evaluación cualitativa basado en el método de juicio de expertos de distintos rubros y sectores (bancario, previsional y telecomunicaciones), donde a cada especialista se le presentó el documento conceptual de la guía GCAMTI (Capítulo 5) junto a los anexos correspondientes.

El juicio experto del sector bancario (Jefe de grupo ciberdefensa), permitió contrastar el GCAMTI con los estándares más rigurosos de la industria. A partir de esta evaluación, se concluye que, si bien el modelo constituye una base sólida y holística, su naturaleza evolutiva exige que, en futuras iteraciones, el ciclo PDCA integre controles técnicos de mayor profundidad. Bajo esta perspectiva, el experto enfatiza la necesidad de transitar desde esquemas de autenticación básicos hacia soluciones robustas de doble factor (TOTP), el endurecimiento de las políticas de gestión de identidades, la implementación de capas de protección perimetral como WAF y, fundamentalmente, la incorporación de un monitoreo avanzado mediante SIEM y ejercicios de pentesting. En definitiva, esta visión experta ratifica que la seguridad no es un estado estático, sino un proceso de mejora continua que debe adaptarse dinámicamente para anticiparse a amenazas de alta complejidad, validando que el enfoque de mejora incremental del modelo es, en efecto, el camino correcto para su maduración operativa.

Complementariamente, se integró la perspectiva de un subgerente del sector previsional, cuya visión aporta un matiz centrado en la viabilidad operativa y la experiencia del usuario. Desde esta óptica, si bien se reconoce la necesidad imperativa de securitizar los accesos, se advierte que cualquier política de seguridad en entidades de alta sensibilidad social debe equilibrar el control con la usabilidad del servicio. El experto destaca que la gestión del cambio es, posiblemente, el componente más desafiante: una seguridad técnica perfecta resulta inoperante si genera fricción desmedida en el ciudadano que requiere realizar consultas sobre sus fondos de pensiones. Bajo este enfoque, el modelo GCAMTI es valorado positivamente por su carácter flexible, dado que permite alinear la robustez técnica del modelo anterior con los tiempos de respuesta y la calidad de atención que el cliente espera de una institución previsional. Así, mientras el experto en ciberseguridad demanda endurecimiento técnico, el experto operativo enfatiza la importancia de una adopción gradual, validando que el enfoque holístico del modelo es indispensable para que los protocolos de seguridad sean percibidos como un valor agregado y no como una barrera burocrática para el usuario final.

Finalmente, la validación se complementó con la visión de un experto en ciberseguridad del sector de telecomunicaciones, quien aporta una mirada enfocada en la escalabilidad masiva y la resiliencia de los canales. A diferencia de los modelos cerrados, el experto subraya que, en un entorno de alta disponibilidad como “las telcos”, el diseño propuesto debe asegurar que el endurecimiento de la seguridad no comprometa la latencia ni la capacidad de respuesta ante picos de demanda. Su juicio refuerza que la virtud del modelo GCAMTI reside en su estructura escalable, la cual permite implementar controles de seguridad de manera modular sin desestabilizar la infraestructura core. El experto coincide con la premisa de la mejora continua mediante el ciclo PDCA, enfatizando que, en un ecosistema donde la superficie de ataque es dinámica, la seguridad debe integrarse de forma invisible para el usuario, manteniendo la integridad del proceso. Con esto, se ratifica que el enfoque evolutivo es la clave para transitar de una mesa de servicio tradicional a una infraestructura de atención resiliente, capaz de proteger la información del cliente final bajo cualquier condición de carga operativa.

Cada especialista priorizó demandas propias de su industria, el fortalecimiento de controles técnicos en la banca, la mitigación de la fricción en el sector previsional y la alta disponibilidad sin latencia en las telecomunicaciones, sus evaluaciones convergen en una premisa central: la verdadera resiliencia en canales de atención no se logra imponiendo barreras infranqueables, sino mediante una gestión del cambio equilibrada.

A partir de la integración de los hallazgos del piloto operativo y el juicio de los expertos sectoriales, se presenta la matriz de trazabilidad que evalúa el grado de cumplimiento de la hipótesis del trabajo de tesina.

Tabla 6 Matriz consolidado de validación hipótesis

Atributo de la Hipótesis	**Evidencia Empírica y Operativa Obtenida**	**Nivel de Validación**	**Brechas Pendientes / Oportunidades de Mejora (Próximo PDCA)**
Holístico (Integración equilibrada de Personas, Procesos y Tecnología)	Articulación exitosa entre Jefaturas, Soporte, Ciberseguridad y Ejecutivos (Personas); despliegue de la Matriz de Controles de Identidad sin alterar la infraestructura base (Procesos); e integración funcional de IVR persuasivo y MFA/OTP dinámico (Tecnología).	Avanzado	Centralizar la impartición de capacitaciones bajo una unidad única para evitar heterogeneidad en el entrenamiento. Unificar la estrategia comunicacional con áreas comerciales en futuros cambios
Evolutivo (Mejora continua basada en el ciclo PDCA y retroalimentación)	Identificación temprana de la higiene de datos como prerrequisito crítico. Adaptación del modelo tras la evaluación de expertos externos (Banca, Previsional, Telco) incorporando requerimientos de madurez futura (TOTP, SIEM, WAF).	Intermedio	Requiere un periodo de observación más prolongado en las fases CHECK y ACT para consolidar métricas cuantitativas de largo plazo. Implementar saneamiento profundo e independiente de las bases de datos
Flexible (Adaptabilidad operativa y mitigación de la fricción	Ajuste sobre la marcha en la estrategia formativa de la primera línea. Capacidad de equilibrar el rigor de autenticación con la usabilidad en el canal previsional/comercial, evitando la interrupción del servicio.	Avanzado	Optimizar la ralentización en los tiempos de resolución iniciales provocada por la curva de aprendizaje de los agentes y la aplicación de la matriz de validación.
Escalable (Diseño modular con capacidad de expansión)	Implementación modular de controles por canal (OTP en Portal, IVR en Call Center) sin colapsar la infraestructura existente ni generar latencia en la atención, validado bajo estándares de alta disponibilidad.	Intermedio	Superar las limitaciones técnicas basales del canal telefónico migrando progresivamente de IVR disuasivo hacia mecanismos robustos (App/MFA). Habilitar licenciamiento integral de BI para analítica avanzada

Como se resume en la matriz, la propuesta GCAMTI alcanza un nivel Avanzado en sus atributos Holístico y Flexible, demostrando que la integración de la tríada PPT eleva la postura de ciberseguridad adaptándose a la realidad operativa de la primera línea. Por su parte, los atributos Evolutivo y Escalable se posicionan en un nivel Intermedio, reflejando que el modelo cuenta con la arquitectura adecuada para crecer, quedando su consolidación supeditada a la resolución de las brechas técnicas y de datos identificadas para las próximas iteraciones del ciclo PDCA.