CAJA DE COMPENSACIÓN FAMILIAR COMPENSAR

CAPÍTULO TÉCNICO

TÉRMINOS DE REFERENCIA

OPTIMIZACIÓN Y SEGURIDAD EN LOS PROCESOS DE AUTENTICACIÓN, CONTROL DE ACCESO Y VALIDACIÓN DE IDENTIDAD EN LA CAJA DE COMPENSACIÓN FAMILIAR COMPENSAR EN LOS NEGOCIOS DE CAJA Y SALUD

BOGOTÁ D.C. NOVIEMBRE DE 2025

TABLA DE CONTENIDO

1. CONDICIONES DE PRESENTACIÓN Y EVALUACIÓN CAPITULO TECNICO 3

2. INFORMACIÓN DE REFERENCIA 5

3. OBJETIVO Y ALCANCE 6

3.1 DESCRIPCIÓN EXISTENTE 8

4. RESPONSABILIDADES 9

5. ANEXOS 10

1. CONDICIONES DE PRESENTACIÓN Y EVALUACIÓN CAPITULO TÉCNICO - 5

El proponente deberá diligenciar cada requerimiento incluyendo una de las siguientes opciones, conforme al anexo técnico: **CUMPLE, NO CUMPLE, CUMPLE CON LIMITACIONES o SUPERA EL REQUERIMIENTO.** La selección debe estar debidamente sustentada cuando aplique, con evidencia objetiva que respalde la declaración. El hecho de declarar “CUMPLE” o “SUPERA EL REQUERIMIENTO” implica que el proveedor entiende completamente el requerimiento, lo acepta y se compromete a cumplirlo en su totalidad conforme a lo solicitado**,** seguido por la respuesta detallada a cada numeral, esto se aplicará tanto en el marco de la presente invitación.

El proponente debe tener en cuenta que las respuestas que suministre en este capítulo deben corresponder con los servicios que se compromete a prestar, constituyéndose en parte de su propuesta. El Proponente debe mencionar explícitamente cuándo un servicio o una característica de este no será entregada, de lo contrario, se asumirá que la misma forma parte de la presentación y propuesta y así será exigida.

El Proponente debe explicar la forma en que cumple con cada requerimiento. COMPENSAR podrá solicitar el pronunciamiento o explicaciones respectivas durante la etapa de estudio de propuestas, sin que con ocasión de las respuestas pueda modificar la propuesta.

COMPENSAR no aceptará que las respuestas a los requerimientos sean referidas a anexos, catálogos o publicaciones del Proponente, debe darse explicación clara y concreta en el texto mismo de la respuesta respectiva. Cualquier información adicional que se referencie no puede modificar, derogar ni contradecir lo contenido en la respuesta punto a punto. En cualquier caso, primará la respuesta dada a continuación de cada requerimiento sobre el contenido de las referencias o de respuestas suministradas en otro numeral.

Si la respuesta al requerimiento es evasiva, si no se suministra la aclaración o explicación solicitada, o si a pesar de haberse expresado “CUMPLE”, de la respuesta recibida se deduce que el requerimiento no se satisface total o parcialmente, o su cumplimiento se sujeta a condición, la presentación y propuesta será descartada.

Los documentos exigidos en el presente capítulo que no hayan sido aportados con la propuesta podrán ser requeridos durante la etapa de estudio de la exploración. De no atenderse el requerimiento, se aplicará lo dispuesto en el párrafo anterior.

La respuesta a las especificaciones técnicas de este capítulo **debe mantener la numeración,** con índice que contenga la relación de todos los numerales y anexos que la conforman, la respuesta debe darse inmediatamente después del requerimiento, en forma completa, clara y respondiendo a lo solicitado de manera específica. De no cumplirse este requerimiento, COMPENSAR procederá a solicitar al proponente la entrega de la propuesta cumpliendo con los requisitos aquí definidos, lo que podrá ser subsanado en un tiempo no mayor a dos días hábiles. Si al recibirse el documento corregido presenta los mismos errores e inconsistencias en la presentación, la propuesta será rechazada en forma definitiva.

La información entregada en medio digital deberá entregarse en carpetas claramente identificadas y en la misma forma en que fueron entregados los documentos del RFI. Los documentos escaneados deben ser completamente legibles y debe ser posible para COMPENSAR realizar búsqueda de palabras e información para facilitar la lectura y entendimiento de estos.

Todos los documentos que integren la propuesta deben ser redactados en idioma español, a excepción de los que contengan información técnica, los cuales pueden ser presentados en inglés. Si se presenta información técnica en idioma inglés y español conjuntamente, en caso de discrepancia prevalecerá la información suministrada en español.

2. INFORMACIÓN DE REFERENCIA - 1

COMPENSAR es una entidad privada, sin ánimo de lucro, dedicada a la protección social integral. Su compromiso con el bienestar de los trabajadores, sus familias y poblaciones vulnerables contribuye directamente al fortalecimiento de la productividad empresarial y a la construcción de una sociedad más saludable, equitativa y con igualdad de oportunidades. Su portafolio de servicios abarca áreas clave como Caja de compensación familiar, salud, educación, turismo, vivienda, empleo recreación y formación deportiva.

En este contexto, COMPENSAR adelantará la exploración de un Plataforma Omnicanal de validación y autenticación de identidad. Esta iniciativa se desarrollará conforme a los términos y alcances definidos en el presente documento. Las soluciones evaluadas se validarán de acuerdo con los componentes tecnológicos existentes en la organización, asegurando su alineación permanente con los objetivos de negocio, la generación de valor y el cumplimiento de sus metas estratégicas.

La información proporcionada por COMPENSAR no implica compromiso alguno en relación con el dimensionamiento o diseño definitivo de la solución. Corresponde al proponente estructurar una oferta técnica que atienda de manera integral los requerimientos definidos en cada línea de los presentes términos de referencia, considerando las particularidades de la operación de TI de la entidad y contemplando mecanismos de ajuste o cambio de acuerdo con las variables específicas de cada línea propuesta.

Toda la información generada y compartida dentro del proceso de exploración será confidencial y de propiedad exclusiva de COMPENSAR. Esto incluye, sin limitarse a: modelos, protocolos, formularios, formatos, listas de chequeo, procedimientos, propuestas y demás elementos utilizados dentro del proceso, los cuales harán parte del Sistema de Información de la entidad.

COMPENSAR tiene como propósito identificar y evaluar soluciones tecnológicas para mecanismos de identidad y autenticación de identidad, que permitan optimizar procesos de autenticación, control de acceso y validación de identidad en los servicios ofrecidos por COMPENSAR. La solución debe garantizar alta precisión, seguridad en el manejo de datos

biométricos, facilidad de integración con sistemas existentes y escalabilidad para su implementación.

A continuación, se presenta una topología general de COMPENSAR para contexto y alcance de la solución:

3. OBJETIVO Y ALCANCE - 2

Explorar, evaluar y definir los requerimientos técnicos, operativos y de seguridad necesarios para implementar una Plataforma Omnicanal de verificación y autenticación de identidad que permita optimizar procesos de identificación y autenticación de usuarios, fortaleciendo la eficiencia organizacional, la experiencia del usuario y la protección de la identidad digital en los servicios digitales y presenciales de Compensar.

Objetivos específicos:

- Identificar los casos de uso prioritarios donde los mecanismos de verificación y autenticación de identidad aporte valor (acceso a sedes, validación de identidad en trámites, control de asistencia, etc.).
- Analizar las tecnologías disponibles en el mercado, sus capacidades, costos, escalabilidad y compatibilidad con los sistemas actuales
- Establecer criterios técnicos de evaluación: precisión, velocidad de procesamiento, tolerancia a condiciones ambientales, interoperabilidad, etc.
- Determinar los requisitos de infraestructura (hardware, software, conectividad) para una implementación piloto y futura escalabilidad.
- Evaluar los riesgos éticos, legales y de privacidad asociados al tratamiento de datos biométricos, conforme a la normativa vigente (como la Ley 1581 de protección de datos en Colombia).

- Diseñar un plan de pruebas piloto que permita validar la solución en escenarios reales con usuarios representativos.

La propuesta deberá incluir licenciamiento, integración con plataformas existentes, soporte técnico especializado y administración continua durante la operación, garantizando visibilidad centralizada, respuesta ante incidentes, mantenimiento evolutivo y protección proactiva de los activos en la nube.

Mecanismos de validación y autenticación de identidad:

Mecanismo	Descripción
Verificación de documentos	Validar la autenticidad de documentos oficiales (como pasaportes, licencias, identificaciones) mediante escaneo, análisis visual o comparación con bases de datos gubernamentales.
Verificación basada en conocimientos (KBA)	El usuario responde preguntas personales o históricas para confirmar su identidad.
Autenticación biométrica	Utiliza características físicas únicas del usuario (huellas dactilares, rostro, iris, voz) para verificar su identidad.
Verificación de bases de datos	Cruza información proporcionada por el usuario con registros en bases de datos oficiales o privadas (por ejemplo, registros civiles, bancarios, educativos).
Verificación basada en comportamiento	Analiza patrones de comportamiento como la forma de escribir, mover el mouse o usar el dispositivo para identificar al usuario.
PIN	Código numérico secreto que el usuario debe ingresar para autenticarse.
OTP por SMS o correo	Un código de un solo uso (One-Time Password) enviado al teléfono o correo electrónico del usuario para confirmar su identidad.
OTP por aplicaciones	Aplicaciones como Google Authenticator o Authy generan códigos temporales que el usuario debe ingresar para autenticarse.
Magic link	Un enlace único enviado por correo electrónico que, al hacer clic, autentica automáticamente al usuario sin necesidad de contraseña.

Tokens FIDO2/WebAuthn	Dispositivos físicos o software que permiten autenticación sin contraseña, usando criptografía de clave pública. Son altamente seguros.
Passkeys almacenadas en nube (iCLoud Keychain)	Credenciales criptográficas guardadas en servicios en la nube, que permiten autenticación sin contraseña desde múltiples dispositivos.
Passkeys almacenadas en hardware local (TPM)	Las claves se guardan en el hardware del dispositivo (como el Trusted Platform Module), lo que mejora la seguridad al evitar el acceso remoto.
Autenticación móvil con desafío criptográfico	El servidor envía un desafío que el dispositivo móvil firma con una clave privada, confirmando la identidad del usuario sin compartir la clave.
Biometría en dispositivos personales (Face ID, Touch ID)	Autenticación local en el dispositivo usando reconocimiento facial o huella digital, sin necesidad de enviar datos biométricos al servidor.
Biometría con respaldo criptográfico (WebAuthn, FIDO2)	Combina biometría con claves criptográficas para autenticación segura, sin compartir datos biométricos con el servidor.

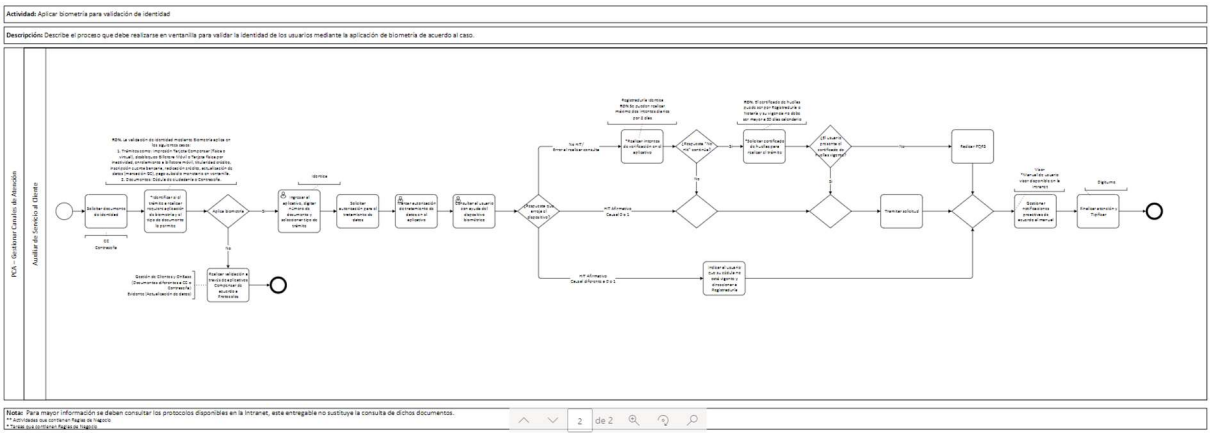
3.1 DESCRIPCIÓN EXISTENTE -

Actualmente, la organización opera con:

- Un servicio de BPO para reconocimiento facial como mecanismo de contingencia para el proceso de validación de identidad en la colocación de créditos.

- **Acceso a gimnasios:** Solución tecnológica que permite brindar acceso, vía control biométrico a los gimnasios de manera ágil para el usuario y segura para Compensar

- **Validación dactilar con dispositivos:** Se confirma la identidad por medio de la huella dactilar para asegurar que la persona que realiza una acción es el titular legitimo de la identidad asociada.



4. RESPONSABILIDADES - 4

Para cada uno de los requerimientos definidos en esta propuesta, el proponente deberá demostrar capacidad técnica, operativa y de ejecución, acorde con el alcance establecido.

Ver archivo "Anexo técnico_funcional Plataforma de verificación y autenticación de identidad"

5. ANEXOS

El proponente deberá entregar completamente diligenciados los Anexos requeridos, conforme a los formatos establecidos y dentro de los plazos definidos.

- Anexo técnico_funcional Plataforma de verificación y autenticación de identidad
- Checklist de Ciberseguridad
- for-prc-0017_checklist_de_seguridad_para_la_adquisicion_de_sistemas_de_informacion