Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería Informática

Diseño de un sistema de gestión de identidades y accesibilidad en el Banco Itaú de Chile - 2024

Tesis

Para optar el Título Profesional de Ingeniero Informático

Autor

Jheisson Victor Rios Flores

Asesor

Dr. Alcibiades Flamencio Sosa Palomino

Huacho-Perú

2026

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo Nº 012-2020-SUNEDU/CD de fecha 27/01/2020)

Facultad de Ingeniería industrial, Sistema e Informática
Escuela Profesional de Ingeniera Informática

INFORMACIÓN DE METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Rios Flores Jheisson Victor	72621073	16-07-2026
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Alcibíades Flamencio Sosa Palomino	15610364	https://orcid.org/0000-0002-0509-1998
DATOS DE LOS MIEMBROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Armas Inga Moises Emilio	10057606	https://orcid.org/0000-0002-8320-5209
Cerna López Walter César	43468609	https://orcid.org/0000-0001-8123-1449
Galdós Felipe Jóse Antonio	15760821	https://orcid.org/0000-0003-4160-6925

Jheisson Víctor Ríos Flores

Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile - 2024

UNIDAD DE INVESTIGACIÓN FIISI - PREGRADO 2026

Unidad de Investigación de la FIISI - 2026

Facultad de Ingeniería Industrial, Sistemas e Informática

Detalles del documento

Identificador de la entrega
trn:oid:::1:3605305424

Fecha de entrega
2 jul 2026, 12:44 p.m. GMT-5

Fecha de descarga
2 jul 2026, 12:47 p.m. GMT-5

Nombre del archivo
TESIS_JHEISSON_RIOS_FLORES.pdf

Tamaño del archivo
4.3 MB

106 páginas

16.417 palabras

103.819 caracteres

turnitin Página 1 de 114 - Portada Identificador de la entrega: trn:oid:::1:3605305424

turnitin Página 2 de 114 - Descripción general de integridad Identificador de la entrega: trn:oid:::1:3605305424

19% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Fuentes principales

18% Fuentes de Internet

10% Publicaciones

13% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.° de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que generarían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dedicatoria

Dedico mi proyecto de tesis a Dios,
a mi mamá y papá y en especial a
mi abuelita en el cielo.

Jheisson Víctor Ríos Flores

Agradecimiento

Agradezco al Ing. Alcibiades Flamencio Sosa Palomino, mi asesor de tesis, por compartir generosamente sus conocimientos, y guiarme en todo el proceso para culminar mi tesis.

Jheisson Víctor Ríos Flores

ÍNDICE

ANEXOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El trabajo de investigación tuvo como propósito evaluar la relación entre el diseño de un sistema de gestión de identidades y la accesibilidad en el Banco ITAÚ de Chile. La propuesta se fundamenta en la centralización del usuario y sus cuentas en un único punto de control de acceso, aplicando el modelo RBAC para la asignación automática de permisos según el rol de cada colaborador, autenticación validada con políticas de contraseña unificada reforzada mediante autenticación, flujos de automatización que se genera de manera automática en todo el ciclo de vida de las identidades y con una correcta segregación de funciones, implementados mediante la plataforma IBM Verify Identity Governance (IVIG) como solución integral de gobierno de identidades. Esta investigación es aplicada, con un enfoque de tipo cuantitativo, diseño no experimental de corte transversal y nivel correlacional. La muestra estuvo compuesta de 14 empleados que pertenecen al área de seguridad de la información. Se aplicó una encuesta mediante un cuestionario en escala Likert. El cuestionario fue validado por expertos y alcanzó una confiabilidad aceptable, con un Alfa de Cronbach superior a 0,80.

Los resultados evidencian que el diseño del sistema de gestión de identidades propuesto se relaciona significativamente con la accesibilidad, obteniéndose un coeficiente de Rho de Spearman r = 0,984, con un valor p menor a 0,001, inferior al criterio de 0,05, lo que permitió aceptar la hipótesis general. En ese sentido, se concluye que el diseño propuesto mejora la accesibilidad tecnológica al garantizar autenticación segura, autoservicio y compatibilidad con sistemas corporativos; fortalece la accesibilidad organizacional mediante roles, jerarquías y documentación estructurada; y optimiza el control de accesos asegurando trazabilidad, privilegios mínimos y auditoría centralizada.

Palabras clave: Gestión de identidades, accesibilidad, RBAC, autenticación, control de accesos.

ABSTRACT

The purpose of this research was to evaluate the relationship between the design of an identity management system and accessibility at Banco ITAÚ in Chile. The proposal is based on centralizing the user and all associated accounts into a single access control point, applying the RBAC model to automatically assign permissions according to each employee's role, authentication validated against Active Directory with a unified password policy reinforced through multifactor authentication (MFA), automated workflows generated automatically throughout the identity lifecycle, and proper segregation of duties. These were implemented using the IBM Verify Identity Governance (IVIG) platform as a comprehensive identity governance solution.

This applied research employed a quantitative approach, a non-experimental, cross-sectional design, and a correlational level of analysis. The sample consisted of 14 employees from the access control area. A Likert-scale questionnaire was administered. The questionnaire was validated by experts and achieved acceptable reliability, with a Cronbach's alpha greater than 0.80.

The results show that the proposed identity management system design is significantly related to accessibility, obtaining a Spearman's Rho coefficient $r = 0.984$, with a p-value less than 0.001, below the criterion of 0.05, which allowed the general hypothesis to be accepted. Therefore, it is concluded that the proposed design improves technological accessibility by ensuring secure authentication, self-service, and compatibility with corporate systems; strengthens organizational accessibility through roles, hierarchies, and structured documentation; and optimizes access control by ensuring traceability, least privilege, and centralized auditing.

Keywords: Identity management, accessibility, RBAC, authentication, access control.

INTRODUCCIÓN

El presente trabajo tuvo como propósito determinar la relación entre el diseño de un sistema de gestión de identidades y la accesibilidad en el Banco ITAÚ de Chile, durante el año 2024, siguiendo los lineamientos metodológicos y normativos de la Universidad.

La investigación inició con el análisis de la situación problemática vinculada al tema seleccionado, contextualizando el entorno internacional, nacional y local, precisando el problema de investigación, así como sus principales causas y efectos y limitaciones tecnológicas que afectan la gestión de identidades y la accesibilidad al interior de la organización.

El estudio se justifica desde un enfoque tecnológico, organizacional y normativo, delimitando el alcance en el ámbito geográfico, la población involucrada y el entorno temático, para luego mostrar la viabilidad en los aspectos técnico, operativos, económicos y metodológicos.

El marco teórico presenta los antecedentes nacionales e internacionales relacionados con las variables del estudio considerando su vigencia, donde se muestran el objetivo de las investigaciones, la metodología utilizada para su desarrollo, así mismo se muestran los resultados y conclusiones obtenidos.

Asimismo, se desarrolla las bases filosóficas para conocer con mayor profundidad el entendimiento de las variables de estudio, posteriormente se definen los principales términos considerados en esta investigación para luego armar la matriz de operacionalización, donde contemplan toda definición conceptual y operacional correspondiente a cada variable analizada mostrando sus dimensiones para su mejor entendimiento e identificando los indicadores para realizar la medición de las variables, así también se muestran las técnicas e instrumentos que

hacen posible la medición de las variables.

Posteriormente, se describe la metodología a seguir para realizar la investigación, identificando el tipo, nivel, diseño, enfoque y los métodos utilizados, sustentado por autores conocedores del tema. Se define la población conformada por los responsables y usuarios vinculados a la gestión de identidades en el Banco ITAÚ de Chile. Se utilizó un cuestionario estructurado en escala Likert para la recolección de datos.

En el desarrollo de los resultados, se describe inicialmente la empresa y, luego, se presenta el diseño del sistema de gestión de identidades. Luego, se efectuaron las pruebas de validez y confiabilidad del instrumento. Asimismo, se analizan las variables y dimensiones del estudio mediante tablas de frecuencia, gráficos e interpretaciones. Finalmente, se aplican las pruebas de hipótesis e inferenciales, demostrándose, a través del coeficiente Rho de Spearman, se evidenció una relación significativa entre ambas variables. Asimismo, se discuten los hallazgos con los antecedentes y teorías revisadas, contrastando coincidencias, diferencias y aportes relevantes.

Finalmente, se obtienen las conclusiones en función de los objetivos y los resultados obtenidos, proponiéndose recomendaciones tecnológicas y organizacionales orientadas a fortalecer el diseño del sistema de gestión de identidades y accesibilidad dentro del Banco ITAÚ de Chile.

Se adjuntan también las referencias bibliográficas correspondientes bajo el formato APA 6ª edición y los anexos documentales. Posteriormente se presenta el resumen de la investigación en idioma español e inglés, donde se muestra fundamentalmente el objetivo, metodología, resultados y conclusión del estudio.

En síntesis, el estudio se orienta a diseñar un sistema de gestión de identidades y determinar la relación con la accesibilidad en el Banco ITAÚ de Chile.

I. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática.

En el contexto de la transformación digital, la gestión de identidades ha adquirido una mayor relevancia para la seguridad informática a nivel mundial. Ali et al. (2020) señalan que la gestión de identidades (Identity Management o IAM) constituye un componente esencial para la seguridad informática, especialmente en un mundo cada vez más digitalizado, donde las organizaciones adoptan constantemente nuevas aplicaciones con nuevas tecnologías que amplían la exposición de riesgos de seguridad.

El robo de identidad representa una amenaza creciente que compromete tanto a usuarios como a organizaciones, ya que los atacantes explotan vulnerabilidades en los sistemas de autenticación para obtener acceso no autorizado a recursos críticos. Según IBM (2025), las credenciales comprometidas continúan siendo uno de los vectores de ataque inicial más frecuentes a nivel mundial, representando un 16% de los casos. En esta línea, ENISA (2025) señala que el phishing es el principal vector de acceso inicial frecuentemente usado para robar credenciales, e identifica el abuso de cuentas válidas como método común para mantener el acceso tras la intrusión, lo que evidencia la necesidad de fortalecer la autenticación multifactor (MFA) como protección mínima en el sector financiero.

La complejidad de este escenario se hace evidente cuando las organizaciones incorporan nuevas aplicaciones sin una gestión centralizada de identidades, multiplicando los puntos de acceso vulnerables a credenciales comprometidas y exponiendo los activos de información a mayores riesgos. Esto se agrava por la creciente complejidad de los entornos digitales bancarios, donde los usuarios acceden a múltiples servicios desde distintos dispositivos, cada uno con su propia credencial (Gartner, 2023). Un aspecto crítico es el aumento del fraude y los ciberataques

dirigidos a robar credenciales y suplantar identidades, lo que obliga a los bancos a equilibrar la seguridad con la usabilidad, enfrentando desafíos técnicos como la integración de múltiples soluciones de autenticación y el cumplimiento de normativas estrictas del sector financiero.

A ello se suma la fragmentación de la identidad, ya que muchos bancos aún operan con sistemas legados que no permiten una gestión centralizada ni una visión unificada del usuario, incrementando la probabilidad de credenciales duplicadas, huérfanas o no auditadas (Accenture, 2022). Un sistema legado es aquel sistema de información que continúa utilizándose dentro de una organización a pesar de haber sido desarrollado con tecnologías obsoletas o poco compatibles con los estándares actuales. Estos sistemas suelen ser difíciles de mantener, actualizar o integrar con nuevas plataformas, pero se mantienen en operación debido a que cumplen funciones críticas para el negocio, contienen datos históricos valiosos o resultaría demasiado costoso sustituirlos (Sommerville, 2011). Además, las nuevas tecnologías fortalecen el control del usuario sobre su identidad y contribuyen a una gestión más eficiente de las identidades (World Economic Forum, 2021).

En el caso de Banco Itaú, el área de seguridad de la información atraviesa un déficit en la atención de los requerimientos de gestión de accesos a nivel organizacional, debido a que actualmente sus procesos no están automatizados, generándose una atención lenta en cada uno de los requerimientos. Otro problema encontrado en la organización es no contar con una herramienta que ayude a centralizar al usuario y sus cuentas en las diversas aplicaciones corporativas lo que retrasa la atención de los requerimientos, dificulta la toma de decisiones y se ve agravado por la falta de aprobaciones oportunas de los jefes inmediatos. Es por eso que, como alternativa para esta problemática se diseña un sistema de gestión de identidades para mejorar la accesibilidad en el Banco Itaú de Chile.

1.2. Formulación del Problema

1.2.1. Problema General

¿En qué medida se relaciona el diseño de un sistema de gestión de identidades con la accesibilidad en el Banco ITAÚ de Chile?

1.2.2. Problemas Específicos

¿En qué medida se relaciona el diseño del sistema de gestión de identidades con la accesibilidad tecnológica de los usuarios en el Banco ITAÚ de Chile?

¿En qué medida se relaciona el diseño del sistema de gestión de identidades con la accesibilidad organizacional en el Banco ITAÚ de Chile?

¿En qué medida se relaciona el diseño del sistema de gestión de identidades con el control de acceso del Banco ITAÚ de Chile?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Determinar en qué medida se relaciona el diseño de un sistema de gestión de identidades con la accesibilidad en el Banco ITAÚ de Chile.

1.3.2. Objetivos Específicos

Determinar el grado de relación entre el diseño del sistema de gestión de identidades y la accesibilidad tecnológica de los usuarios en el Banco ITAÚ de Chile.

Determinar el grado de relación entre el diseño del sistema de gestión de identidades y la accesibilidad organizacional dentro del Banco ITAÚ de Chile.

Determinar el grado de relación entre el diseño del sistema de gestión de identidades y el control de acceso en el Banco ITAÚ de Chile.

1.4. Justificación de la Investigación

La gestión de identidades y accesos (IAM) adquirió relevancia estratégica en las organizaciones modernas, principalmente en las instituciones financieras, donde la protección de la información sensible fortalece la continuidad del negocio, el cumplimiento normativo y los estándares de seguridad.

En el caso del Banco Itaú de Chile, la creciente digitalización de procesos, el uso de múltiples plataformas corporativas (Active Directory, SAP, Azure AD, Core Banking, entre otras) y la incorporación de colaboradores internos y externos, demandan un sistema robusto que centralice al usuario y sus cuentas en un único punto de control, gestionando los accesos de manera automatizada, auditable y alineada con las políticas organizacionales y normativas vigentes.

El análisis de la relación entre ambas variables permitió determinar cómo un diseño basado en roles (RBAC), una política de contraseña unificada reforzada con autenticación multifactor (MFA) y criterios de gobernanza se vincula con la ciberseguridad, el acceso seguro y oportuno a los recursos tecnológicos, la eficiencia operativa y la trazabilidad organizacional.

Desde una perspectiva académica, esta investigación brinda un modelo replicable en otras organizaciones que buscan implementar soluciones de IAM basadas en plataformas empresariales como IBM Verify Identity Governance (IVIG).

1.5. Delimitación del Estudio

a) Delimitación geográfica

Este trabajo de investigación fue realizado en el Banco ITAÚ de Chile, en el área de seguridad de la información, responsable de la administración de credenciales, los procesos de autenticación y el control de acceso a las aplicaciones. No se consideraron otras sedes del Banco Itaú en otros países.

b) Delimitación poblacional

La investigación se aplicó a 14 colaboradores vinculados directamente a los procesos de administración de identidades, control de accesos, cumplimiento normativo y soporte tecnológico.

c) Delimitación temática

La investigación se centró en el diseño de un sistema de gestión de identidades y su relación con la accesibilidad, considerando componentes como la centralización del usuario y sus cuentas en un único punto de control de acceso, la autenticación multifactor (MFA), el control de acceso basado en roles (RBAC), la gestión de altas, modificaciones y bajas de usuarios, la automatización de permisos, la auditoría y el cumplimiento normativo.

1.6. Viabilidad del Estudio

La investigación resultó factible desde las perspectivas técnica, operativa, económica y metodológica. Desde el punto de vista técnico, se contó con acceso a información relevante sobre los procesos desde la administración de las identidades,

los criterios de gestión de permisos, la estructura organizacional del Banco ITAÚ de Chile, lo que permitió elaborar una propuesta sustentada. Fue operativamente viable debido a la participación efectiva de los 14 colaboradores del área de seguridad de la información, quienes proporcionaron datos fundamentales mediante el cuestionario estructurado. Económicamente, el estudio no generó costos significativos, pues se emplearon herramientas conceptuales, fuentes bibliográficas digitales y encuestas electrónicas. Finalmente, desde la perspectiva metodológica, el estudio fue factible al sustentarse en un enfoque cuantitativo, con diseño no experimental y método correlacional. Asimismo, se empleó un cuestionario con escala Likert previamente validado, alineado con las variables gestión de identidades y accesibilidad, lo que permitió asegurar la validez y confiabilidad de los resultados obtenidos.

II. MARCO TEORICO

2.1. Antecedentes de la investigación

2.1.1. Investigaciones internacionales

Glöckler et al. (2024), en su publicación denominada "*Una revisión sistemática de los requisitos de gestión de identidades y accesos en empresas y las posibles contribuciones de la identidad auto soberana*", publicado en la revista Business & Information Systems Engineering por la editorial Springer Fachmedien Wiesbaden GmbH (Alemania), tuvieron como objetivo identificar y clasificar los principales requerimientos de IAM en el contexto organizacional.

La investigación adoptó un enfoque de Design Science Research (DSR) y realizo en tres etapas: primero, se realizó una revisión sistemática de la literatura especializada; luego, se efectuó un análisis basado en entrevistas a expertos; y finalmente, se diseñó y evaluó un prototipo de identidad autogestionada, el cual fue validado con la participación de 12 especialistas.

Los resultados obtenidos ayudaron con la agrupación de todos los requisitos de IAM en las siguientes categorías principales: seguridad y cumplimiento, operabilidad, aspectos tecnológicos y factores relacionados con los usuarios. Asimismo, el prototipo desarrollado mostró que la identidad autogestionada contribuyó a mejorar la manejabilidad y la usabilidad de los sistemas IAM y facilitó la aplicación de buenas prácticas, como el principio de menor privilegio. Sin embargo, se evidenció que esta aproximación no resolvió de manera integral todos los desafíos presentes en la gestión de identidades empresariales.

Finalmente, el estudio concluyó que la identidad autogestionada aportó beneficios claros en términos de usabilidad y gestión de identidades y resultó prometedora para determinados casos de uso empresariales.

Olabanji et al. (2024), en el estudio abordado sobre la *"La inteligencia artificial aplicada a la gestión de identidades y accesos en la nube"*, publicado en SSRN Electronic Journal, perteneciente a SSRN – Social Science Research Network / Elsevier Inc. (Estados Unidos), analizaron el uso de la inteligencia artificial en las plataformas de gestión de identidades y accesos utilizados en infraestructura cloud. Tuvo como objetivo evaluar como la inteligencia artificial podría mejorar los procesos de autenticación, autorización y control de acceso en sistemas IAM basados en la nube. Con ese propósito, los autores emplearon una revisión crítica de la literatura y un análisis conceptual, acorde con la naturaleza de un working paper publicado en SSRN, en el cual se identificaron diversas técnicas de inteligencia artificial aplicables a IAM, tales como el aprendizaje supervisado y no supervisado para la biometría comportamental, el análisis de anomalías y los esquemas de autenticación continua y contextual.

Los resultados evidenciaron que la inteligencia artificial permitió implementar mecanismos de autenticación adaptativa y continua, como la biometría comportamental y el análisis contextual, así como mejorar la detección temprana de anomalías y reducir la ocurrencia de falsos positivos. Finalmente, el estudio concluyó que la inteligencia artificial potenció los sistemas IAM, especialmente en entornos de computación en la nube y arquitecturas distribuidas, siempre que fuera implementada junto con controles adecuados de privacidad, transparencia de los modelos, validación continua y mecanismos de mitigación de sesgos, por lo que se recomendó la adopción de marcos de gobernanza de datos y auditoría de algoritmos.

Riasat et al. (2025), en el artículo titulado *"Fortaleciendo la resiliencia cibernética: Un análisis sobre la adopción de herramientas de seguridad emergentes en aplicaciones de banca móvil"*, publicado por MDPI – Multidisciplinary Digital Publishing Institute en la revista Computers (Suiza), los autores analizaron los factores que influyeron en la adopción de herramientas de seguridad emergentes por parte de los usuarios de aplicaciones de banca móvil. El estudio tuvo como objetivo investigar los elementos que condicionaron la aceptación de mecanismos de seguridad como la biometría, la autenticación multifactor (MFA), las alertas basadas en inteligencia artificial o SMS y el uso de contraseñas robustas.

La investigación se desarrolló mediante un enfoque cualitativo, en el cual se realizaron 22 entrevistas semiestructuradas a usuarios de banca móvil, empleando técnicas de muestreo por criterio y bola de nieve. Posteriormente, la información recopilada fue analizada a través de un análisis temático apoyado en la herramienta NVivo.

Los resultados mostraron que la adopción de las herramientas de seguridad por parte de los usuarios estuvo principalmente por la facilidad de uso de estos mecanismos de seguridad, el grado de confianza generado por la aplicación y la agilidad del acceso. Asimismo, se evidenció que la biometría y las alertas basadas en inteligencia artificial o mensajes SMS fueron bien aceptadas por los usuarios, mientras que la autenticación multifactor, a pesar de ser percibida como un mecanismo más seguro, presentó una menor adopción debido a la falta de conocimiento y concienciación por parte de los usuarios.

Finalmente, el estudio concluyó que las instituciones financieras necesitaron implementar campañas de concienciación en seguridad, mejorar la experiencia de usuario mediante la integración transparente de la autenticación multifactor y adoptar estrategias

centradas en la confianza y la usabilidad, con el fin de incrementar la adopción de controles IAM más robustos. Si bien el estudio fue realizado en Pakistán, los autores señalaron que sus hallazgos tuvieron implicancias prácticas relevantes para la industria bancaria a nivel global.

Schlatt et al. (2022), en el estudio denominado *"Diseño de un marco para procesos digitales KYC basados en identidad autosoberana sobre blockchain"*, publicado por Elsevier B.V. en la revista Information & Management (Países Bajos), desarrollaron un marco conceptual orientado a optimizar los procesos digitales de *Know Your Customer* (KYC) en el sector bancario mediante el uso de identidad autosoberana (Self-Sovereign Identity, SSI) soportada sobre tecnologías de *ledger* distribuido. El estudio tuvo como objetivo diseñar un marco que permitiera reducir los costos operativos, las fricciones en la experiencia del cliente y los problemas asociados a la privacidad de los datos en los procesos tradicionales de KYC.

Metodológicamente, se basó en un enfoque de Design Science Research, en el cual se analizó el problema del KYC desde las perspectivas regulatoria y operativa, se diseñó un marco SSI aplicado a los procesos KYC y se derivaron principios de diseño orientados a su implementación. Asimismo, los autores realizaron un prototipado conceptual del marco propuesto y discutieron sus características y viabilidad con especialistas del sector.

Los resultados evidenciaron que el marco basado en identidad autosoberana permitió que el propio cliente gestione sus credenciales de identidad, reduciendo la duplicidad de verificaciones entre entidades financieras y fortaleciendo la protección de los datos personales mediante credenciales verificables y esquemas de almacenamiento fuera de la cadena (off-chain). Además, se plantearon principios de diseño orientados a compatibilizar el uso de tecnologías blockchain con los requerimientos de protección de datos personales.

Finalmente, se concluyó que la identidad autosoberana representa una alternativa viable para la digitalización y mejora de los procesos KYC en la banca, debido a su contribución en la reducción de costos y en el fortalecimiento de la privacidad del cliente.

Olivares (2019), en el estudio denominado *"Elementos para una metodología de gestión de identidad digital en la empresa"*, desarrollado en un centro de investigación e innovación tecnológica en México, propuso una metodología orientada a gestionar la identidad digital en pequeñas y medianas empresas mexicanas.

El objetivo principal de la tesis consistió en proponer un enfoque de gestión de identidad digital aplicable a las pequeñas y medianas empresas, incorporando componentes técnicos y normativos que, según la autora, no habían sido considerados de manera integral en las soluciones existentes.

El estudio se desarrolló en un planteamiento investigativo que se basa en el análisis documental y también una revisión bibliográfica. Para ello, se evaluaron estudios de caso realizados en México y en otros países, así como estándares internacionales vinculados con la identidad digital. Con base en el análisis de la literatura especializada y de los marcos normativos vigentes, se formuló la propuesta metodológica presentada en la tesis.

Los resultados evidenciaron que las soluciones de identidad digital disponibles en ese momento no incorporaron de manera suficiente aspectos normativos y técnicos relevantes para la realidad de las PYMES mexicanas A partir de los hallazgos obtenidos, la autora identificó un conjunto de elementos fundamentales para el diseño de una metodología de gestión de identidad digital, integró perspectivas tecnológicas como la gestión de credenciales digitales junto con consideraciones normativas propias del contexto mexicano y propuso un esquema

de gestión adaptado al entorno empresarial local, con un enfoque orientado a la innovación en la gestión de la información.

Finalmente, la tesis concluyó que la gestión de la identidad digital en las empresas debió ser abordada desde un enfoque estratégico, considerando de manera conjunta la infraestructura tecnológica y el cumplimiento de normas nacionales e internacionales. Asimismo, se determinó que la metodología propuesta ofreció un marco orientador que permitió a las PYMES estructurar su gestión de identidad digital, con potencial de extensión hacia otros ámbitos, como el sector público y el comercio.

2.1.2. Investigaciones nacionales

Mendoza y Paucar (2023), ambos autores del estudio denominado *"Diseño de un sistema de administración y gobierno de identidades en una entidad financiera en el Perú"*, desarrollada en la universidad UPC para optar el título de Ingeniero, plantearon una solución de gobierno de identidades para una entidad financiera peruana. Su propósito del estudio fue realizar la integración de dos plataformas que facilitaran la administración y gobierno de identidades, con la finalidad de atender las disposiciones establecidas por la Superintendencia de Banca, Seguros y AFP (SBS), como organismo regulador del sistema financiero.

El estudio se sustentó en una metodología orientada a identificar los supuestos y requisitos establecidos en el reglamento de seguridad de la SBS. A partir de ello, los autores definieron los módulos y flujos requeridos para la gestión de identidades y accesos, además de comparar las funcionalidades de diversas soluciones disponibles en el mercado.

Los resultados evidenciaron que el sistema propuesto permitió administrar y controlar eficazmente el acceso en la entidad financiera, alcanzando un 86 % de cumplimiento de las subcategorías de los estándares de la NIST. Finalmente, se concluyó que la puesta en marcha de la aplicación contribuiría al fortalecimiento de la seguridad y al cumplimiento regulatorio de la entidad financiera.

Díaz y Muñoz (2023), en el trabajo de investigación titulado *"Sistema de control biométrico para la gestión de accesos de empleados de un hospital en Moyobamba"*, desarrollada en la sede la Universidad Cesar Vallejo para el grado de ingeniero, se evaluó la importancia de implementar una solución biométrica para la administración de accesos del

personal hospitalario. El objetivo de la investigación es determinar de qué manera el uso de un sistema de control biométrico mejorará en la administración de los accesos del personal del hospital.

La investigación desarrollada es aplicada, de nivel explicativo y diseño preexperimental. La muestra es de 14 trabajadores, cinco pertenecen al área de RRHH y nueve al área de Tecnologías de Información. Para la recolección de datos, los autores utilizaron un cuestionario y una ficha de observación.

A partir de los resultados se evidenciaron una significancia de 0,001, se ubica por debajo del criterio de aceptación establecido de 0.05, lo que evidenció que la plataforma tuvo una satisfacción positiva y considerable en la gestión de accesos.

Finalmente, se concluyó que la solución biométrica optimizó la administración de accesos del personal, contribuyendo al aumento de la seguridad y la eficiencia en los procesos del hospital.

Racacha (2024), en su trabajo de investigación titulado *"Diseño de un sistema de gestión de datos biométricos, y el control de asistencia de la I.E.P. Nuestra Señora del Carmen, Huacho – 2023"*, realizada en la Universidad Nacional José Faustino Sánchez Carrión para el grado de ingeniero, evaluó la relación entre la variable diseño de un sistema de gestión de datos biométricos y la variable control de asistencia en la Institución Educativa. El objetivo es determinar el grado de relación que existe entre las dos variables.

La investigación es de tipo cuantitativo, alcance correlacional y diseño no experimental. La muestra se conformó por 51 estudiantes de secundaria. Se utilizó un cuestionario estructurado en escala Likert para la obtención de datos.

Como parte final se obtuvo un resultado de la investigación nos arroja que un 58.80 % de estudiantes consideró que el diseño de la solución de administración biométrica presentó un grado de aceptación alto, el porcentaje restante de estudiantes calificó la variable en un nivel medio, representando el 41,20 %. Asimismo, el análisis estadístico mostró una asociación significativa entre las variables estudiadas, con un valor de correlación de 0,826 obtenido según el análisis de Spearman. Finalmente, se concluyó que ambas variables presentaron una relación significativa en la institución educativa.

Contreras y Vega (2019), en el trabajo de investigación denominado *"Implementación de un sistema de gestión de identidades privilegiadas para el control de acceso en una empresa de retail"*, elaborada en la Universidad de San Martín de Porres (USMP) para el grado de ingeniero. El objetivo fue reducir los riesgos internos de seguridad informática a través de la puesta en marcha de un sistema que permitiera una gestión adecuada de contraseñas y un control efectivo de los accesos privilegiados.

La investigación se desarrolló inicialmente de un análisis de cómo se encontraba la empresa respecto a la seguridad de la información. Sobre esta base, los autores diseñaron e implementaron una plataforma que los ayudaran en su gestión de cuentas privilegiadas, en el cual se aplicaron normativas de seguridad y controles de acceso basados en roles.

Los resultados evidenciaron una reducción en el tiempo necesario para realizar el proceso de autenticación. Previo a la puesta en marcha del sistema, el acceso a diez dispositivos tomó en promedio 20 minutos, mientras que después de la implementación se redujo a un máximo de un minuto mediante el uso de la funcionalidad de *single sign-on*. Esta mejora permitió incrementar la eficiencia operativa al optimizar el tiempo de acceso a los sistemas.

Finalmente, los autores concluyeron que la aplicación de una solución para el gobierno de accesos privilegiados favoreció la disminución del riesgo de acceso y fuga indebida de información en los activos de TI, al incorporar un esquema de administración basado en roles y controles establecidos.

Rojas & Mendoza de los Santos (2024), en el estudio denominado *"La evolución de la gestión de la identidad (IAM) en la seguridad de la información"*, publicado en Biotech & Engineering, revista académica de la Universidad Nacional Tecnológica de Lima Sur. La investigación tuvo como finalidad mostrar una visión general y estructurada de la evolución de IAM durante las últimas décadas, enfrentando desafíos cada vez más complejos derivados del crecimiento de las plataformas o sistemas digitales.

La investigación se basó en una revisión sistemática de literatura, mediante la cual se analizaron fuentes académicas y técnicas relacionadas con la evolución de la gestión de identidades y accesos (IAM). Si bien el artículo no definió una muestra específica, se infirió que la revisión abarcó múltiples estudios, artículos académicos y documentos técnicos vinculados a la gestión de identidades y accesos.

Los resultados permitieron ordenar la información en secciones relacionadas con los principales momentos de la transformación de IAM, destacándose en puntos relevantes, mejoras tecnológicos y desafíos que a lo largo del tiempo se van superando. Asimismo, se mostraron nuevas tendencias, un resumen de las tendencias que actualmente se tiene perspectivas en el mercado y tendencias emergentes en el gobierno de identidades y accesos. El análisis resaltó la importancia de aplicar estándares y buenas prácticas de seguridad de la información en toda plataforma, así como la incorporación de tecnologías como la biometría

y la inteligencia artificial, las cuales fueron evaluadas desde un enfoque cualitativo en relación con la experiencia del usuario y su implementación en distintos sistemas especializados.

Finalmente, se concluyó que la gestión de identidades y accesos se consolidó como un pilar esencial de la seguridad de la información, al integrar mecanismos tecnológicos que fortalecen la gestión de accesos, la seguridad de los datos y la experiencia del usuario.

2.2. Bases Teóricas

2.2.1. Sistema de Gestión de identidades

La gestión de identidades permite administrar, controlar y supervisar las identidades de usuarios y entidades dentro de una organización. Se caracteriza por garantizar que cada usuario o entidad cuente con una identidad única y confiable, asociada a los permisos y restricciones correspondientes.

Mathias & Rosencrance (2021) señalan que la gestión de identidades (Identity Management o ID) es el proceso organizativo y tecnológico orientado a garantizar que las personas y procesos dispongan del acceso adecuado a los recursos de TI. Comprende en la identificación, autenticación y autorización de cada usuario que permite el acceso a las plataformas en general, asociando a cada identidad un conjunto de derechos, restricciones y condiciones de uso. Las identidades gestionadas pueden corresponder tanto a usuarios humanos (empleados, terceros, socios) como a procesos de software o servicios que requieren interactuar con sistemas corporativos.

La gestión de identidades trabaja de manera estrecha con la gestión de accesos**,** diferenciándose en que la primera responde a la pregunta "¿quién es el usuario?", mientras que la segunda aborda "¿a qué puede acceder y qué puede hacer?". Como función principal consiste en asegurar que solo los usuarios únicamente que hayan superado los procesos de autenticación y autorización puedan acceder a las plataformas, controlando el aprovisionamiento de cuentas, la incorporación de nuevos usuarios, la modificación de permisos ante cambios organizacionales y la revocación oportuna de accesos cuando dejan de ser necesarios.

Un aspecto clave de la gestión de identidades es el gobierno de identidades**,** se entiende como el conjunto de políticas, controles y procesos que definen cómo se administran los roles, los permisos y las reglas de acceso en la organización. Este modelo de gobierno de identidades como buenas prácticas se emplea el control de acceso basado en roles (RBAC), donde todos los permisos se basan por su cargo o puesto funcional dentro de la organización. Este modelo ayuda a tener un mejor control de los accesos y tener un perfilamiento.

2.2.1.1. Importancia de la gestión de identidades en ciberseguridad

La gestión de identidades se consolidó como un componente esencial para la seguridad de la información y la ciberseguridad**,** impacta de forma directa en la reducción de riesgos como accesos no permitidos, movimientos inusuales dentro de la red corporativa, uso indebido de las cuentas huérfanas y aprovechamiento de credenciales comprometidas. Un sistema IAM bien diseñado permite:

- Limitar privilegios excesivos y aplicar el principio de mínimo privilegio**.**
- Reducir la superficie de ataque de la organización.
- Estandarizar y automatizar criterios de acceso.
- Proveer evidencia de cumplimiento frente a normativas y auditorías.

Los sistemas IAM modernos incorporan conceptos como identidad federada**,** Single Sign-On (SSO) **y** autenticación multifactor (MFA)**,** integrándose con múltiples aplicaciones corporativas para mejorar tanto la seguridad como la experiencia del usuario.

2.2.1.2. Seguridad y autenticación

Microsoft (2024) indica que la seguridad y autenticación en sistemas informáticos se refieren al conjunto de mecanismos diseñados para proteger datos, sistemas e identidades frente a accesos no autorizados y para verificar que los usuarios o servicios que intentan acceder sean realmente quienes dicen ser.

La seguridad de la información tiene tres pilares:

- Confidencialidad: Solo es accesible la información para quienes estén autorizados.
- Integridad: los datos no se alteran de forma no autorizada.
- Disponibilidad**:** los sistemas y servicios están accesibles cuando se requieren.

El proceso de autenticación verifica si usuario puede acceder. Esto puede realizarse mediante contraseñas, certificados digitales, tokens, credenciales biométricas o esquemas de autenticación multifactor (MFA)**,** combinando algo que el usuario sabe, algo que tiene y algo que es (Microsoft, 2024).

Desde una perspectiva de ciberseguridad, se suman controles como:

- Uso de protocolos seguros (SSL/TLS) para proteger la transmisión de credenciales.
- Gestión segura de contraseñas.
- Políticas de bloqueo de cuenta y caducidad de credenciales.
- Monitorización de intentos fallidos y actividad sospechosa.

2.2.1.3. Gestión del ciclo de vida de las identidades

ManageEngine (2025), nos indica que la administración de identidades durante todas sus etapas abarca procesos, roles y políticas que permiten administrar de manera correcta la identidad, desde el alta de la identidad hasta su baja o desactivación definitiva. Este ciclo se alinea con el enfoque Alta, Baja y Movimiento (ABM)**:**

- Alta: creación de la identidad y aprovisionamiento inicial de cuentas cuando una persona ingresa a la organización
- Modificaciones: ajuste de accesos cuando el usuario cambia de rol, unidad, proyecto o nivel de responsabilidad.
- Baja: desactivación o eliminación de cuentas y revocación de accesos cuando finaliza la relación con la organización.

Además, resalta que la automatización de estos procesos es esencial para reducir errores humanos, mejorar la eficiencia operativa y asegurar que los accesos se mantengan alineados con la situación actual de cada usuario. Asimismo, JumpCloud (2023) nos indica que una mala práctica de la administración de identidades durante todas sus etapas representa una condición que compromete la seguridad de la información, ya que las cuentas inactivas y los permisos no revocados a tiempo pueden propiciar accesos indebidos y posibles fugas de datos.

2.2.1.4. Experiencia del usuario y confianza en el IAM

Si bien la gestión de identidades tiene un fuerte componente técnico, también impacta en la experiencia del usuario interno y en su nivel de confianza hacia los sistemas corporativos. IBM (2022) indica que la percepción del usuario sobre la seguridad, facilidad de uso y transparencia de los procesos influye en la adopción y uso adecuado de las soluciones tecnológicas.

En el contexto de una plataforma IAM, la experiencia del usuario se ve influenciada por factores como:

- Simplicidad para iniciar sesión y acceder a los sistemas necesarios.
- Claridad y rapidez en los procesos para solicitar nuevos accesos.
- Disponibilidad de mecanismos de autoservicio para recuperación o cambio de contraseña.
- Visibilidad sobre los accesos vigentes y el estado de sus solicitudes.

2.2.2. Accesibilidad

Para la presente investigación, la accesibilidad se entiende desde una perspectiva tecnológica y organizacional, enfocada en ciberseguridad, es decir, como la capacidad del sistema y de los procesos que se tienen definidos nos va a permitir que los usuarios que estén autorizados ingresen de manera segura, oportuna y eficiente a los activos tecnológicos mínimos requeridos para su correcto cumplimiento de lo que indica su puesto funcional, sin introducir barreras innecesarias ni fricciones operativas que afecten la continuidad del negocio.

Desde el enfoque de seguridad de la información, la accesibilidad no implica la reducción de controles, sino el equilibrio entre protección y operatividad, de modo que los mecanismos de seguridad no incentiven prácticas inseguras, como el uso compartido de credenciales, el almacenamiento indebido de contraseñas o la evasión de controles formales. Un sistema accesible, desde esta perspectiva, facilita el acceso correcto al mismo tiempo que preserva los pilares esenciales de la seguridad de la información.

SMOWL (2023) señala que, en entornos digitales, la accesibilidad implica que los sistemas sean utilizables, estables y confiables para sus usuarios, garantizando de manera simultánea la protección de la información. Dentro las plataformas IAM, la accesibilidad se traduce en los siguientes aspectos:

- Disponibilidad continua de los servicios de autenticación y autorización.
- Interfaces claras y consistentes para la solicitud, aprobación y revisión de

accesos.

- Procesos ágiles que reduzcan los tiempos de espera para la asignación o modificación de permisos.
- Coherencia entre la estructura organizacional del banco y la forma en que se definen roles, perfiles y accesos.

Desde una perspectiva de ciberseguridad, una accesibilidad bien gestionada contribuye a reducir riesgos operativos y de seguridad, debido a que nos permite asignar los accesos de manera segura, verificable, auditable y conforme con a su puesto funcional del usuario.

2.2.2.1. Accesibilidad tecnológica

La accesibilidad tecnológica comprende la capacidad de los entornos de las plataformas e infraestructuras tecnológicas de la organización para proporcionar un acceso estable, seguro y eficiente a los recursos de TI. En el ámbito de la ciberseguridad, este concepto se relaciona directamente con la resiliencia de los servicios de autenticación y control de accesos frente a fallas técnicas, incidentes de seguridad o picos de demanda.

Desde esta perspectiva, la accesibilidad tecnológica implica asegurar que:

- Los servicios de autenticación y autorización mantengan niveles adecuados de disponibilidad y desempeño.
- Las integraciones entre el sistema IAM y las aplicaciones corporativas funcionen de manera confiable y segura.
- Los portales de acceso y consolas de administración presenten interfaces claras y consistentes para tareas como iniciar sesión, solicitar accesos o revisar permisos asignados.
- Las políticas de seguridad como autenticación multifactor, caducidad de contraseñas o bloqueo de cuentas se implementen de forma que fortalezcan la protección sin generar fricción excesiva para el usuario legítimo.

Una adecuada accesibilidad tecnológica permite que los controles de seguridad se apliquen de manera uniforme y centralizada, reduciendo la dependencia de soluciones manuales o excepciones que incrementan el riesgo de incidentes de seguridad.

2.2.2.2. Accesibilidad organizacional

La accesibilidad organizacional se centra en cómo los procesos internos, las normas o políticas de seguridad y estructura de la organización influyen en la capacidad de los usuarios para obtener y asegurar que los usuarios cuenten con los accesos correspondientes a sus funciones, sin comprometer la seguridad de la información.

Desde el enfoque de la gestión de identidades, la accesibilidad organizacional incluye aspectos como:

- Claridad en la definición de roles de negocio y los permisos asociados a cada rol.
- Existencia de flujos de solicitud y aprobación de accesos alineados con la jerarquía, responsabilidades y segregación de funciones del banco.
- Tiempos de respuesta razonables para la aprobación, modificación o revocación de accesos.
- Políticas claramente definidas sobre quién puede aprobar determinados accesos y bajo qué criterios.
- Ejecución de campañas periódicas de certificación de accesos para validar que los permisos otorgados sigan siendo necesarios.

Desde el enfoque de ciberseguridad, una accesibilidad organizacional adecuada contribuye a prevenir accesos excesivos, privilegios innecesarios y cuentas obsoletas, fortaleciendo el control interno y el cumplimiento normativo.

2.2.3. Control de acceso

Dentro de un sistema de gestión de identidades, permite regular la asignación de permisos sobre los recursos tecnológicos de la organización. Para ello, considera criterios como el usuario autorizado, las condiciones de acceso y el nivel de privilegio que se asigna. IDPro (2022) establece que, en el contexto de IAM, se basa en:

- Verificar la identidad del usuario (autenticación**).**
- Evaluar si el usuario tiene los permisos adecuados para la acción que intenta realizar **(**autorización**).**
- Aplicar políticas de acceso basadas en roles, atributos, contexto o combinaciones de estos.

Estos atributos se almacenan y administran en repositorios centrales (directorios o bases de datos), que son utilizados por las soluciones IAM para tomar decisiones de acceso (IBM, 2021).

2.3. Bases filosóficas

La gestión de identidades y la accesibilidad organizacional, en el contexto de la ingeniería informática, tienen bases filosóficas que se relacionan con cuestiones ontológicas, epistemológicas y axiológicas. A continuación, se exploran estas bases:

2.3.1. Gestión de Identidades

- **Ontología de la Identidad Digital**: La gestión de identidades implica una comprensión profunda de qué constituye una identidad. Desde un enfoque ontológico, se cuestiona el concepto de la identidad en el espacio digital y cómo se relaciona con la identidad física (Marcos, 2024).

- **Epistemología de la Autenticación**: La autenticación, un componente clave de la gestión de identidades, plantea preguntas sobre cómo conocemos y verificamos la identidad de los usuarios. Esto implica reflexionar sobre la fiabilidad de los métodos de autenticación y su impacto en la seguridad (UNIR, 2022).

- **Axiología de la Privacidad**: La gestión de identidades también involucra consideraciones éticas sobre la privacidad y el uso responsable de la información personal. Se debe equilibrar la necesidad de seguridad con el derecho a la privacidad (UNIR, 2022).

2.3.2 Accesibilidad Organizacional

- **Ontología de la Inclusión**: La accesibilidad organizacional se basa en la idea de que todos deben tener acceso a los mismos recursos, sin importar sus características individuales. Esta pregunta explora si los sistemas de la organización están diseñados con una visión inclusiva, asegurando que todas las personas, independientemente de su rol o capacidades, puedan utilizarlos eficientemente (Fundación Contrato, 2024).

- **Epistemología del Diseño Inclusivo**: El diseño se basa en comprender las diversas necesidades de los usuarios. La encuesta busca obtener información sobre si los empleados creen que el sistema fue diseñado con un enfoque que considere la diversidad de los usuarios y sus capacidades, evaluando si el sistema responde adecuadamente a las necesidades de todos (Redalyc, 2023).

- **Axiología de la Equidad**: La accesibilidad organizacional promueve de garantizar que todos los empleados tengan acceso igualitario a los sistemas y recursos organizacionales. Esto se basa en una axiología que valora la justicia y la igualdad en el acceso a los recursos digitales y físicos (Safe City, 2024).

2.4. Definición de términos básicos

- **Identidad**

  Target (2024) indica que una identidad digital representa el conjunto de atributos únicos que identifican a un usuario dentro de un sistema empresarial.

- **Gestión de identidades (Identity Management)**

  IBM (2023) define la gestión de identidades como el proceso orientado a administrar y controlar las identidades dentro de una organización, asegurando que los usuarios cuenten con los accesos correspondientes según sus funciones, roles y permisos asignados.

- **Gestión de accesos (Access Management)**

  Target (2024) sostiene que la gestión de accesos se enfoca en controlar los permisos y niveles de acceso que tienen los usuarios en los sistemas, asegurando que cada identidad acceda solo a los recursos autorizados, bajo políticas corporativas y reglas de seguridad.

- **IAM (Identity and Access Management)**

  Red Hat (2023) describe IAM como el marco organizacional y tecnológico encargado de gestionar identidades digitales y controlar los accesos.

- **Ciclo de vida de identidades (Identity Lifecycle Management – ILM)**

  ManageEngine (2025) sostuvo que el ciclo de vida de identidades (ILM) permite administrar cuentas y permisos desde el alta del usuario hasta su baja, considerando modificaciones durante su permanencia en la organización bajo el modelo Joiner–Mover–Leaver.

- **Control de acceso basado en roles (RBAC)**

  NIST (2022) explica que el modelo RBAC asigna permisos a roles y no directamente a los usuarios, permitiendo administrar privilegios de acuerdo con funciones, responsabilidades y estructura organizacional, reduciendo riesgos y simplificando la administración.

- **Segregación de funciones (SoD – Segregation of Duties)**

  Ferroni (2016) afirma que la segregación de funciones es un principio de seguridad que busca evitar que un usuario concentre permisos conflictivos que puedan generar fraudes, manipulaciones de datos o riesgos operativos, fortaleciendo el control interno.

- **Autenticación multifactor (MFA)**

  Microsoft (2024) indica que la autenticación multifactor es un método que utiliza dos o más factores (contraseña, token, biometría) para comprobar la identidad del usuario antes de permitir el acceso, fortaleciendo la protección contra accesos no autorizados.

- **Single Sign-On (SSO)**

  Okta (2024) define SSO como un mecanismo que facilita el acceso a diversas aplicaciones mediante una sola autenticación, logrando eficiencia operativa, mejora de experiencia y reducción de riesgos relacionados a contraseñas múltiples.

- **Principio de mínimo privilegio**

  Ferroni (2016) indica que este principio se basa en asignar únicamente los privilegios requeridos para que cada usuario cumpla sus responsabilidades,

reduciendo así el riesgo de accesos no autorizados y cumpliendo las normativas y estándares de seguridad.

- **IBM Verify Identity Governance (IVIG)**

  IBM (2023) describe IBM Verify Identity Governance como una plataforma de gobernanza de identidades diseñada para gestionar accesos, roles, certificaciones, cumplimiento normativo, flujos de aprobación y automatización del ciclo de vida de identidades.

- **Certificación de accesos**

  ISACA (2023) define la certificación de accesos como una revisión periódica de permisos para validar o retirar accesos según corresponda, asegurando que se mantengan adecuados, vigentes y conforme a políticas y auditorías.

- **Aprovisionamiento automático**

  SailPoint (2024) define el aprovisionamiento automático como el proceso mediante el cual se asignan, modifican o revocan credenciales y permisos en aplicaciones corporativas, de forma automatizada y basada en roles, eventos organizacionales o políticas definidas.

- **Cumplimiento normativo (Compliance)**

  ISACA (2023) sostiene que el cumplimiento normativo implica el alineamiento de los procedimientos de administración de identidades y accesos con estándares y regulaciones como ISO 27001, Basilea, CMF, GDPR y otras normativas aplicables al entorno financiero.

- **Sistemas Legados**

IBM (2023) define los sistemas legados como plataformas, aplicaciones o infraestructuras tecnológicas antiguas que siguen siendo operativas dentro de una organización, aunque fueron desarrolladas con tecnologías obsoletas o poco compatibles con soluciones modernas.

2.5 Hipótesis de investigación

2.5.1 Hipótesis General

El diseño de un sistema de gestión de identidades se relaciona con la accesibilidad en el Banco ITAÚ de Chile.

2.5.2 Hipótesis Específicas

El diseño del sistema de gestión de identidades se relaciona con la accesibilidad tecnológica en el Banco ITAÚ de Chile.

El diseño del sistema de gestión de identidades se relaciona con la accesibilidad organizacional en el Banco ITAÚ de Chile.

El diseño del sistema de gestión de identidades se relaciona con el control de acceso en el Banco ITAÚ de Chile.

2.6. Operacionalización de variables

Tabla 1.

Matriz de operacionalización de variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO	PREGUNTAS
Sistema de gestión de identidades	(Mathias & Rosencrance, 2021). El sistema de gestión de identidades se define como el conjunto de procesos y herramientas que permiten administrar identidades digitales y controlar el acceso a los recursos tecnológicos de una organización, garantizando seguridad, trazabilidad y alineación con las funciones del usuario.	Se mide mediante un cuestionario con escala Likert que evalúa la seguridad y autenticación, la gestión del ciclo de vida de identidades y la experiencia del usuario, a partir del uso de MFA, la administración de cuentas y la confiabilidad del acceso.	Seguridad y Autenticación	Nivel de autenticación multifactor (MFA) Prevención de accesos no autorizados Cumplimiento de estándares (ISO27001, NIST, Gobierno corporativo)	Cuestionario (Escala Likert)	1-3
			Gestión del Ciclo de Vida de Identidades	Eficiencia en creación, modificación y eliminación de cuentas Desactivación automática de cuentas inactivas Actualización periódica de roles y permisos		4-6
			Experiencia del Usuario y Confianza en el IAM	Integración con sistemas internos (SAP, Active Directory, VPN, Core Bancario) Rapidez y confiabilidad en acceso Confianza tecnológica del usuario		7-9
Accesibilidad	(SMOWL, 2023). La accesibilidad se define como la capacidad de los sistemas y procesos organizacionales para permitir que los usuarios autorizados accedan de forma segura y oportuna a los recursos tecnológicos necesarios para el desempeño de sus funciones, manteniendo un equilibrio entre facilidad de uso y controles de seguridad.	Se mide mediante un cuestionario con escala Likert que evalúa la accesibilidad tecnológica, la accesibilidad organizacional y el control de acceso, considerando la disponibilidad de los sistemas, la facilidad de uso, los procesos internos y la correcta asignación de privilegios.	Accesibilidad Tecnológica	Acceso desde diferentes plataformas y dispositivos Tiempo de disponibilidad y respuesta Usabilidad de herramientas tecnológicas (portal, autoservicio, autenticador)		10-12
			Accesibilidad Organizacional	Adaptación a roles y jerarquías del banco Disponibilidad de documentación accesible Necesidad de capacitación para usuarios		13-15
			Control de acceso	Efectividad de la autenticación Aplicación del principio de privilegios mínimos Auditoría y monitoreo de accesos		16-18

Nota: Elaboración propia

III. METODOLOGIA

3.1. Diseño metodológico

3.1.1. Tipo de Investigación

La investigación fue de tipo aplicada, ya que se orientó a resolver una problemática específica en un contexto real mediante el uso de conocimientos científicos.

Según Hernández Sampieri et al. (2022), este tipo de estudio busca atender problemas prácticos, a diferencia de la investigación básica, cuyo propósito principal es ampliar el conocimiento teórico.

3.1.2. Nivel de Investigación

La investigación fue de nivel correlacional, porque permitió determinar el grado de asociación entre las variables estudiadas, sin manipularlas ni establecer una relación causal (Hernández Sampieri et al., 2022).

3.1.3. Diseño

La investigación presentó un diseño no experimental, debido a que las variables fueron observadas en su contexto natural, sin manipulación por parte del investigador.

Según Hernández Sampieri et al. (2022), este diseño permite analizar fenómenos, relaciones o tendencias tal como se presentan en la realidad.

3.1.4. Enfoque

El estudio presentó un enfoque cuantitativo, porque analizó datos numéricos para medir la relación entre las variables mediante métodos estadísticos (Hernández Sampieri et al., 2022).

3.2. Población y muestra

3.2.1 Población

La población estuvo conformada por 14 colaboradores del área de Seguridad de la Información: 11 operadores, dos coordinadores y un jefe de área.

3.2.2 Muestra

El estudio fue censal, por lo tanto, no aplica la muestra.

3.3. Técnicas e instrumentos de recolección de datos:

3.3.1 Técnicas para emplear

Se utilizó la encuesta como técnica y el cuestionario como instrumento, detallado en el Anexo 2.

3.3.2 Descripción de los instrumentos

El instrumento utilizó una escala de medición tipo Likert que permitirá recabar la opinión de los operadores del área de Seguridad de la Información respecto al proceso actual de gestión de identidades y accesos, así como sobre el sistema automatizado propuesto para mejorar dicho proceso.

Fue sometido a validación por juicio de expertos y a una prueba de confiabilidad mediante la herramienta estadística Alfa de Cronbach.

3.4. Técnicas para el procesamiento de datos

El análisis de los datos obtenidos de la encuesta se indica como el conjunto de actividades sistemáticas que permiten organizar, transformar, analizar e interpretar la información recolectada a través de un cuestionario, con el objetivo de convertir esos datos en resultados útiles y significativos para la investigación (Hernández Sampieri et al., 2022).

Este proceso incluye etapas como la codificación, digitalización, limpieza, análisis estadístico y presentación de resultados. Asegura que los datos recopilados se convertirán en información válida, confiable y comprensible, lista para responder los objetivos e hipótesis del estudio.

En el estudio a realizar primero se elaborará la base de datos en el programa SPSS, considerando para ello lo recopilado en la encuesta a través del cuestionario de preguntas; luego se utilizará las herramientas descriptivas para describir las variables de estudio y las herramientas inferenciales para realizar la prueba de hipótesis.

3.5. Matriz de consistencia (Anexo 01)

IV. RESULTADOS

4.1. Análisis de resultados

4.1.1. Prueba de validez y confiabilidad del instrumento

4.1.1.1. Prueba de validez

La prueba se realizó con la evaluación del instrumento por 5 jueces expertos cuyas fichas de evaluación se muestran en el anexo 3, cuyo resultado se presenta a continuación:

$$\boldsymbol{Validez} = \frac{\boldsymbol{Total\ opinión}}{\boldsymbol{Total\ máximo}} = \frac{\mathbf{210}}{\mathbf{10x5x5}} = \frac{\mathbf{210}}{\mathbf{250}} = \mathbf{0,84} = \mathbf{84\%}$$

Valor aceptable para su aplicación Ver anexo 3

4.1.1.2. Prueba de confiabilidad

En la investigación se empleó el estadístico Alfa de Cronbach haciendo uso del software SPSS se obtuvo como resultado:

Tabla 2. *Alfa de Cronbach*

Alfa de Cronbach	N de elementos
,872	18

Lo que muestra un indicador confiable, ver anexo 4.

4.1.2. Descripción de las variables

4.1.2.1. Variable gestión de identidades

Tabla 3. *Gestión de identidades.*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	3	21,4	21,4
	De acuerdo	3	21,4	42,8
	Totalmente de acuerdo	8	57,1	99,9
	Total	14	100,0	

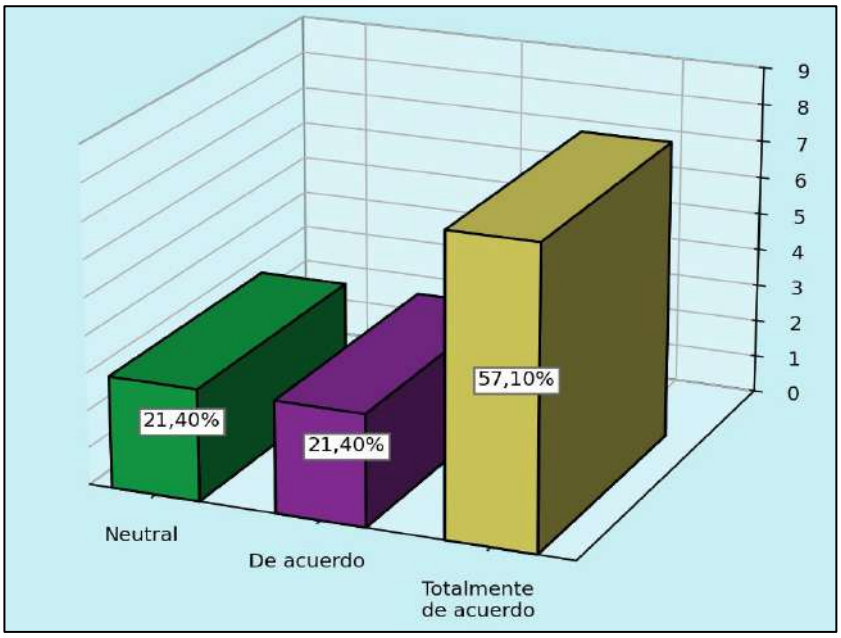


Figura 1. Gestión de identidades

Según la Tabla 3 y la Figura 1, el 21,4% de los colaboradores se ubica en la categoría neutral, el 21,4% en de acuerdo y el 57,1% en totalmente de acuerdo respecto a la variable gestión de identidades. En ese sentido, predominan las respuestas favorables, lo que permite señalar que existe una percepción positiva sobre el diseño propuesto en esta variable.

4.1.2.1.1. Dimensión Seguridad y Autenticación

Tabla 4. ***Seguridad y Autenticidad.***

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	4	28,6	28,6
	De acuerdo	6	42,9	71,5
	Totalmente de acuerdo	4	28,6	100,1
	Total	14	100,0	

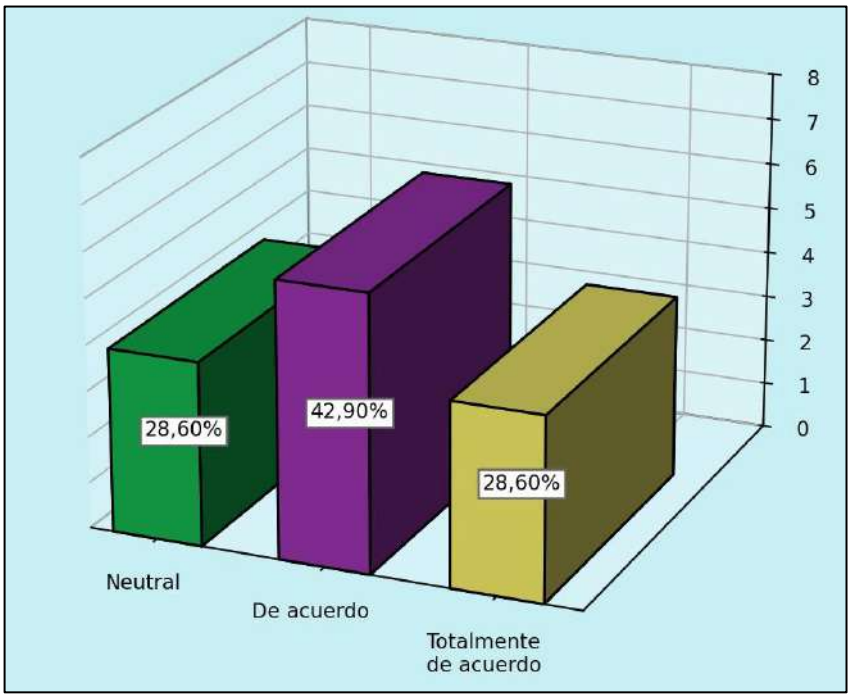


Figura 2. Seguridad y Autenticidad.

Según la Tabla 4 y la Figura 2, el 28,6% de los colaboradores se ubica en la categoría neutral, el 42,9% en de acuerdo y el 28,6% en totalmente de acuerdo respecto a la dimensión seguridad y autenticación. Por ello, se observa que la mayoría de las respuestas se concentra en niveles favorables, lo que refleja una valoración positiva de esta dimensión.

4.1.2.1.2. Gestión del ciclo de vida de identidades

Tabla 5. *Gestión del ciclo de vida de identidades.*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	3	21,4	21,4
	De acuerdo	2	14,3	35,7
	Totalmente de acuerdo	9	64,3	100,0
	Total	14	100,0	

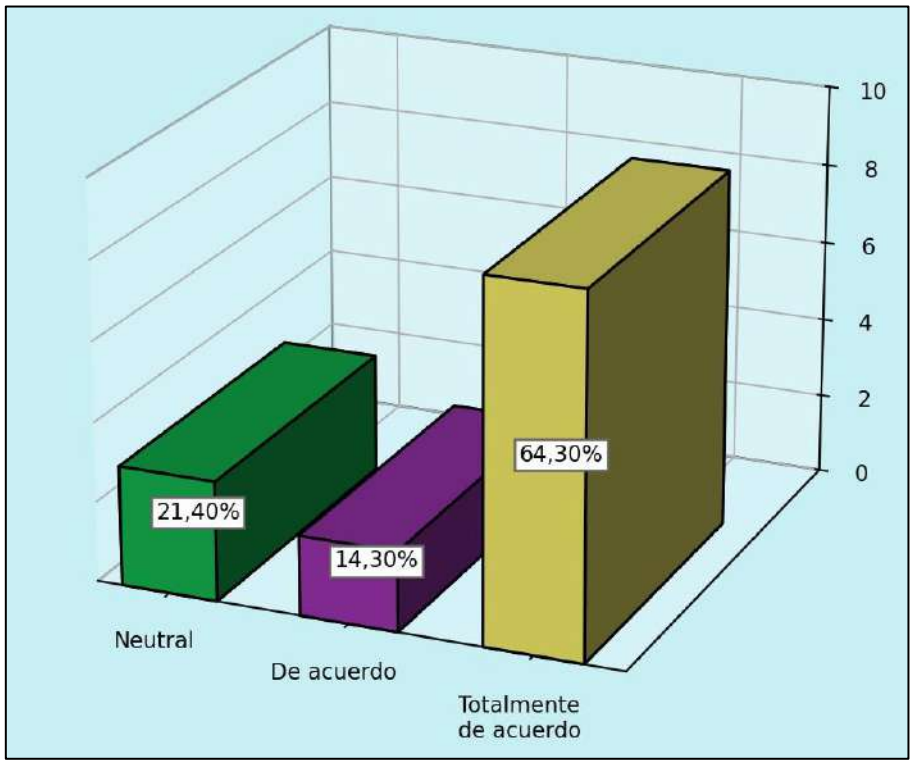


Figura 3. Gestión del ciclo de vida de identidades

Según la Tabla 5 y la Figura 3, el 21,4% de los colaboradores se ubica en la categoría neutral, el 14,3% en de acuerdo y el 64,3% en totalmente de acuerdo respecto a la dimensión gestión del ciclo de vida de identidades. En consecuencia, predomina la categoría totalmente de acuerdo, lo que indica una valoración favorable de esta dimensión del sistema propuesto

4.1.2.1.3. Dimensión Usuario y confianza en el IAM

Tabla 6. Experiencia del Usuario y confianza en el IAM

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	2	14,3	14,3
	De acuerdo	4	28,6	42,9
	Totalmente de acuerdo	8	57,1	100,0
	Total	14	100,0	

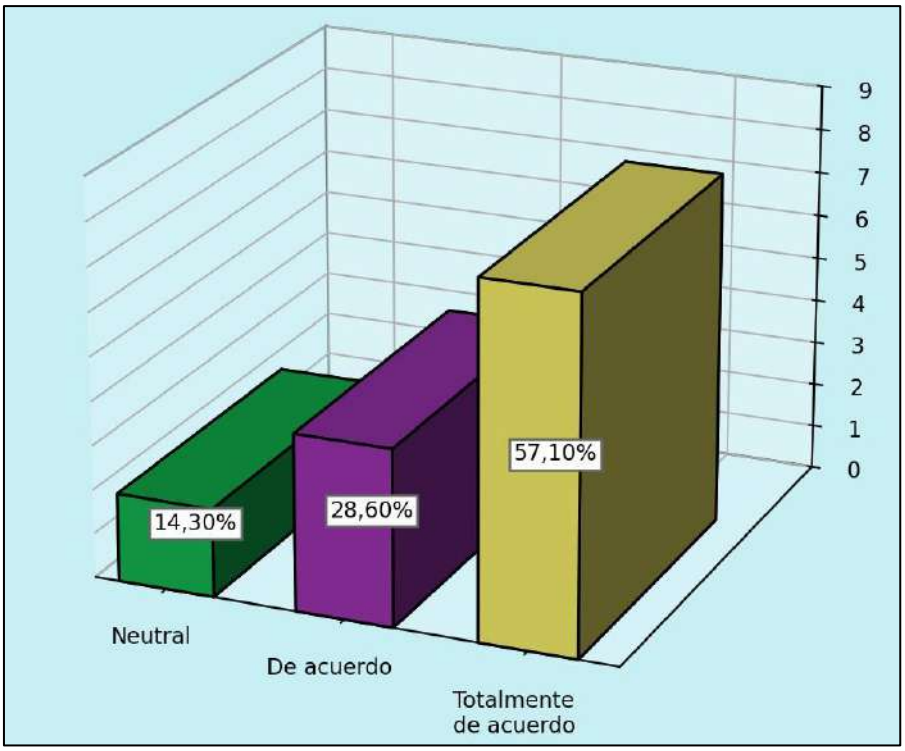


*Figura 4***.** Experiencia del Usuario y confianza en el IAM.

Según la Tabla 6 y la Figura 4, el 14,3% de los colaboradores se ubica en la categoría neutral, el 28,6% en de acuerdo y el 57,1% en totalmente de acuerdo respecto a la dimensión experiencia del usuario y confianza en el IAM. Por lo tanto, se observa una mayor concentración de respuestas favorables, lo que muestra una valoración positiva de esta dimensión.

4.1.2.2. Variable accesibilidad

Tabla 7. Accesibilidad

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	1	7,1	7,1
	De acuerdo	7	50,0	57,1
	Totalmente de acuerdo	6	42,9	100,0
	Total	14	100,0	

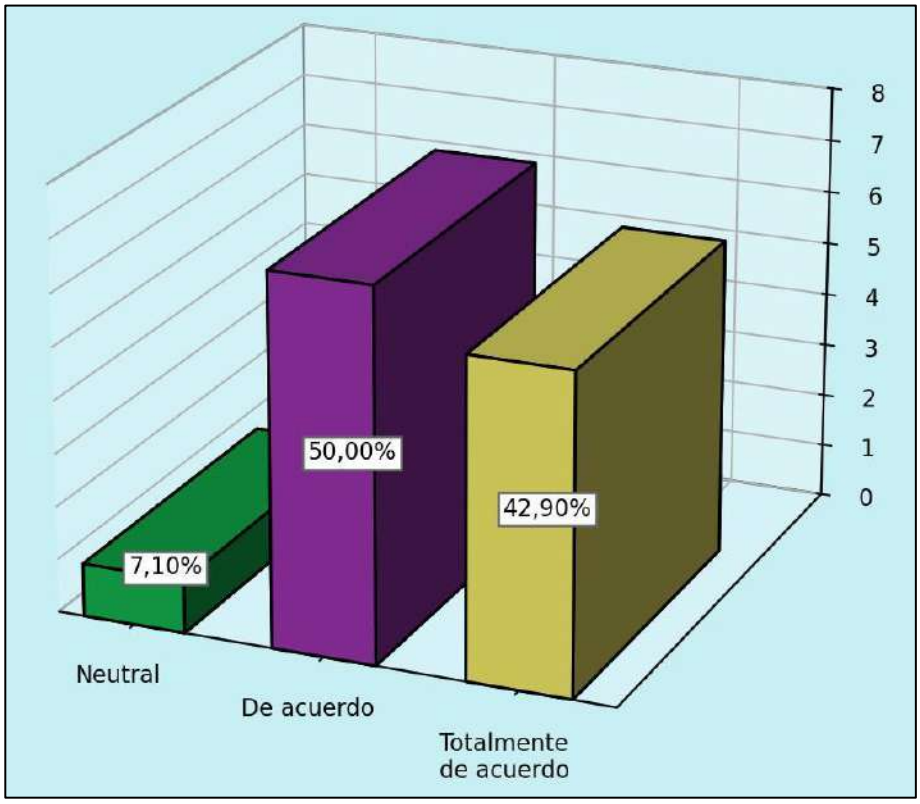


Figura 5. Accesibilidad.

Según la Tabla 7 y la Figura 5, el 7,1% de los colaboradores se ubica en la categoría neutral, el 50,0% en de acuerdo y el 42,9% en totalmente de acuerdo respecto a la variable accesibilidad. En ese sentido, predominan las respuestas favorables, lo que permite señalar una percepción positiva sobre esta variable.

4.1.2.2.1. Dimensión accesibilidad tecnológica

Tabla 8. *Accesibilidad tecnológica.*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	2	14,3	14,3
	De acuerdo	4	28,6	42,9
	Totalmente de acuerdo	8	57,1	100,0
	Total	14	100,0	

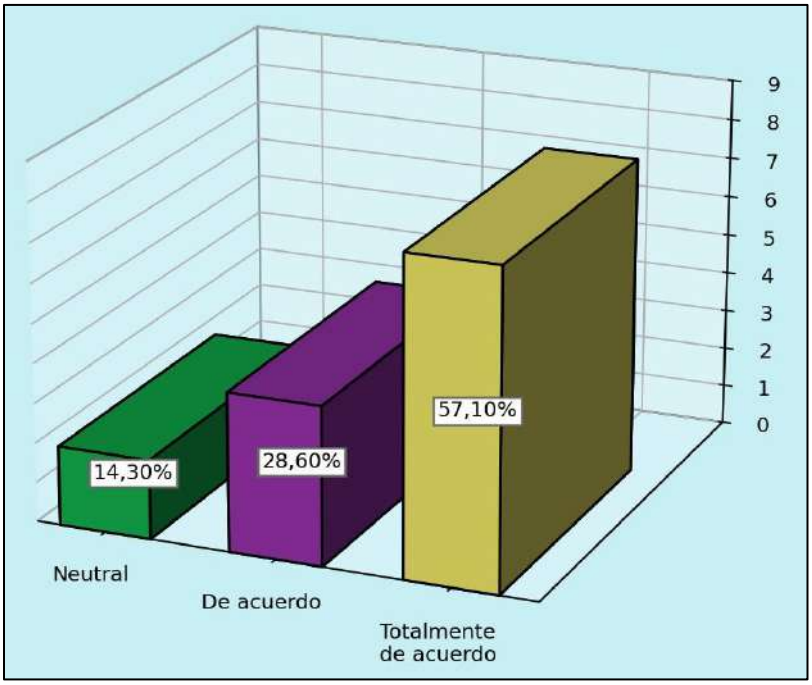


*Figura 6***.** Accesibilidad Tecnológica.

Según la Tabla 8 y la Figura 6, el 14,3% de los colaboradores se ubica en la categoría neutral, el 28,6% en de acuerdo y el 57,1% en totalmente de acuerdo respecto a la dimensión accesibilidad tecnológica. En consecuencia, la mayor parte de las respuestas se ubica en niveles favorables, lo que refleja una valoración positiva de esta dimensión.

4.1.2.2.2. Dimensión accesibilidad organizacional

Tabla 9. *Accesibilidad Organizacional.*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	3	21,4	21,4
	De acuerdo	4	28,6	50,0
	Totalmente de acuerdo	7	50,0	100,0
	Total	14	100,0	

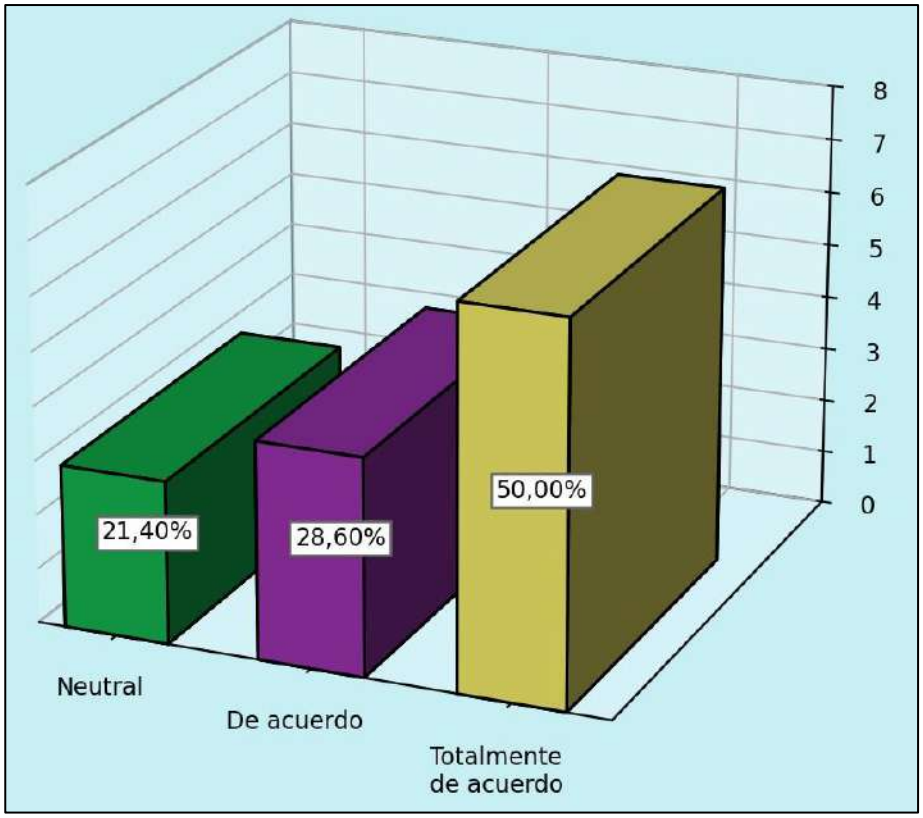


*Figura 7***.** Accesibilidad Organizacional.

Según la Tabla 9 y la Figura 7, el 21,4% de los colaboradores se ubica en la categoría neutral, el 28,6% en de acuerdo y el 50,0% en totalmente de acuerdo respecto a la dimensión accesibilidad organizacional. Por ello, predominan las respuestas favorables, lo que muestra una percepción positiva de esta dimensión.

4.1.2.2.3. Dimensión control de acceso

Tabla 10. *Control de acceso.*

		Frecuencia	Porcentaje	Porcentaje acumulado
Válidos	Neutral	2	14,3	14,3
	De acuerdo	5	35,7	50,0
	Totalmente de acuerdo	7	50,0	100,0
	Total	14	100,0	

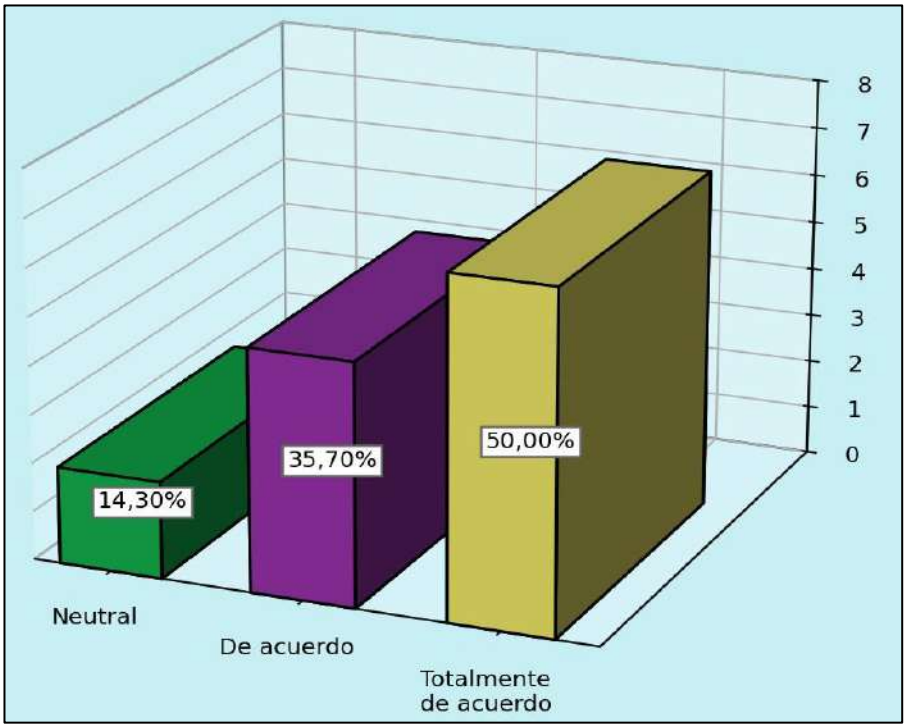


Figura 8. Control de acceso.

Según la Tabla 10 y la Figura 8, el 14,3 % de los colaboradores se ubica en la categoría neutral, el 35,7% en de acuerdo y el 50,0% en totalmente de acuerdo respecto a la dimensión control de acceso. En consecuencia, las respuestas se concentran principalmente en niveles favorables, lo que indica una valoración positiva de esta dimensión.

4.2. Contrastación de hipótesis

4.2.1. Contrastación de la hipótesis general

Ho: El diseño de un sistema de gestión de identidades no se relaciona con la accesibilidad en el Banco ITAÚ de Chile.

Ha: El diseño de un sistema de gestión de identidades se relaciona con la accesibilidad en el Banco ITAÚ de Chile.

Tabla 11. *Contrastación de la hipótesis general.*

			Gestión de identidades	Accesibilidad
Rho de Spearman	Gestión de identidades	Coeficiente de correlación	1,000	,984
		Sig. (bilateral)	.	,000
		N	14	14
	Accesibilidad	Coeficiente de correlación	,984	1,000
		Sig. (bilateral)	,000	.
		N	14	14

En la Tabla 11, se observa que el sig bilateral es de 0,000; lo cual se demuestra que la hipótesis alterna se acepta esto significa que el diseño de un sistema de gestión de identidades se relaciona con la accesibilidad en el Banco ITAÚ de Chile y el grado de relación es de 0,984 y tiene una dirección positiva.

4.2.1.1. Contrastación de la hipótesis específica 1

Ho: El diseño del sistema de gestión de identidades no se relaciona con la accesibilidad tecnológica en el Banco ITAÚ de Chile.

Ha: El diseño del sistema de gestión de identidades se relaciona con la accesibilidad tecnológica en el Banco ITAÚ de Chile.

Tabla 12. *Contrastación de la hipótesis específica 1.*

			Gestión de identidades	Accesibilidad Tecnológica
Rho de Spearman	Gestión de identidades	Coeficiente de correlación	1,000	,936
		Sig. (bilateral)	.	,000
		N	14	14
	Accesibilidad Tecnológica	Coeficiente de correlación	,936	1,000
		Sig. (bilateral)	,000	.
		N	14	14

En la Tabla 12, se observa que el sig bilateral es de 0,000; lo cual se demuestra que la hipótesis alterna se acepta esto significa que el diseño de un sistema de gestión de identidades se relaciona con la accesibilidad tecnológica en el Banco ITAÚ de Chile y el grado de relación es de 0,936 y tiene una dirección positiva.

4.2.1.2. Contrastación de la hipótesis específica 2

Ho: El diseño del sistema de gestión de identidades no se relaciona con la accesibilidad organizacional en el Banco ITAÚ de Chile.

Ha: El diseño del sistema de gestión de identidades se relaciona con la accesibilidad organizacional en el Banco ITAÚ de Chile.

Tabla 13. *Contrastación de la hipótesis específica 2.*

			Gestión de identidades	Accesibilidad Organizacional
Rho de Spearman	Gestión de identidades	Coeficiente de correlación	1,000	,974
		Sig. (bilateral)	.	,000
		N	14	14
	Accesibilidad Organizacional	Coeficiente de correlación	,974	1,000
		Sig. (bilateral)	,000	.
		N	14	14

En la Tabla 13, se observa que el sig bilateral es de 0,000; lo cual se demuestra que la hipótesis alterna se acepta esto significa que el diseño de un sistema de gestión de identidades se relaciona con la accesibilidad organizacional en el Banco ITAÚ de Chile y el grado de relación es de 0,974 y tiene una dirección positiva.

4.2.1.3. Contrastación de la hipótesis específica 3

Ho: El diseño del sistema de gestión de identidades no se relaciona con el control de acceso en el Banco ITAÚ de Chile.

Ha: El diseño del sistema de gestión de identidades se relaciona con el control de acceso en el Banco ITAÚ de Chile

Tabla 14. *Contrastación de la hipótesis específica 3.*

			Gestión de identidades	Control de acceso
Rho de Spearman	Gestión de identidades	Coeficiente de correlación	1,000	,964
		Sig. (bilateral)	.	,000
		N	14	14
	Control de acceso	Coeficiente de correlación	,964	1,000
		Sig. (bilateral)	,000	.
		N	14	14

La Tabla 14, se observa que el sig bilateral es de 0,000; lo cual se demuestra que la hipótesis alterna se acepta esto significa que el diseño de un sistema de gestión de identidades se relaciona con el control de acceso en el Banco ITAÚ de Chile y el grado de relación es de 0,964 y tiene una dirección positiva.

V. DISCUSIÓN

5.1. Discusión de resultados

Los resultados obtenidos demuestran que el objetivo de la investigación se cumple; esta afirmación se sustenta en la prueba de hipótesis, la cual presenta un nivel de significancia $p < 0,001$, valor menor al nivel de significancia establecido de 0,05, lo que representa que existe relación entre la variable gestión de identidades y la variable accesibilidad en el Banco ITAÚ de Chile. Asimismo, la intensidad de la relación es de 0,984, con dirección positiva.

Estos resultados se asemejan a lo obtenido por Díaz y Muñoz (2023), quienes demuestran la relación entre la variable control biométrico y la gestión de acceso, obteniendo un nivel de significancia bilateral de 0,001. Del mismo modo, Racacha (2024) establece que existe una relación significativa entre el sistema de gestión de datos biométricos y el control de asistencia, con un coeficiente de 0,826 según la prueba de correlación de Spearman. Además, Schlatt et al. (2022), en el artículo "Diseño de un marco para procesos digitales KYC basados en identidad autosoberana sobre blockchain", muestran que diseñar un marco para procesos digitales puede preservar la privacidad mediante el uso de credenciales verificables y mecanismos de protección de datos.

Además, Mathias y Rosencrance (2021) sostienen que la gestión de identidades o identificaciones está relacionada con el acceso adecuado a los recursos tecnológicos, lo que coincide con los resultados obtenidos en el presente estudio, donde también se demuestra la relación de la gestión de identidades con la accesibilidad

tecnológica, la accesibilidad organizacional y el control de acceso, con coeficientes de 0,936, 0,974 y 0,964, respectivamente, todos con dirección positiva y significancia menor a 0,05.

Se debe manifestar también que durante la realización del estudio hubo cierta reserva con la información, debido a la naturaleza de las políticas de seguridad del sector bancario, lo que se constituyó en una variable interviniente.

VI. CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Se determinó como el diseño de un sistema de gestión de identidades mantiene relación significativamente con la accesibilidad en el Banco ITAÚ de Chile, de acuerdo con la prueba Rho de Spearman, en la que se obtuvo un coeficiente de correlación de 0,984 y un nivel de significancia $p < 0,001$, valor menor a 0,05. Por lo tanto, se acepta la hipótesis general de investigación.

Asimismo, se determinó que el diseño del sistema de gestión de identidades se relaciona significativamente con la accesibilidad tecnológica en el Banco ITAÚ de Chile, según la prueba Rho de Spearman, en la que se obtuvo un coeficiente de correlación de 0,936 y un nivel de significancia $p < 0,001$, valor menor a 0,05.

En consecuencia, se acepta la primera hipótesis específica. Del mismo modo, se determinó que el diseño del sistema de gestión de identidades se relaciona significativamente con la accesibilidad organizacional en el Banco ITAÚ de Chile, de acuerdo con la prueba Rho de Spearman, en la que se obtuvo un coeficiente de correlación de 0,974 y un nivel de significancia $p < 0,001$, valor menor a 0,05. Por ello, se acepta la segunda hipótesis específica.

Finalmente, se determinó que el diseño del sistema de gestión de identidades se relaciona significativamente con el control de acceso en el Banco ITAÚ de Chile, según la prueba Rho de Spearman, en la que se obtuvo un coeficiente de correlación de 0,964 y un nivel de significancia $p < 0,001$, valor menor a 0,05. En tal sentido, se acepta la tercera hipótesis específica.

6.2. Recomendaciones

A partir de la relación identificada entre el diseño del sistema de gestión de identidades y la accesibilidad en el Banco ITAÚ de Chile, se recomienda que la organización fortalezca la administración de accesos mediante una solución centralizada que permita gestionar de forma ordenada a los usuarios, credenciales y perfiles, con la finalidad de mejorar tanto la seguridad como la facilidad de acceso a los recursos tecnológicos (Aplicaciones).

Asimismo, teniendo en cuenta la relación identificada con la accesibilidad tecnológica, se recomienda mantener actualizadas las herramientas y plataformas de acceso, procurando que estas sean compatibles con distintos dispositivos, sistemas y canales utilizados por los colaboradores. Del mismo modo, considerando la relación con la accesibilidad organizacional, se recomienda que el banco asegure una adecuada estructuración de roles, perfiles y privilegios de acceso, complementada con documentación precisa y actividades de capacitación para los usuarios. De igual forma, al haberse evidenciado relación con el control de acceso, se recomienda reforzar la asignación de permisos bajo el principio de privilegios mínimos y establecer mecanismos permanentes de auditoría y monitoreo que permitan detectar accesos inusuales o posibles irregularidades.

Finalmente, se recomienda incorporar mecanismos de autenticación robusta, como la autenticación multifactor, especialmente en los sistemas críticos del banco, así como promover una cultura de seguridad entre los usuarios mediante acciones de sensibilización y actualización continua que estén alineados a las buenas prácticas.

VII. REFERENCIAS

Fuentes bibliográficas

Contreras, J. A. R., & Vega, G. J. V. (2019). Implementación de un sistema de gestión de identidades privilegiadas para el control de acceso en una empresa de retail *[Tesis de ingeniero, Universidad San Martín de Porres].*

Hernández Sampieri, R., Fernández-Collado, C., & Baptista Lucio, P. (2022). *Metodología de la investigación* (7ª ed.). McGraw-Hill.

Mendoza Corrales, A. J., & Paucar Rimac, T. K. (2023). Diseño de un sistema de administración y gobierno de identidades en una entidad financiera en el Perú [Trabajo de suficiencia profesional,

Olivares Torrijos, C. E**.** (2019). *Elementos para una metodología de gestión de identidad digital en la empresa* (Tesis de maestría). INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación. repositorionacionalcti.mx

Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized digital identity and verifiable credentials. Manning Publications.

Fuentes electrónicas

Accenture. (2022). Banca basada en la identidad digital: Un nuevo modelo de confianza*.* *https://www.accenture.com/us-en/insights/banking/digital-identity-banking*

Ali, M., Pal, A., & Khan, S. U. (2020). Identity management in cloud computing: A taxonomy and survey. Journal of Network and Computer Applications, 159, 102595. https://doi.org/10.1016/j.jnca.2020.102595

Díaz Bustamante, W., & Muñoz Apagüeño, V. (2023). *Sistema de control biométrico para la gestión de accesos de empleados de un hospital Moyobamba, 2023* (Tesis de grado). Universidad César Vallejo. https://hdl.handle.net/20.500.12692/135297

ENISA. (2022). Directrices sobre procesos seguros de verificación de identidad. *Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/publications/identity-verification*

Gartner (2023). Cuadrante Mágico para la Gestión de Acceso. *https://www.gartner.com/en/documents/4002530*

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of Self-Sovereign identity. *Business & Information Systems Engineering, 66, 421–440. https://doi.org/10.1007/s12599-023-00830-x*

IBM. (2021). ¿Qué es la gestión de identidades y accesos (IAM)? Recuperado de https://www.ibm.com/es-es/topics/identity-access-management

IBM. (2022). *¿Qué es la experiencia del cliente (CX)?*. Recuperado el 24 de mayo de 2022, de https://www.ibm.com/es-es/topics/customer-experience.

IBM. (2025). Cost of a Data Breach Report 2025. IBM Security. https://www.ibm.com/reports/data-breach

IDPro Body of Knowledge. (2022). Arquitectura de Referencia IAM (v2). Recuperado de https://bok.idpro.org/article/76/galley/247/download/

ISACA. (2023). Information systems & cybersecurity certificates. Recuperado , de https://www.isaca.org/credentialing/certificates

Ferroni, S. (2016, 19 de mayo). *Implementing segregation of duties: A practical experience based on best practices*. *ISACA Journal*. Recuperado, de https://www.isaca.org/resources/isaca-journal/issues/2016/volume-3/implementing-segregation-of-duties-a-practical-experience-based-on-best-practices

Fundación Contrato. (2024). *Accesibilidad en la empresa: requerimientos legales y sugerencias*. Recuperado de https://fundacioncontrato.cl/blog/guias-para-la-empresa/accesibilidad-en-la-empresa/

JumpCloud. (2023). Gestión del ciclo de *vida de la identidad*. Recuperado el 5 de abril de 2025, de https://jumpcloud.com/es/platform/user-management

Maler, E., & Reed, D. (2008). The Venn of identity: Options and issues in federated identity management. IEEE Security & Privacy, 6(2), 16–23. https://doi.org/10.1109/MSP.2008.32

ManageEngine. (2025). *Gestión del ciclo de vida de la identidad digital*. Recuperado el 5 de abril de 2025, de https://www.manageengine.com/latam/identity-360/gestion-de-ciclo-de-vida-de-la-identidad-digital.html

Marcos, A. (2024). *Filosofía de la Informática: una agenda tentativa*. Recuperado de http://fcaenlinea1.unam.mx/anexos/1156/1156_u6_act4_p16.pdf

Mathias, C., & Rosencrance, L. (2021, 14 de septiembre). *Gestión de identidades o gestión de IDs*. *ComputerWeekly.com*. Recuperado, de https://www.computerweekly.com/es/definicion/Gestion-de-identidades-o-gestion-de-IDs.Universidad Peruana de Ciencias Aplicadas]. RENATI. https://renati.sunedu.gob.pe/handle/renati/412691

Microsoft. (2024) *¿Qué es la autenticación? Definición y métodos*. Recuperado de https://www.microsoft.com/es-es/security/business/security-101/what-is-authentication NIST (2022). National Institute of Standards and Technology. *Role Based Access Control (RBAC) project*. Recuperado, de https://csrc.nist.gov/projects/role-based-access-control

Okta. (2024, 27 de agosto). *¿Qué es el inicio de sesión único (SSO)?* Recuperado de https://www.okta.com/es-mx/blog/identity-security/single-sign-on-sso

Olabanji, S. O., Olaniyi, O. O., Adigwe, C. S., Okunleye, O. J., & Oladoyinbo, T. O. (2024). AI for Identity and Access Management (IAM) in Cloud. *SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4706726*

Racacha, A. D. L**.** (2024). *Diseño de un sistema de gestión de datos biométricos, y el control de asistencia de la I.E.P. Nuestra Señora del Carmen, Huacho – 2023*. Universidad Nacional José Faustino Sánchez Carrión. Repositorio Institucional UNJFSC – ALICIA: http://hdl.handle.net/20.500.14067/10056

Red Hat. (2023). *¿Qué es la gestión de las identidades y del acceso? RedHat.com*. Recuperado , de https://www.redhat.com/es/topics/security/what-identity-and-access-management-iam

Redalyc. (2023). *Integración de Técnicas de Usabilidad y Accesibilidad en el Proceso de Desarrollo de Software*. Recuperado de https://www.redalyc.org/journal/1331/133115019001.pdf.

Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening cybersecurity resilience: An investigation of customers' adoption of emerging security tools in mobile banking apps. Computers, 14(4), 129. https://doi.org/10.3390/computers14040129.

Rojas Alza, A. B., & Mendoza de los Santos, A. C. (2024). La Evolución de la Gestión

de la Identidad (IAM) en la Seguridad de la Información. Revista Científica: BIOTECH AND ENGINEERING, 4(1). https://doi.org/10.52248/eb.Vol4Iss1.131

Safe City. (2024). *Accesibilidad y empresa: construir un futuro sin barreras*. Recuperado de https://safecitying.com/accesibilidad-y-empresa-construir-un-futuro-sin-barreras/

SailPoint. (2024). *¿Qué es el aprovisionamiento automatizado?* Recuperado , de https://www.sailpoint.com/identity-library/what-is-automated-provisioning

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). *Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity.* Information & Management. https://doi.org/10.1016/j.im.2021.103553.

SMOWL. (2023). *Tecnologías accesibles por un mundo más sostenible*. Recuperado de https://smowl.net/es/blog/tecnologias-accesibles/

Sommerville, I. (2011). *Software Engineering* (9th ed.). Boston: Addison-Wesley

Target Tech. (2024). *What is Identity Governance and Administration (IGA)?*. Recuperado el 4 de abril de 2025, de https://www.techtarget.com/searchsecurity/definition/identity-governance-and-administration-IGA

UNIR. (2022). *¿Qué es el identity and access management o IAM?* Recuperado de https://www.unir.net/revista/ingenieria/identity-and-access-management/

UDIT. (2024). *Seguridad informática: qué es, tipos y características*. Recuperado de https://udit.es/actualidad/seguridad-informatica-que-es-tipos-y-caracteristicas/

World Economic Forum. (2021). *Annual Report 2021-2022*. Recuperado el 10 de febrero de 2025, de https://www.weforum.org/publications/annual-report-2021-2022/.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). https://ieeexplore.ieee.org/document/7163223

ANEXOS

Anexo 01. Matriz de consistencia

. **TITULO**:" Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile - 2024"

Problemas	Objetivos	Hipótesis	Variables	Indicadores	Métodos
Problema general ¿En qué medida se relaciona el diseño de un sistema de gestión de identidades con la accesibilidad en el Banco ITAÚ de Chile? **Problemas específicos** ¿En qué medida se relaciona el diseño del sistema de gestión de identidades con la accesibilidad tecnológica de los usuarios en el Banco ITAÚ de Chile? ¿En qué medida se relaciona el diseño del sistema de gestión de identidades con la accesibilidad organizacional en el Banco ITAÚ de Chile? ¿En qué medida se relaciona el diseño del sistema de gestión de identidades con el acceso del Banco ITAÚ de Chile?	**Objetivos generales** Determinar en qué medida se relaciona el diseño de un sistema de gestión de identidades con la accesibilidad en el Banco ITAÚ de Chile. **Objetivos específicos** Determinar el grado de relación entre el diseño del sistema de gestión de identidades y la accesibilidad tecnológica de los usuarios en el Banco ITAÚ de Chile. Determinar el grado de relación entre el diseño del sistema de gestión de identidades y la accesibilidad organizacional en el Banco ITAÚ de Chile. Determinar el grado de relación entre el diseño del sistema de gestión de identidades y el control de acceso en el Banco ITAÚ de Chile.	**Hipótesis general** El diseño de un sistema de gestión de identidades se relaciona con la accesibilidad en el Banco ITAÚ de Chile. **Hipótesis especificas** El diseño de un sistema de gestión de identidades se relaciona con la accesibilidad tecnológica en el Banco ITAÚ de Chile. El diseño de un sistema de gestión de identidades se relaciona con la accesibilidad organizacional en el Banco ITAÚ de Chile. El diseño de un sistema de gestión de identidades se relaciona con el control de acceso en el Banco ITAÚ de Chile.	**Variable 1** Gestión de identidades **Dimensiones** Seguridad y Autenticación Gestión del Ciclo de Vida de Identidades Experiencia del Usuario **Variable 2** Accesibilidad **Dimensiones** Accesibilidad Tecnológica Accesibilidad Organizacional Control de acceso	Nivel de autenticación MFA Prevención de accesos no autorizados Cumplimiento de estándares Efectividad de aprovisionamiento, bajas y modificaciones Desactivación automática de cuentas inactivas Actualización de roles y permisos Integración tecnológica con otros sistemas Rapidez y confiabilidad en acceso Confianza tecnológica del usuario Acceso desde diferentes plataformas y dispositivos Tiempo de disponibilidad y respuesta Usabilidad de herramientas tecnológicas Adaptación a roles y jerarquías Necesidad de capacitación Efectividad de autenticación Aplicación del principio de privilegios mínimos Auditoría y monitoreo de accesos	**Tipo de Investigación**: Aplicada **Nivel de la investigación**: Correlacional **Enfoque:** Cuantitativo **Diseño**: No experimental **Población** 14 personas **Muestra** =censal Técnicas para la recolección de datos: Encuesta Instrumentos de recolección de datos: Cuestionario Técnicas para el procesamiento de la información: Programa SPSS y Excel; Estadística descriptiva e inferencial para la prueba de hipótesis Para presentación de datos Cuadros, Tablas estadísticas y Gráficos, indicadores. Para el informe final: Esquema propuesto por el RGT-UNJFSC.

Anexo 2. Cuestionario de preguntas

A.-Presentación:

Las preguntas mostradas contéstalas con toda sinceridad, nos servirán para medir la variable gestión de identidades y accesibilidad en el Banco ITAÚ de Chile; se respetará el anonimato y confidencialidad en sus respuestas.

B.- Indicaciones:

Contestar cada pregunta marcando la respuesta marcando con una "X", en el recuadro que corresponda.

- ✓ La escala de calificación es la siguiente:

Totalmente en desacuerdo (1)	En desacuerdo (2)	Neutral (3)	De acuerdo (4)	Totalmente de acuerdo (5)

N°	Variable: Gestión de identidades	VALORACIÓN				
	Dimensión 01: Seguridad y Autenticación	1	2	3	4	5
1	¿Considera que el diseño propuesto incorpora adecuadamente mecanismos de autenticación multifactor (MFA) para proteger los accesos?					
2	¿Considera que el sistema diseñado podría reducir los riesgos de accesos no autorizados o incidentes de seguridad?					
3	¿Considera que la propuesta está alineada con buenas prácticas y estándares de seguridad de la organización?					
	Dimensión 02: Gestión del ciclo de vida de identidades					
4	¿Considera que el sistema diseñado facilitaría la creación, modificación y eliminación de cuentas de usuario según los roles asignados?					
5	¿Cree que el diseño permitiría desactivar automáticamente cuentas inactivas o no autorizadas?					
6	¿Considera que el diseño propuesto permitiría mantener actualizados los roles y permisos de acuerdo con cambios organizacionales?					
	Dimensión 03: Experiencia del Usuario y confianza en el IAM					
7	¿Considera que el sistema diseñado facilitaría un acceso integrado y confiable a los sistemas corporativos del banco?					
8	¿Está de acuerdo en que la propuesta ofrece una experiencia de acceso eficiente, confiable y segura para los usuarios?					
9	¿Considera que el diseño planteado generaría mayor confianza tecnológica entre los usuarios sobre el uso y seguridad de sus identidades?					
	Variable: Accesibilidad					
	Dimensión 01: Accesibilidad Tecnológica					
10	¿Está de acuerdo en que el sistema diseñado permitiría gestionar accesos desde diferentes dispositivos y plataformas corporativas?					
11	¿Considera que la propuesta permitiría un acceso oportuno y continuo a los sistemas para los usuarios autorizados?					
12	¿Considera que las herramientas tecnológicas incluidas en la propuesta serían fáciles de usar y accesibles para los colaboradores?					
	Dimensión 02: Accesibilidad Organizacional					
13	¿Está de acuerdo en que el diseño propuesto se adapta a la estructura organizacional, roles y jerarquías del Banco ITAÚ?					
14	¿Considera que la propuesta contempla documentación clara, accesible y adecuada para los usuarios según su perfil?					
15	¿Considera que la propuesta contempla una capacitación adecuada para facilitar el uso del sistema por parte de los colaboradores?					

	Dimensión 03: Control de acceso					
16	¿Está de acuerdo en que el diseño propuesto garantizaría que solo usuarios autorizados accedan a sistemas críticos?					
17	¿Considera que la propuesta respeta el principio de privilegios mínimos, asignando accesos según rol y función?					
18	¿Cree que el sistema diseñado permitiría auditar y monitorear los accesos para detectar irregularidades?					

Gracias por su colaboración

Anexo 3. Juicio de expertos

CRITERIOS	JUECES					Total
	J1	J2	J3	J4	J5	
Claridad:	*4*	3	3	5	4	19
Objetividad:	*3*	5	4	3	5	20
Actualidad:	*4*	4	3	4	4	19
Organización:	*3*	5	4	4	4	20
Suficiencia:	*5*	5	5	4	4	23
Intencionalidad:	*5*	4	4	4	3	20
Consistencia:	5	4	4	5	5	23
Coherencia:	4	5	4	4	4	21
Metodología:	5	4	5	4	5	23
Pertinencia:	5	4	4	5	4	22
TOTAL: de Opinión	43	43	40	42	42	210

Nota: Elaboración propia.

$$\boldsymbol{Validez = \frac{Total\ opinión}{Total\ máximo} = \frac{210}{10x5x5} = \frac{210}{250} = 0,84 = 84\%}$$

Total, Máximo = (Número de criterios). (Número de Jueces). (Puntaje Máximo de Respuesta).

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO:

TEMA: Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile-2024

JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo 2 = Malo 3 = Regular 4 = Bueno 5 = Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.				X	
Objetividad: Esta expresado en conductas observables.			X		
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organización: Existe una organización lógica.			X		
Suficiencia: Comprende los aspectos de cantidad y calidad.					X
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.					X
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.				X	
Metodología: La estrategia responde a los propósitos del estudio.					X
Pertinencia: El instrumento es adecuado al tipo de investigación.					X

Muchas Gracias por su Respuesta.

Datos y Firma del Juez Experto:
Dr. Collantes Rosas, Victor Manuel
DNI: 15623576

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO:

TITULO: Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile - 2024

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo 2 = Malo 3 = Regular 4 = Bueno 5 = Muy Bueno

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.			X		
Objetividad: Esta expresado en conductas observables.					X
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organización: Existe una organización lógica.					X
Suficiencia: Comprende los aspectos de cantidad y calidad.					X
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.				X	
Coherencia: Establece coherencia entre las variables y los indicadores.					X
Metodología: La estrategia responde a los propósitos del estudio.				X	
Pertinencia: El instrumento es adecuado al tipo de investigación.				X	

Muchas Gracias por su Respuesta.

Firma del Juez Experto
APELLIDOS Y NOMBRE: RIVERA MORALES LUIS ARSENIO
CIP: 58358

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO:

TITULO: Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile - 2024

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo **2 = Malo** **3 = Regular** **4 = Bueno** **5 = Muy Bueno**

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.			X		
Objetividad: Esta expresado en conductas observables.				X	
Actualidad: Adecuado al avance de la ciencia y la tecnología.			X		
Organización: Existe una organización lógica.				X	
Suficiencia: Comprende los aspectos de cantidad y calidad.					X
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.				X	
Coherencia: Establece coherencia entre las variables y los indicadores.				X	
Metodología: La estrategia responde a los propósitos del estudio.					X
Pertinencia: El instrumento es adecuado al tipo de investigación.				X	

Muchas Gracias por su Respuesta.

Firma del Juez Experto
APELLIDOS Y NOMBRE : GALLARDO ANDRÉS THOMAR ANGEL
CIP: 138158

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACION CON JUICIO DE EXPERTO:

TITULO: **Diseño de un sistema de gestión de identidades y accesibilidad en el Banco ITAÚ de Chile - 2024**

OPINION 6 JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo 2 = Malo 3 = Regular 4= Bueno 5 = Muy Bueno

CRITERIOS	VALORACION				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.					X
Objetividad: Esta expresado en conductas observables.			X		
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organizaci6n: Existe una organización lógica.				X	
Suficiencia: Comprende los aspectos de cantidad y calidad.				X	
intencionalidad: Adecuado para conocer las opiniones de las encuestadas.				X	
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.				X	
Metodología: La estrategia responde a los propósitos del estudio.				X	
Pertinencia: El instrumento es adecuado al tipo de investiQaci6n.					X

Muchas Gracias por su Respuesta.

Firma del Juez Experto
APELLIDOS Y NOMBRE: CANALES CHANGANAQUI ALDO MANUEL
GIP: 158627

Universidad Nacional
José Faustino Sánchez Carrión

VALIDACIÓN CON JUICIO DE EXPERTO:

TITULO: Diseño de un sistema de gestión de identidad y accesibilidad en el Banco ITAÚ de Chile - 2024

OPINIÓN Ó JUICIO DE EXPERTO:

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "**X**" dentro del cuadrado de Valoración, solo una vez por cada criterio, el que Ud. Considere su opinión.

1 = Muy Malo **2 = Malo** **3 = Regular** **4 = Bueno** **5 = Muy Bueno**

CRITERIOS	VALORACIÓN				
	1	2	3	4	5
Claridad: Esta formulado con lenguaje apropiado.				X	
Objetividad: Esta expresado en conductas observables.					X
Actualidad: Adecuado al avance de la ciencia y la tecnología.				X	
Organización: Existe una organización lógica.				X	
Suficiencia: Comprende los aspectos de cantidad y calidad.				X	
Intencionalidad: Adecuado para conocer las opiniones de las encuestadas.			X		
Consistencia: Basados en aspectos teóricos científicos de organización.					X
Coherencia: Establece coherencia entre las variables y los indicadores.				X	
Metodología: La estrategia responde a los propósitos del estudio.					X
Pertinencia: El instrumento es adecuado al tipo de investigación.				X	

Muchas Gracias por su Respuesta.

Firma del Juez Experto
APELLIDOS Y NOMBRE : DÍAZ RONCEROS ERNESTO
CIP: 197965

Anexo 4. Indicadores de alfa de Cronbach

Valoración de los indicadores de alfa de Cronbach

Rangos	Magnitud
0,81 a 1,00	Muy Alta
0,61 a 0,80	Alta
0,41 a 0,60	Moderada
0,21 a 0,40	Baja
0,01 a 0,20	Muy Baja

Anexo 5. Sobre la empresa

Banco Itaú Chile surge como resultado de una importante operación estratégica en el año 2006, cuando Bank of America Corporation acordó con Banco Itaú Holding Financiera S.A., con sede en Brasil, la transferencia de las operaciones de BankBoston en Chile y Uruguay.

Este acuerdo permitió a la entidad brasileña adquirir una posición relevante en el mercado financiero de América del Sur, a cambio de una participación accionaria.

La transacción se materializó el 26 de febrero de 2007, fecha en que Banco Itaú Chile inició formalmente sus operaciones en el país.

Esta integración marcó un hito relevante en la banca regional, fortaleciendo la expansión del grupo Itaú en el continente.

Desde su llegada a Chile, el banco ha evolucionado significativamente, no solo en volumen de operaciones, sino también en la sofisticación de sus servicios y en su transformación tecnológica. A lo largo de los años, Banco Itaú Chile ha incorporado

innovaciones que lo han posicionado como un actor clave en la industria financiera nacional.

En 2014, se llevó a cabo la integración de Banco Itaú Chile con Corpbanca, originando una entidad financiera con mayor presencia en el mercado y una cartera de productos más amplia.

Esta unión consolidó al banco como uno de los principales del sistema financiero chileno, con fuerte presencia en los segmentos de personas, empresas y banca corporativa.

Actualmente, el Grupo Itaú se posiciona como una de las principales entidades financieras de América Latina y mantiene relevancia dentro del sistema bancario internacional.

Es reconocido por su sólido gobierno corporativo, su responsabilidad social empresarial y su estrategia orientada a generar valor económico, social y ambiental para sus principales partes interesadas.

Organigrama Institucional

La estructura organizacional del Banco Itaú Chile se representa a través de un organigrama jerárquico, encabezado por el Directorio, seguido de la Gerencia General, desde donde se articulan las principales divisiones de negocio y apoyo. Este diseño permite una gestión eficiente y alineada con los objetivos estratégicos del banco, promoviendo la colaboración entre áreas y asegurando el cumplimiento normativo.

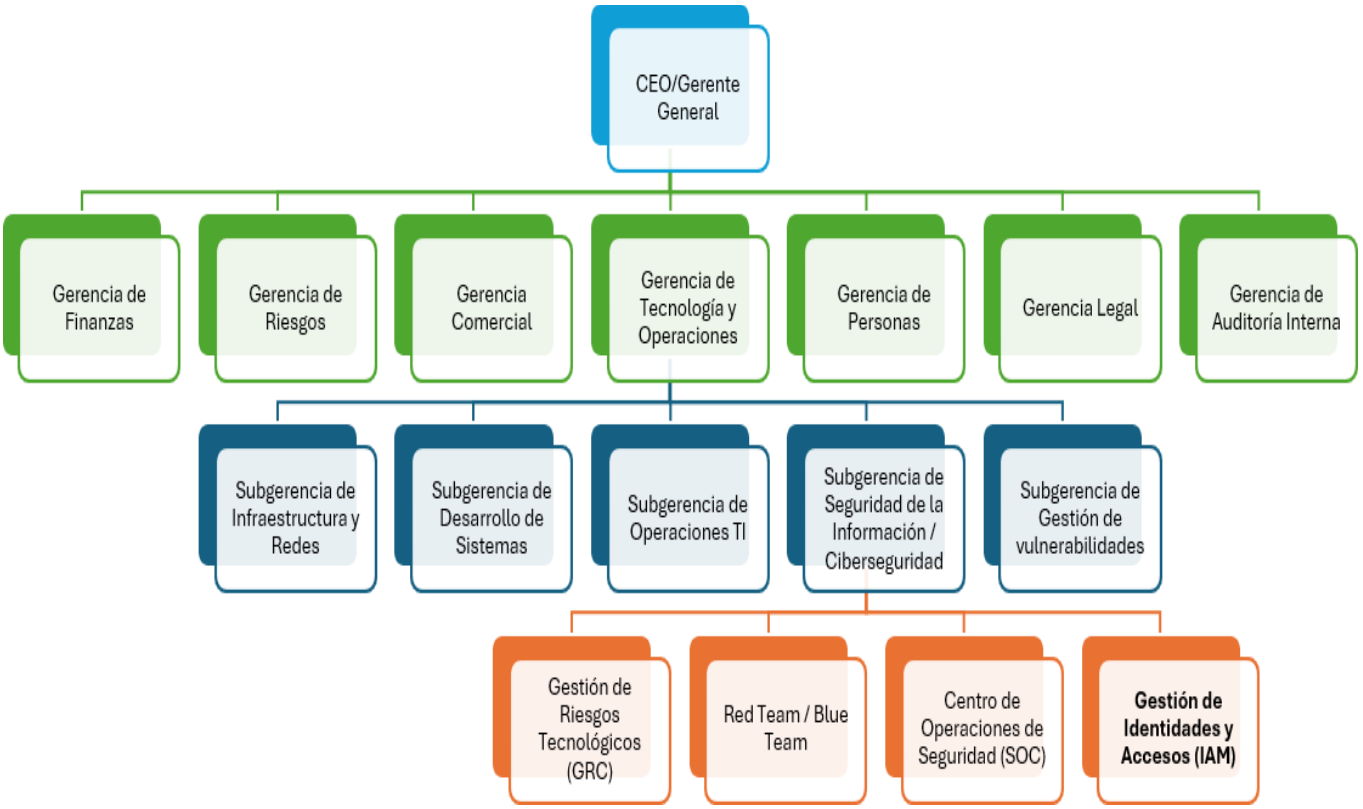


Figura 9. Organigrama de la organización.

Anexo 6. Diseño del sistema de gestión de identidades

Presentación de la propuesta

Ante el avance de la modernización tecnológica y creciente exposición a riesgos cibernéticos, el Banco Itaú de Chile enfrenta desafíos críticos en la administración de accesos a sus sistemas esenciales, tales como plataformas financieras, aplicaciones reguladas, sistemas de gestión y servicios en la nube. La asignación manual de permisos, la existencia de cuentas huérfanas, accesos excesivos o no autorizados, así como la ausencia de un control efectivo del ciclo de vida de los usuarios, representan riesgos operacionales, de cumplimiento normativo y de seguridad de la información.

Ante esta problemática, se propuso una solución integral para la administración de identidades y accesibilidad (IAM), basada en el modelo Role-Based Access Control (RBAC) y soportado tecnológicamente en la plataforma IBM Verify Identity Governance (IVIG). Esta solución permite centralizar y automatizar la administración de identidades, aplicar controles de gobernanza, implementar segregación de funciones (SoD), fortalecer la trazabilidad de accesos y asegurar el cumplimiento de normativas.

El diseño propuesto tiene como enfoque principal estructurar los accesos con base en funciones y actividades de negocio, minimizando el riesgo por privilegios excesivos, asegurando la correspondencia entre el rol del usuario y los permisos asignados, y habilitando mecanismos de aprobación, recertificación y auditoría continua.

Modelo RBAC aplicado al Banco Itaú de Chile

El modelo Role-Based Access Control (RBAC) se fundamenta en la asignación de permisos a partir de los roles funcionales que desempeñan los usuarios dentro de la organización.

En este enfoque, el acceso ya no se otorga a nivel individual, sino que se estructura mediante roles, los cuales agrupan permisos específicos asociados a funciones laborales, actividades de negocio y niveles de riesgo.

Esto permitió gestionar los accesos de manera centralizada, coherente y alineada con criterios de privilegios estrictamente necesarios y acceso limitado a la información requerida

En el contexto del Banco Itaú de Chile, los roles definidos bajo el modelo RBAC representan funciones como Ejecutivo Comercial, Analista de Riesgos, Supervisor de Operaciones, Especialista TI, Compliance Officer o Auditor Interno.

Cada uno de estos roles se vincula a actividades de negocio, sistemas corporativos (Azure AD, SAP, Core Banking, CRM, IGI), módulos y permisos específicos, según el nivel de responsabilidad y criticidad de sus funciones.

La aplicación de RBAC permite establecer una estructura ordenada, controlada y escalable de accesos, aportando beneficios clave:

Beneficio	Descripción
Seguridad reforzada	Los usuarios acceden únicamente a los recursos necesarios según sus funciones (principio de mínimo privilegio).
Administración eficiente	Los cambios de cargo o función actualizan automáticamente los permisos asignados (Joiner–Mover–Leaver).
Trazabilidad y auditoría	Cada asignación, modificación o revocación de accesos queda registrada con evidencia para cumplimiento y auditoría.
Segregación de funciones (SoD)	Se previenen combinaciones conflictivas de permisos que puedan generar riesgo operativo o fraude (ej. Registrar y Aprobar).
Cumplimiento normativo	Contribuye al cumplimiento de normas.

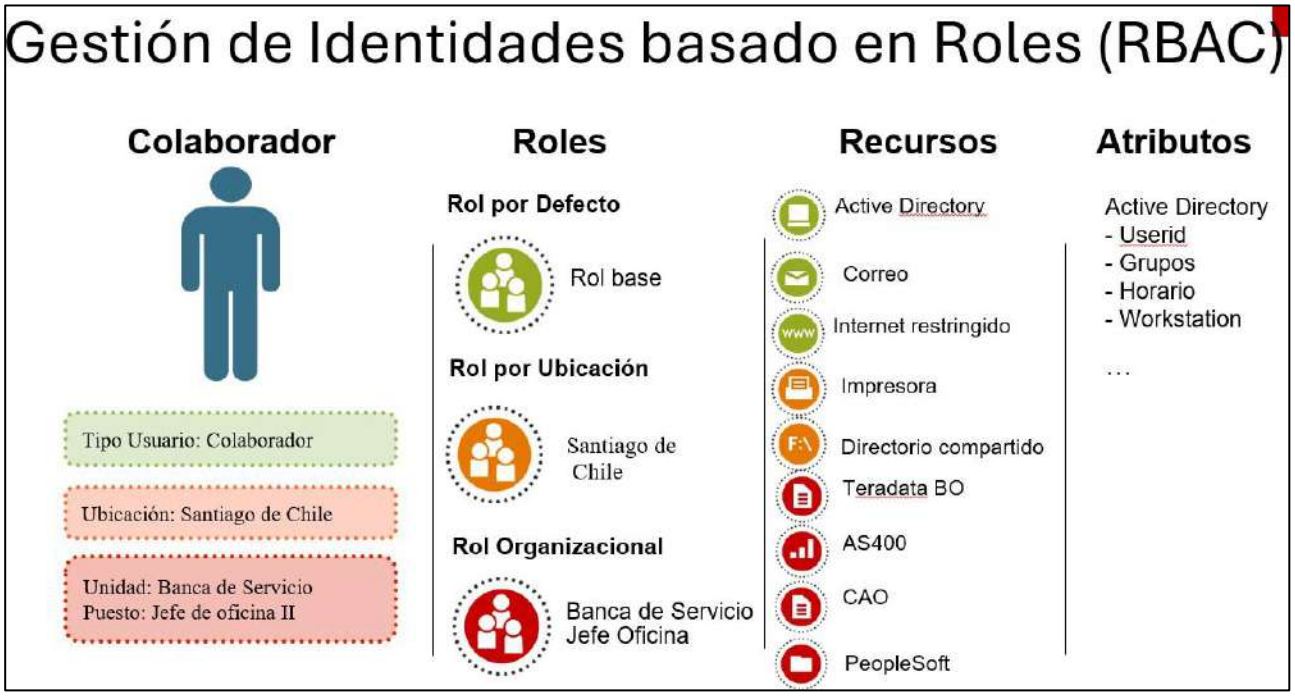


Figura 10. Diagrama conceptual del modelo RBAC aplicado al Banco ITAÚ.

Gestión centralizada de identidades y accesibilidad con IBM Verify Identity Governance V11

La solución propuesta para la gestión centralizada de identidades y accesibilidad en el Banco Itaú de Chile se fundamenta en la implementación de la plataforma IBM Verify Identity Governance (IVIG). Esta herramienta permite automatizar el ciclo de vida de los accesos, gestionar identidades bajo el modelo RBAC, aplicar políticas de segregación de funciones (SoD), ejecutar procesos de certificación periódica y garantizar la trazabilidad completa de los accesos a sistemas críticos.

El diseño propuesto contempla una arquitectura modular, que integra autenticación corporativa, administración de roles, provisión automática de accesos, workflows aprobatorios, auditoría y cumplimiento regulatorio De esta manera, se asegura que los usuarios accedan únicamente a los recursos necesarios según sus funciones, con respaldo normativo, evidencia auditable y menor riesgo operativo.

Para su implementación, la plataforma se despliega en dos componentes funcionales complementarios, que trabajan de forma integrada y cumplen roles diferenciados dentro del modelo de gobernanza de accesos:

Consola de Administración de Accesos.

Interfaz dirigida al equipo de Gestión de Accesos. Desde esta consola se realiza la administración centralizada de identidades, se configuran políticas de acceso, se gestionan roles RBAC y políticas SoD, se ejecutan

procesos de certificación y se generan reportes para cumplimiento normativo y auditoría.

A través de esta consola, la organización garantiza:

- Control corporativo sobre accesos y permisos.
- Cumplimiento de normas
- Gobierno y trazabilidad de identidades, cuentas y roles críticos.
- Prevención de accesos conflictivos mediante SoD y controles de mitigación.

A continuación, detallamos la interfaz de la consola de administración:

Acceso al sistema (Login corporativo)

El ingreso a IBM Verify Identity Governance se realiza mediante una interfaz de autenticación integrada con Active Directory (AD), lo que permite a los colaboradores iniciar sesión utilizando sus credenciales corporativas.

Esta integración habilita autenticación centralizada, reduce el uso de múltiples contraseñas, mejora la experiencia del usuario e incrementa el nivel de seguridad al incorporar políticas institucionales de acceso.

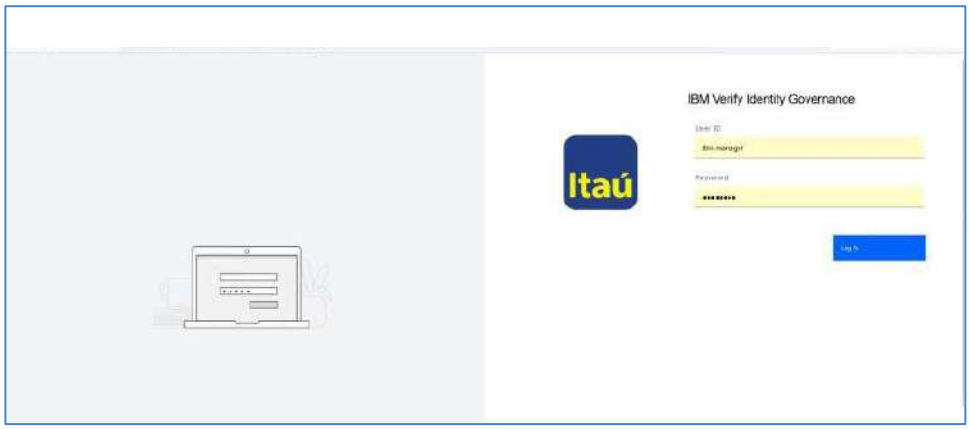


Figura 11. Pantalla de login con autenticación vía Active Directory.

Dashboard personalizado según rol

Una vez autenticado, el usuario accede a un panel dinámico que muestra indicadores clave (KPIs) sobre el estado de identidades, roles activos, cuentas huérfanas, violaciones SoD, campañas de certificación y cumplimiento normativo. El contenido mostrado varía según el rol del usuario (administrador, auditor, supervisor, etc.).

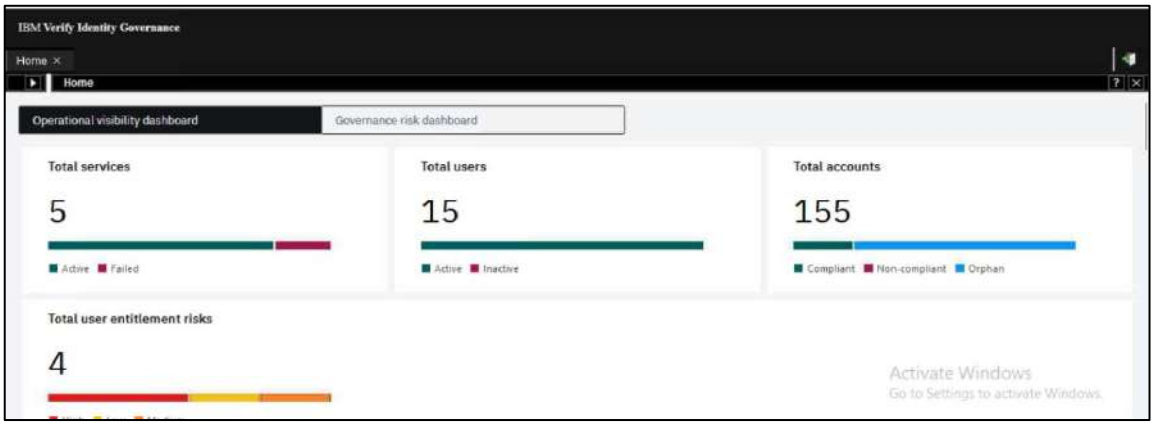


Figura 12. Pantalla del dashboard de inicio, servicios, usuarios, cuentas y SoD

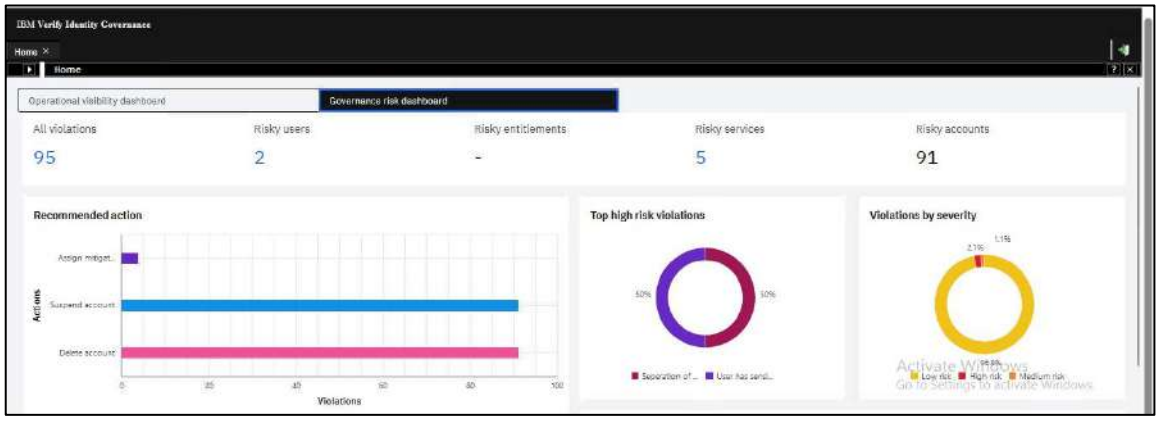


Figura 13. Pantalla del dashboard riesgos.

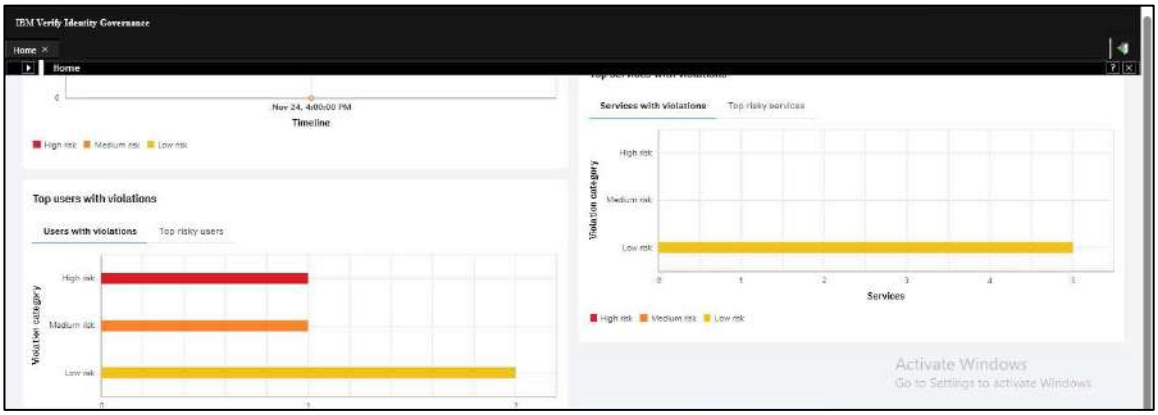


Figura 14. Pantalla del dashboard de usuarios y su nivel de riesgos.

Gestión de identidades y entidades

Este módulo permite centralizar la administración de identidades, visualizar los usuarios registrados, su tipo (empleado, contratista, auditor, técnico), su estado (activo, inactivo, suspendido) y los roles asignados.

Desde esta vista se puede acceder a los detalles de perfil, cuentas vinculadas, roles, unidad organizativa y certificados de acceso.

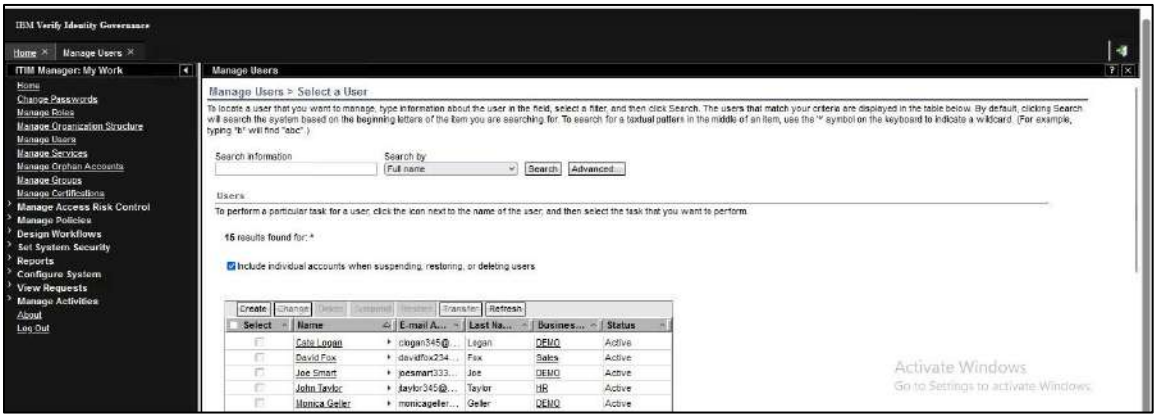


Figura 15. Vista del módulo “Manage Users”, con usuarios, estado, unidad de negocio y acciones administrativas.

Cuentas vinculadas a una identidad

Este apartado muestra todas las cuentas asociadas a una identidad en diversas aplicaciones como SAP, Active Directory, Azure AD, Core Banking o sistemas internos.

Se visualizan permisos técnicos, estado de la cuenta, últimos accesos y nivel de riesgo, lo cual permite detectar cuentas huérfanas, duplicadas o con privilegios excesivos.

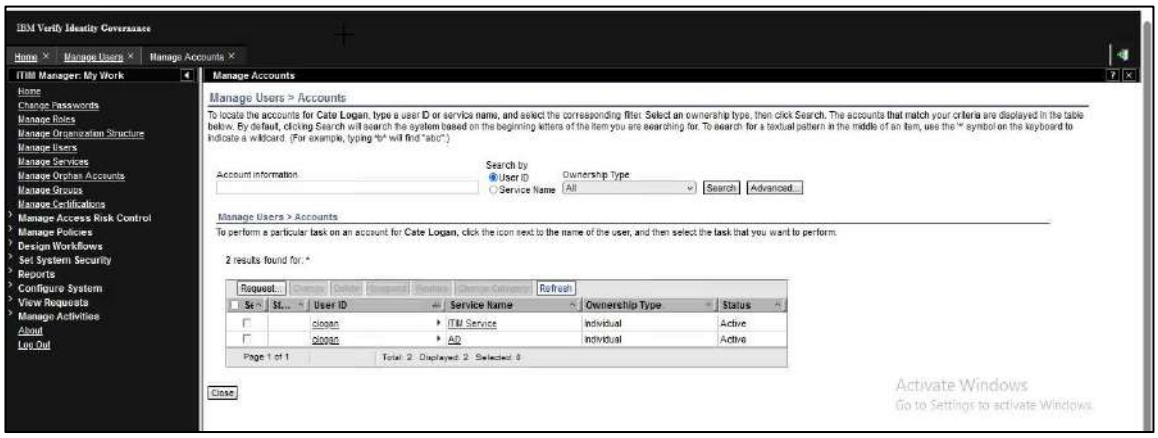


Figura 16. Vista de Gestión de cuentas vinculadas a una misma identidad con visualización de roles, estado y nivel de riesgo.

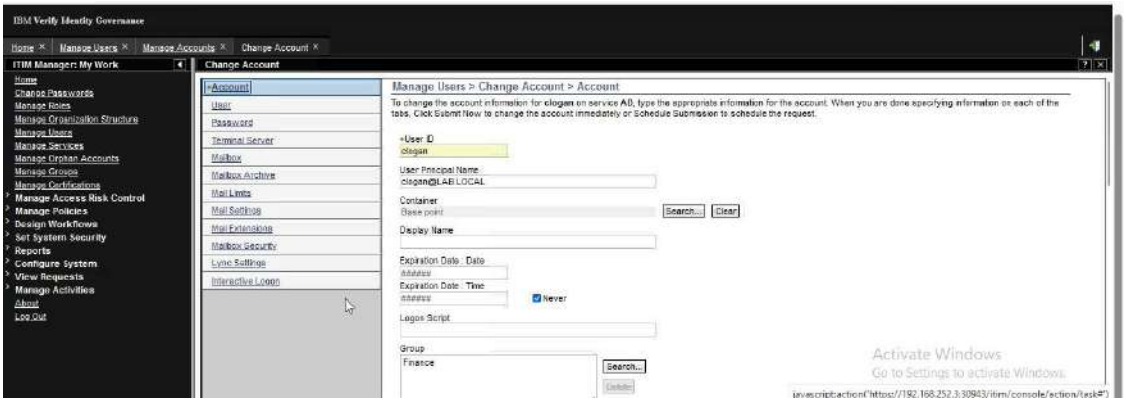


Figura 17. Visualización de información completa de la cuenta del usuario.

Gestión y asignación de roles (RBAC)

El módulo Manage Roles permite gestionar los roles de organizacionales (Dinámicos) y roles manuales (Estáticos) definidos bajo el modelo RBAC del Banco Itaú. Desde esta vista, el administrador puede crear, modificar o desactivar roles; asignarles servicios o aplicaciones; definir la unidad de negocio a la que pertenecen; y vincularlos a políticas de suministro, SoD y campañas de certificación.

Cada rol representa un conjunto predefinido de permisos asociados a una función laboral. Por ejemplo, los roles "Finance", "Development" o "BirthRightAccess" agrupan los accesos necesarios según la posición del usuario dentro del banco, considerando únicamente los privilegios necesarios y la información que el usuario requiere para desempeñar sus actividades.

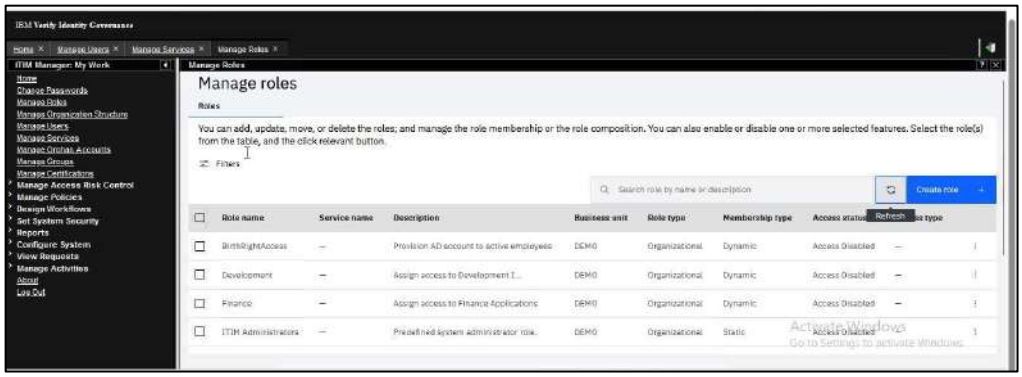


Figura 18. Vista del módulo Manage Roles, con roles de negocio, unidad organizativa, tipo de membresía y estado de acceso.

Unidad organizativa

El sistema permite vincular cada identidad con su unidad organizativa (área, filial, departamento, sucursal), lo cual determina los roles permitidos, supervisores de aprobación, responsables de certificación y políticas aplicables.

Figura 19. Vista estructura organizacional del Banco Itaú integrada en IBM IVIG.

Servicios y Perfiles de Aplicación

El módulo Manage Services permite visualizar y administrar los servicios y sistemas integrados al modelo de gestión de identidades, como Active Directory (AD), Azure AD, Linux, Core Banking, SAP, HRIS o IBM Verify SaaS.

Cada servicio representa una aplicación empresarial donde los usuarios pueden tener cuentas técnicas, accesos operativos o privilegios administrativos.

9

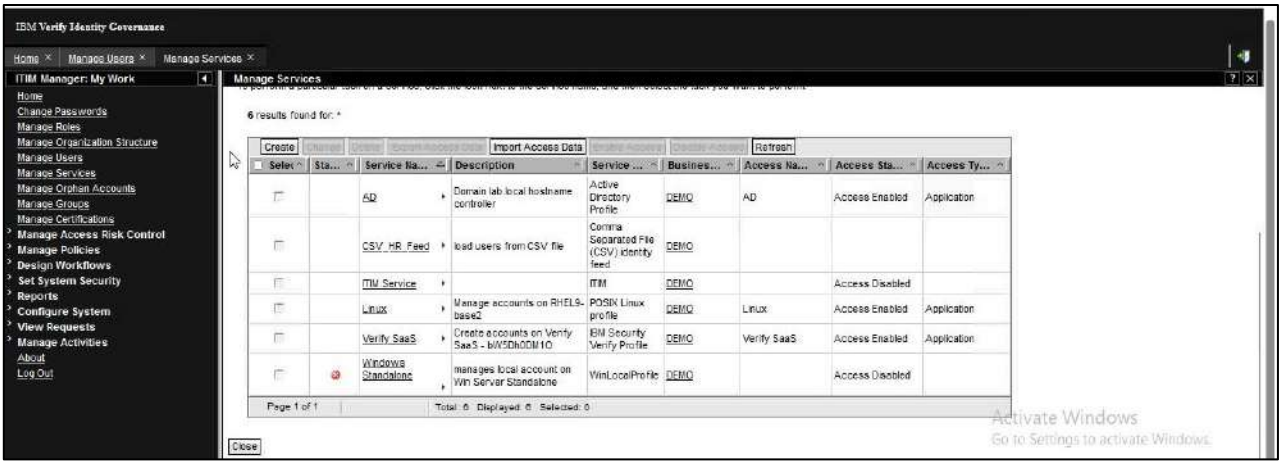


Figura 20. Vista Gestión de servicios y perfiles de aplicación integrados en IBM Verify Identity Governance.

Políticas de suministro

El módulo Políticas de suministro permite configurar y administrar las políticas de provisión automática de accesos.

Estas políticas definen qué permisos son otorgados a los usuarios cuando se les asigna un rol, cambian de posición dentro de la organización o cuando ingresan o salen de la empresa, en cumplimiento con el ciclo JML (Joiner–Mover–Leaver).

Cada política de provisión se vincula a un rol del modelo RBAC y determina los permisos técnicos (entitlements) que serán otorgados automáticamente en los sistemas conectados, tales como Active Directory, SAP, Azure AD, Linux o Core Banking.

Figura 21. Vista de las políticas de suministro en IBM Verify Identity Governance

Políticas de Contraseña y Seguridad de Autenticación en IBM IVIG

Dentro del módulo Manage Policies → Manage Password Policies, IBM IVIG permite definir reglas específicas para el control de contraseñas, garantizando el cumplimiento de estándares regulatorios y mejores prácticas de seguridad.

La vista Rules muestra los parámetros configurables que permiten asegurar la robustez, complejidad, rotación y trazabilidad de las credenciales utilizadas en la plataforma.

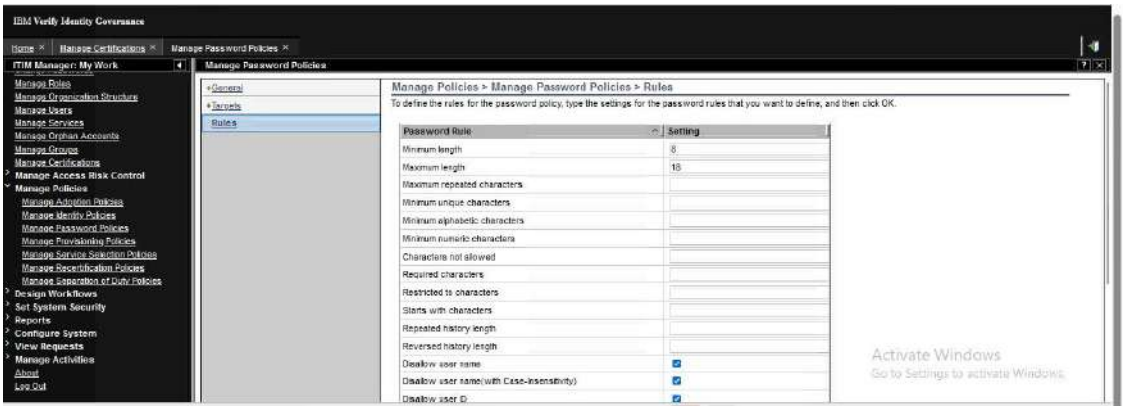


Figura 22. Vista de Configuración de reglas de contraseñas en IBM Verify Identity Governa

Gestión de Riesgos y Segregación de Funciones (SoD)

La plataforma IBM Verify Identity Governance permite identificar, gestionar y mitigar riesgos operacionales derivados del acceso indebido a funciones conflictivas. En el contexto del Banco Itaú, se utiliza el modelo SoD (Segregation of Duties) para prevenir que un mismo usuario tenga permisos que puedan generar fraude, manipulación financiera o incumplimiento regulatorio.

Actividades de negocio

Las Actividades de negocio representan tareas críticas dentro de los procesos del banco, como creación de órdenes, gestión de nómina, autorizaciones financieras, acceso a datos sensibles o administración de infraestructura.

Estas actividades se utilizan como base para construir reglas de SoD, evaluar riesgos y asociar controles preventivos.

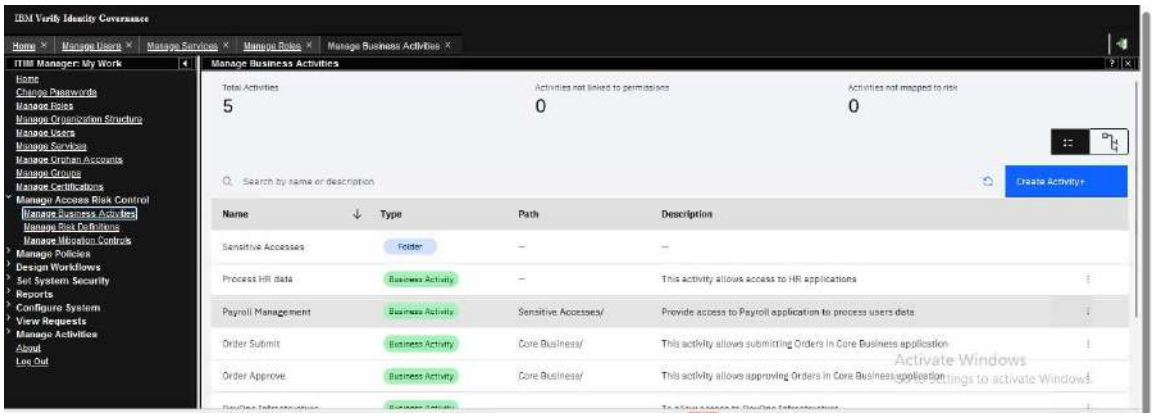


Figura 23. Vista de actividades de negocio definidas en IBM IVIG.

Definición de Riesgos de Acceso y Conflictos SoD

En esta sección se configuran los riesgos asociados a la combinación inadecuada de actividades o roles.

Aquí se definen riesgos sensibles (acceso a información crítica) y riesgos SoD (conflictos de aprobación y ejecución en un mismo usuario).

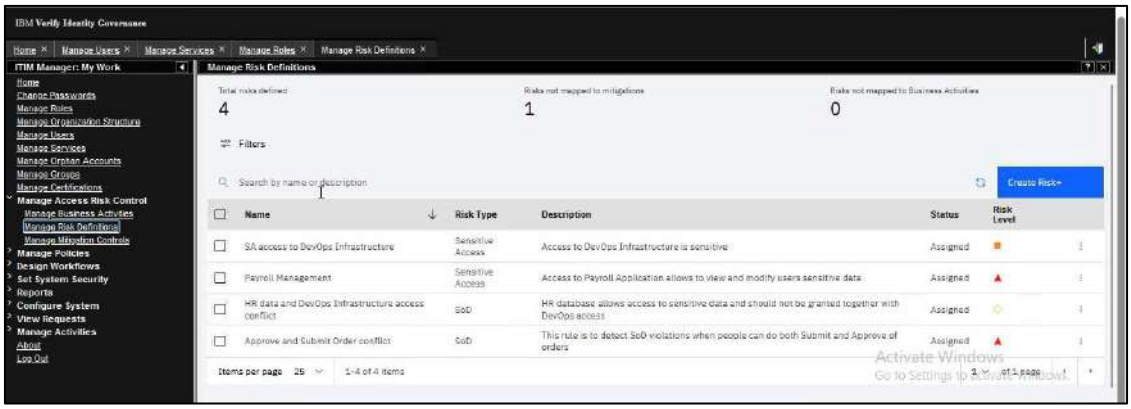


Figura 24. Vista de Definición de riesgos SoD y accesos sensibles.

Controles de mitigación

Cuando una función conflictiva es necesaria por razones operativas excepcionales, el sistema aplica controles compensatorios para mantener la trazabilidad y el cumplimiento. IBM IVIG permite configurar medidas como:

Supervisión del acceso por parte de un superior

✓ Revisión semanal de registros de actividad

✓ Autorización dual (four-eyes principle)

✓ Auditoría trimestral o inmediata

✓ Reportes automáticos a cumplimiento y riesgo

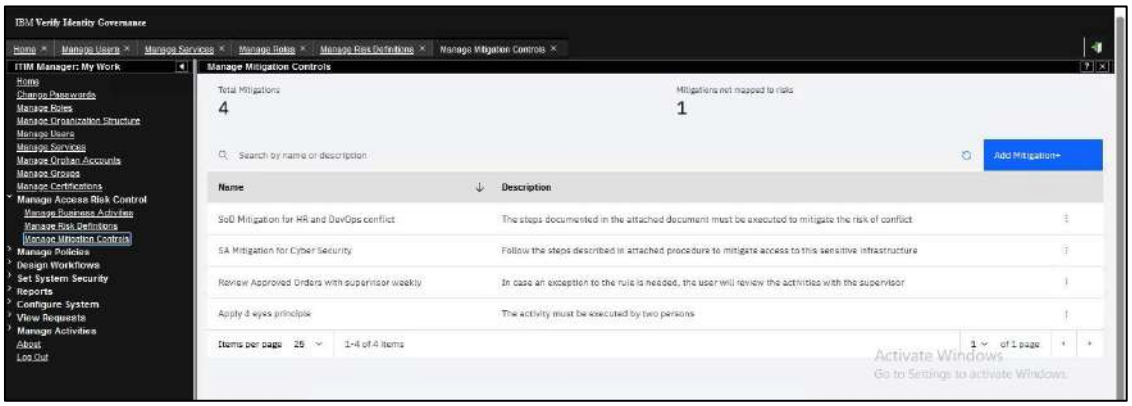


Figura 25. Vista de los controles de mitigación.

Reportes

El módulo Requests Reports permite generar informes detallados sobre todas las operaciones relacionadas con la gestión de accesos: solicitudes, aprobaciones, rechazos, tipo de acceso, fecha, usuario solicitante, autorizador, cambios aplicados y justificación.

Estos reportes son fundamentales para cumplir con los requisitos de auditoría interna y externos.

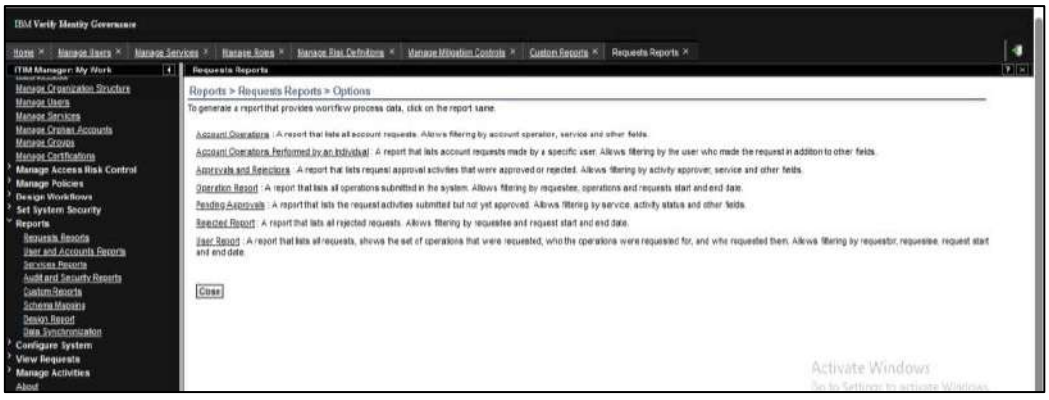


Figura 26. Vista del módulo de reportes.

Gestión de Solicitudes de Acceso

El módulo View All Requests permite visualizar el historial completo de solicitudes realizadas en el sistema, incluyendo peticiones de creación de cuentas, asignación de roles, modificación de permisos o deshabilitación de accesos.

Cada solicitud queda registrada con información detallada sobre quién la realizó, el tipo de acceso solicitado, el sistema afectado, la fecha, el resultado y el estado de aprobación.

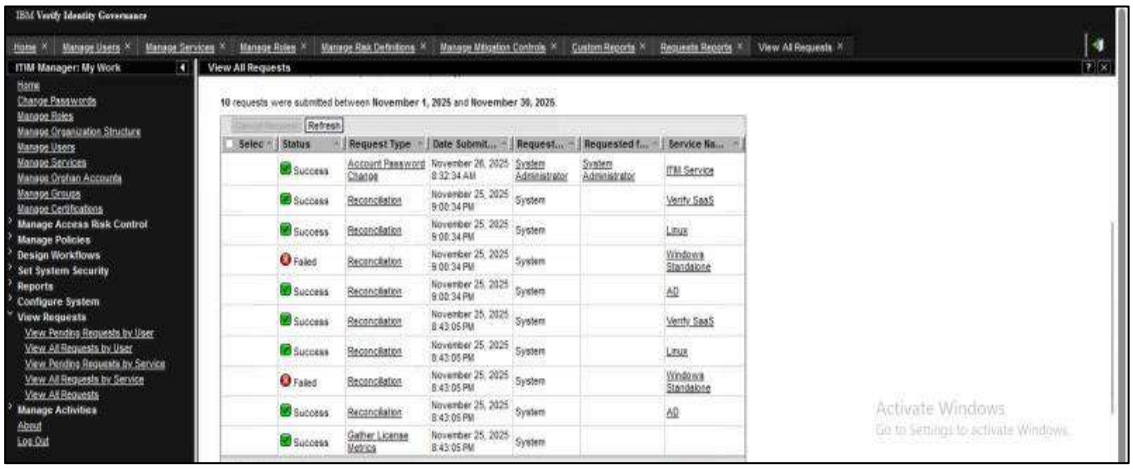


Figura 27. Vista de registro de solicitudes de acceso realizadas en IBM Verify Identity Governance.

Portal del Usuario Final

Interfaz orientada a los colaboradores del Banco Itaú, diseñada para facilitar la autogestión de accesos, reduciendo la carga operativa de TI y fortaleciendo la eficiencia organizacional. Desde este portal, cada usuario puede

✓ Solicitar accesos a aplicaciones según catálogo autorizado

✓ Realizar seguimiento de solicitudes (estado, aprobación, rechazo)

✓ Recuperar contraseñas.

✓ Gestionar datos del perfil y ver los accesos habilitados.

✓ Aprobar accesos si es supervisor, dueño de aplicación o auditor.

Este portal permite equilibrar gobernanza, autonomía del usuario y operatividad, contribuyendo directamente a los objetivos del banco en materia de continuidad operativa, seguridad y cumplimiento.

Pantalla de Login

El acceso al portal de autogestión se realiza mediante una pantalla de autenticación, que permite validar la identidad del usuario utilizando credenciales corporativas del Active Directory, o bien mediante mecanismos de MFA (doble factor) si el rol o nivel de privilegio así lo requiere.

Esta autenticación es administrada mediante un inicio de sesión único, lo que permite un ingresar de formar centralizada y seguro a los módulos del sistema sin necesidad de múltiples inicios de sesión. Al validar exitosamente la identidad, el usuario es redirigido al portal, donde podrá acceder a opciones personalizadas según su rol (puesto funcional).

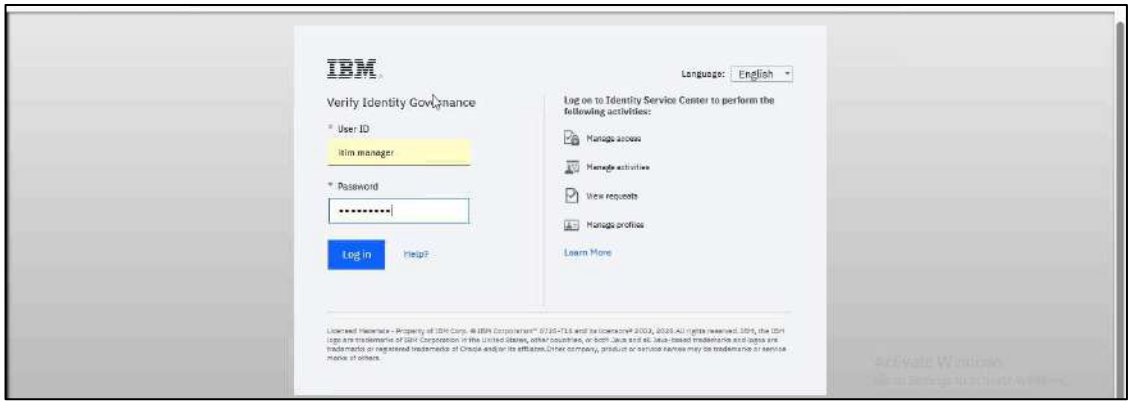


Figura 28. Pantalla de autenticación para acceso al Identity Service Center de IBM IVIG

Interfaz principal del usuario final

Una vez autenticado, el usuario accede al Portal de Autogestión**,** donde se despliega un panel de inicio con las funcionalidades habilitadas según su rol organizacional (empleado, supervisor, auditor, dueño de aplicación, responsable de riesgos, etc.).

Este portal permite que cada colaborador gestione sus accesos de forma segura, eficiente y trazable, sin depender del área de TI, lo que mejora la operación, disminuye tiempos de solicitud y fortalece el cumplimiento de políticas IAM.

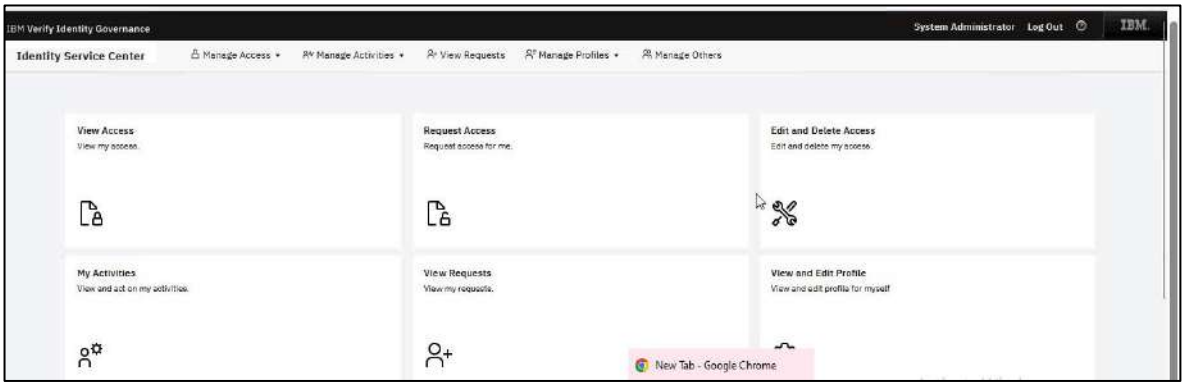


Figura 29. Interfaz principal– Autogestión de accesos y actividade

Gestión de perfil de identidad

La funcionalidad View and Edit Profile permite a los usuarios consultar y actualizar la información asociada a su identidad dentro del sistema.

De esta forma, IBM IVIG asegura que los accesos otorgados estén alineados con el cargo, unidad organizativa, ubicación y funciones que el colaborador desempeña dentro del Banco Itaú.

Figura 30. Gestión y visualización del perfil de identidad desde el Portal de Usuario Final

Autogestión de Contraseñas

En este módulo, el usuario final puede realizar el cambio de su contraseña de manera autónoma, sin depender del equipo de gestión de accesos o Mesa de Ayuda. Este módulo permite mejorar la operatividad, reducir tiempos de respuesta y fortalecer el cumplimiento de controles de seguridad.

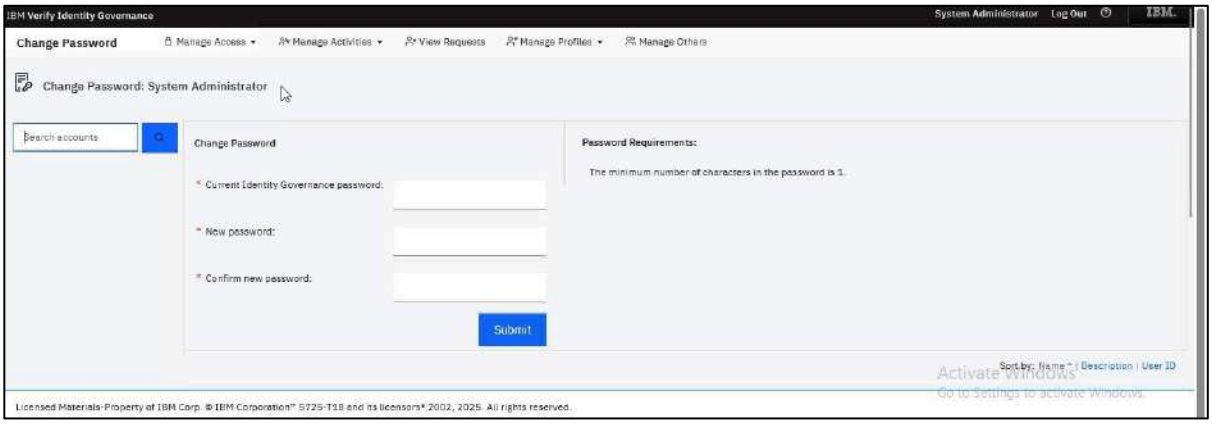


Figura 31. Vista del módulo de cambio de contraseña

Seguimiento y estado de mis solicitudes

Este módulo permite al usuario final realizar el seguimiento de todas las solicitudes que ha generado en la plataforma, tales como pedidos de acceso, activación de cuentas, sincronización de contraseñas o modificaciones de perfil. A través de un portal intuitivo, el usuario puede visualizar el estado de cada solicitud (Pendiente, Aprobado, Rechazado, En Proceso o Completado) y acceder a los detalles asociados, como fechas, aprobadores, etapas del workflow y sistemas involucrados.

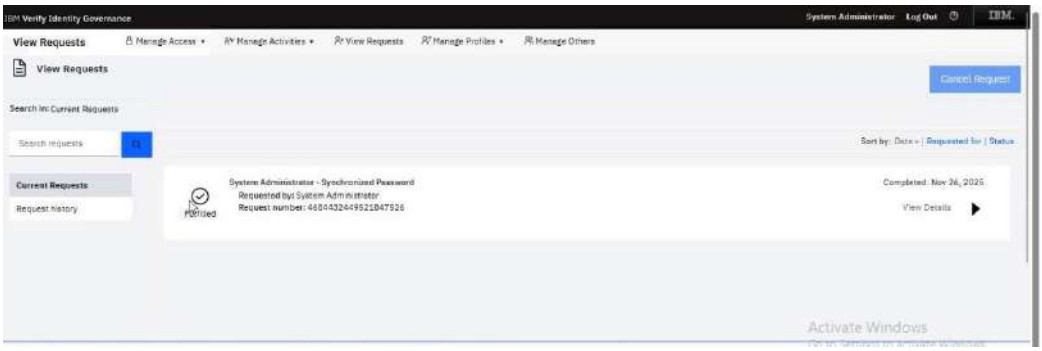


Figura 32. Vista del Módulo de seguimiento de solicitudes

Plan de despliegue de la solución de gestión de identidades para la mejora de la accesibilidad

La solución planteada se desarrolló mediante un plan de implementación estructurado, que asegura el despliegue ordenado, seguro y controlado de la plataforma IBM Verify Identity Governance (IVIG), considerando tanto componentes técnicos como organizacionales (roles, procesos JML, gestión del cambio y cumplimiento normativo).

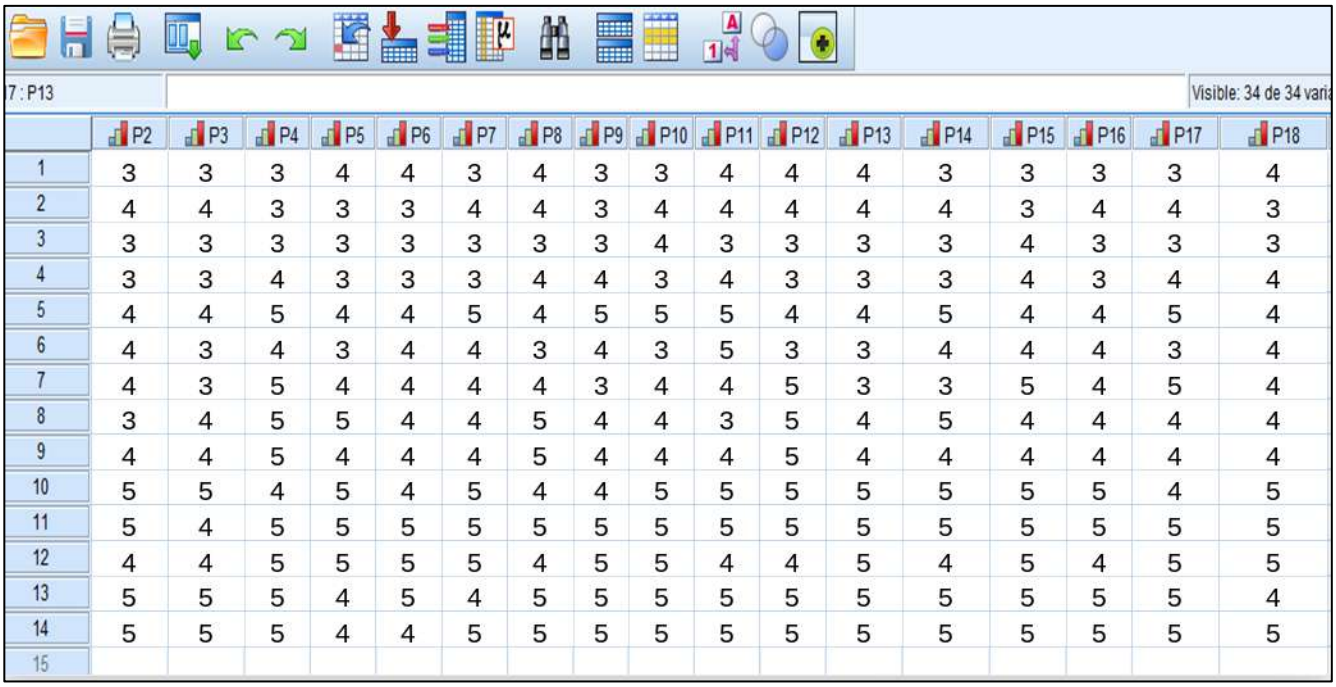
Este plan se organiza en cinco fases, alineadas con metodologías de implementación ITIL, COBIT y Project Management Institute (PMI), integrando aspectos de seguridad, automatización y gobernabilidad del acceso.

Tabla 15.

Plan de Implementación del Sistema de Gestión

Fase	Actividad principal	Detalle de actividades	Duración
1	Análisis técnico y diseño de arquitectura	Levantamiento de roles (RBAC), accesos, matrices SoD, flujos JML, sistemas críticos, arquitectura de identidad.	2 semanas
2	Instalación de infraestructura y configuración HA	Instalación de IVIG, servidores, clústeres, LDAP, base de datos, alta disponibilidad (HA)	3 semanas
3	Implementación de IVIG y conectores	Configuración de conectores (Active Directory, SAP, Azure AD), roles, password, SoD, políticas de provisión.	6 semanas
4	Pruebas funcionales y de integración (UAT / QA)	Pruebas técnicas, validación SoD, estrés, performance, user testing, mitigación de errores.	2 semanas
5	Capacitación, documentación y traspaso operativo	Capacitación a administradores, áreas negocio, mesa de ayuda, entrega de manuales, cuadro RACI, aseguramiento normativo.	1 semana

Anexo 7. Matriz de datos del instrumento aplicado

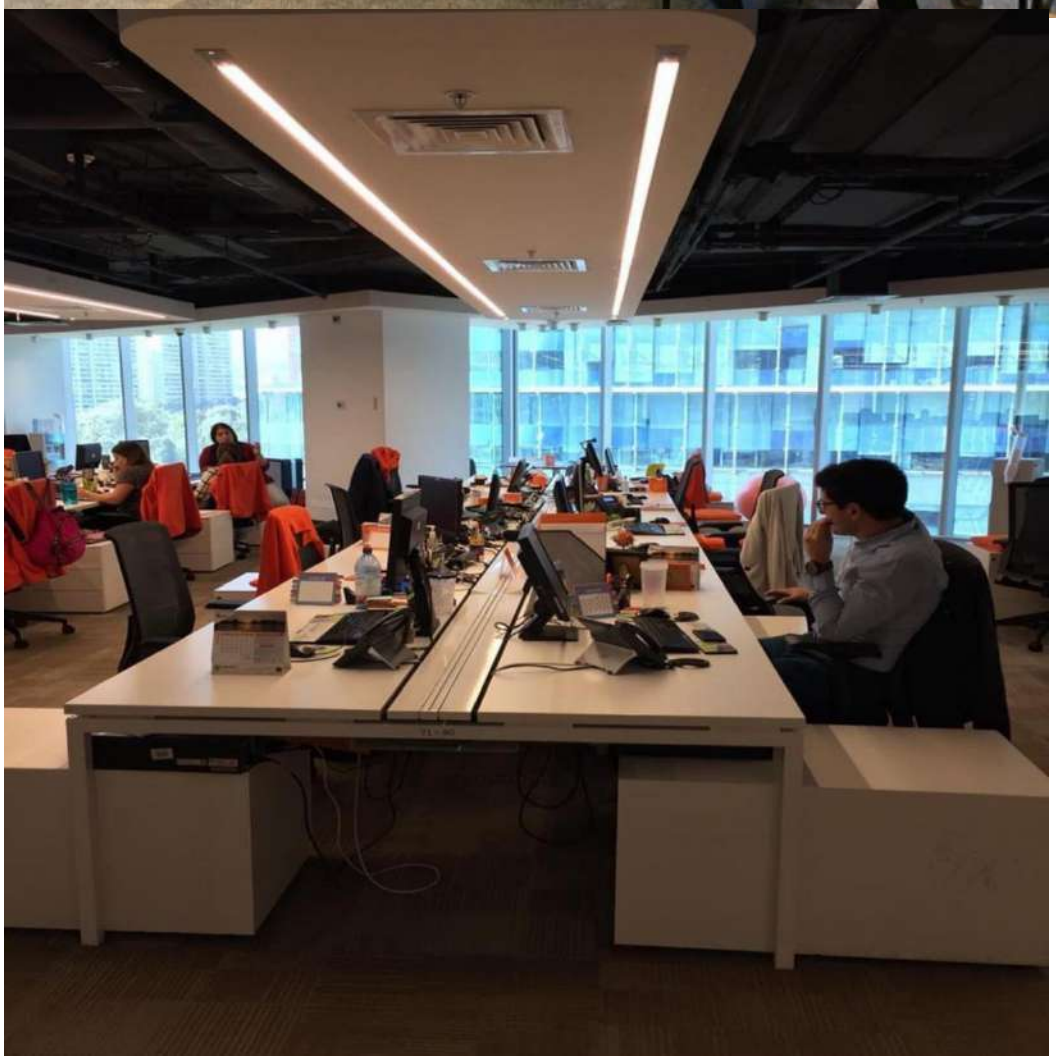


7 : P13 — Visible: 34 de 34 varia

	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18
1	3	3	3	4	4	3	4	3	3	4	4	4	3	3	3	3	4
2	4	4	3	3	3	4	4	3	4	4	4	4	4	3	4	4	3
3	3	3	3	3	3	3	3	3	4	3	3	3	3	4	3	3	3
4	3	3	4	3	3	3	4	4	3	4	3	3	3	4	3	4	4
5	4	4	5	4	4	5	4	5	5	5	4	4	5	4	4	5	4
6	4	3	4	3	4	4	3	4	3	5	3	3	4	4	4	3	4
7	4	3	5	4	4	4	4	3	4	4	5	3	3	5	4	5	4
8	3	4	5	5	4	4	5	4	4	3	5	4	5	4	4	4	4
9	4	4	5	4	4	4	5	4	4	4	5	4	4	4	4	4	4
10	5	5	4	5	4	5	4	4	5	5	5	5	5	5	5	4	5
11	5	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
12	4	4	5	5	5	5	4	5	5	4	4	5	4	5	4	5	5
13	5	5	5	4	5	4	5	5	5	5	5	5	5	5	5	5	4
14	5	5	5	4	4	5	5	5	5	5	5	5	5	5	5	5	5
15																	

Anexo 8. Jornada laboral en el Banco Itaú

Anexo 9. Banco Itaú – Equipo de seguridad de la información



Anexo 10. Edificio Corporativo Banco Itaú Chile