Propuesta de un modelo de gestión del ciclo de vida de identidades para una empresa del sector retail: evaluación de alternativas tecnológicas para mejorar la seguridad, eficiencia operativa y cumplimiento normativo.

Elaborado por:

Tatiana Ortiz Rodriguez

Nestor Julian Ortiz Gutierrez

Sergio Andres Palomares Sanabria

Iván Alexander La Rotta Castro

Universidad EAN

Escuela de Formación en Investigación

Seminario de Investigación de Pregrado

Bogotá

31/07/2025

Resumen

El sector retail se enfrenta a retos crecientes en la administración del ciclo de vida de identidades, derivados de la alta rotación laboral y la integración de Múltiples sistemas digitales. Esta investigación propone el diseño de un modelo de gestión de identidades orientado a fortalecer la seguridad de la información, incrementar la eficiencia operativa y garantizar el cumplimiento normativo. La investigación adopta un enfoque mixto con diseño no experimental, de tipo transversal y aplicado. Se emplean cuestionario de preguntas abiertas, análisis comparativo de soluciones tecnológicas y una matriz de valoración para la recolección y análisis de datos. El estudio se sustenta en marcos teóricos como RBAC y ABAC, integrando criterios de automatización, trazabilidad y cumplimiento de estándares internacionales Los hallazgos de esta investigación aprueban que un modelo integral de gestión del ciclo de vida de identidades, basado en la combinación de Oracle Identity Management y Okta Identity Governance, responde eficazmente a los principales desafíos del sector retail. En conjunto, estos resultados validan que un IAM diseñado bajo un enfoque mixto y secuencial no solo fortalece la seguridad de la información y el cumplimiento normativo, sino que también impulsa la agilidad y la eficiencia operativa de las empresas retail, aportando una herramienta estratégica para gestionar identidades en entornos digitales cada vez más complejos y dinámicos.

Palabras clave: Gestión de identidades, seguridad de la información, administración de accesos, cumplimiento normativo, eficiencia operativa, sector retail.

TABLA DE CONTENIDO

CONTENIDO DE FIGURAS

CONTENIDO DE TABLAS

CONTENIDO DE ANEXOS

PROBLEMA DE INVESTIGACIÓN

En el sector retail, la seguridad de la información, la eficiencia operativa y el cumplimiento normativo dependen en gran medida de una gestión adecuada de las identidades y accesos de los usuarios a los sistemas informáticos. Sin embargo, la falta de un modelo estructurado para administrar el ciclo de vida de identidades ha generado vulnerabilidades significativas en las organizaciones, propiciando accesos no autorizados, errores en la asignación de privilegios y dificultades en la trazabilidad de los usuarios dentro de la infraestructura digital. Según Keshet (2024), la ausencia de un sistema de administración de identidades aumenta el riesgo de brechas de seguridad y puede comprometer la integridad de los datos corporativos. Este problema se ve agravado por la creciente digitalización de los procesos empresariales, donde múltiples sistemas interconectados requieren controles rigurosos de autenticación y autorización para evitar la filtración o manipulación de información crítica.

El origen del problema radica en la gestión manual y descentralizada de las identidades digitales, lo que genera inconsistencias en el control de accesos y aumenta la probabilidad de errores humanos. En las empresas del sector retail, caracterizadas por una alta rotación de personal y la integración constante de nuevas herramientas tecnológicas, la administración de credenciales de usuario se vuelve un proceso complejo y susceptible a fallos. SINFOPAC, (2024), sostienen que la falta de automatización en la gestión del ciclo de vida de identidades incrementa la carga operativa de los departamentos de Tecnologías de la Información (TI), reduciendo la capacidad de respuesta ante incidentes de seguridad y comprometiendo la continuidad del negocio. Además, la ausencia de controles centralizados impide establecer mecanismos de auditoría de efectivos, lo que dificulta la detección temprana de accesos sospechosos o fraudes internos.

Los síntomas de este problema incluyen accesos prolongados de extrabajadores, privilegios mal asignados y la imposibilidad de verificar de manera eficiente qué usuarios tienen

acceso a qué recursos dentro de la organización. Esto no solo expone a la empresa a posibles ataques cibernéticos, sino que también genera ineficiencias en la gestión de roles y permisos.

Un sistema de seguridad centrado en la identidad permite mitigar los riesgos asociados al acceso no autorizado mediante la implementación de controles dinámicos y políticas de acceso alineadas con el principio de privilegio mínimo. No obstante, cuando la organización carece de un modelo estructurado de administración de identidades, se presentan dificultades para asegurar la asignación y revocación oportuna de permisos, lo cual incrementa la probabilidad de incidentes relacionados con la fuga de información y ocasiona posibles pérdidas económicas significativas.

Si esta situación persiste sin intervención, la empresa podría enfrentar consecuencias graves tanto en términos de seguridad como de cumplimiento regulatorio. Normativas internacionales como la ISO/IEC 27002:2013 establecen la necesidad de contar con un sistema robusto de gestión de identidades para proteger la información sensible y prevenir accesos indebidos. Rojas (2023), advierte que el incumplimiento de estos estándares no solo exponen a las organizaciones a ciberataques, sino que también puede traducirse en sanciones legales y una pérdida de confianza por parte de clientes y socios estratégicos. Además, la falta de una administración eficiente de identidades afecta la operatividad del negocio, ralentizando la incorporación de nuevos empleados y dificultando la integración de plataformas digitales.

Para abordar esta problemática, es necesario diseñar un modelo de gestión del ciclo de vida de identidades que permita automatizar los procesos de autenticación, asignación de roles y monitoreo de accesos en la empresa del sector retail (Montoya & Restrepo, 2012). La implementación de un modelo basado en mejores prácticas de administración de identidades puede contribuir a mejorar la eficiencia operativa y garantizar el cumplimiento normativo. Camacho (2024), destaca que la adopción de sistemas de identidad bien estructurados reduce significativamente los incidentes de seguridad y optimiza la gestión de permisos en

organizaciones de gran tamaño. En este sentido, el desarrollo de un modelo de aplicación específico para la empresa permitirá evaluar alternativas tecnológicas disponibles en el mercado y seleccionar aquella que mejor se ajuste a sus necesidades operativas y estratégicas.

Pregunta de investigación

¿Cómo impacta la implementación de un modelo de gestión del ciclo de vida de identidades en la seguridad, eficiencia operativa y cumplimiento normativo de una empresa del sector retail?

OBJETIVOS

Objetivo general

Proponer un modelo de gestión del ciclo de vida de identidades para una empresa del sector retail, considerando alternativas tecnológicas disponibles en el mercado y sus implicaciones en seguridad de la información, eficiencia operativa y cumplimiento normativo.

Objetivos específicos

Analizar los beneficios y desafíos asociados a la implementación de un sistema de gestión del ciclo de vida de identidades en la empresa.

Explorar los factores críticos de éxito y las barreras en la adopción de sistemas de administración de identidades en empresas del sector retail.

Evaluar dos sistemas de gestión del ciclo de vida de identidades disponibles en el mercado, comparando su funcionalidad, escalabilidad, costos y compatibilidad con la empresa.

Formular un modelo de gestión del ciclo de vida de identidades adaptado a la empresa objeto de estudio, basado en la evaluación de alternativas.

Validar la viabilidad del modelo propuesto mediante una matriz de valoración que permita determinar su alineación con las necesidades de la empresa.

JUSTIFICACIÓN

El desarrollo de un modelo de gestión del ciclo de vida de identidades en una empresa del sector retail responde a la necesidad de fortalecer la seguridad de la información, optimizar la eficiencia operativa y garantizar el cumplimiento normativo. La conveniencia del estudio radica en que las organizaciones dependen cada vez más de sistemas digitales para la gestión de accesos y permisos, lo que hace imprescindible la implementación de estrategias que minimicen riesgos asociados a accesos indebidos y vulnerabilidades en la infraestructura tecnológica. Según Rodríguez (2023), la gestión de identidades es un componente clave en la seguridad organizacional, ya que permite garantizar que solo los usuarios autorizados accedan a información crítica.

Desde la perspectiva de la relevancia social, la investigación contribuye a la protección de datos sensibles de clientes, empleados y proveedores, fortaleciendo la confianza en la organización y reduciendo los riesgos de fraude o manipulación de información. El sector retail maneja grandes volúmenes de transacciones y datos personales, lo que lo convierte en un objetivo frecuente de ciberataques y accesos no autorizados. Flores (2023), señala que la adopción de modelos de administración de identidades mejora la seguridad de los datos en entornos empresariales, reduciendo incidentes de filtración de información y garantizando la transparencia en la gestión de accesos. Por ello, este estudio no solo beneficia a la empresa analizada, sino que también puede servir como referencia para otras organizaciones del sector que enfrentan problemáticas similares en el manejo de identidades digitales.

En cuanto a sus implicaciones prácticas, la investigación permite evaluar alternativas tecnológicas viables que pueden optimizar la administración del ciclo de vida de identidades en la organización. La falta de un sistema adecuado genera costos operativos elevados, errores en la asignación de permisos y dificultades en auditorías de seguridad. El Ministerio de Tecnologías de la Información y las Comunicaciones [MinTic] (2021), enfatiza que los sistemas de gestión de

identidades reducen la carga administrativa de los departamentos de TI y mejoran la capacidad de respuesta ante incidentes. Al desarrollar un modelo basado en las mejores prácticas y herramientas disponibles en el mercado, se proporcionará a la empresa una solución adaptable y escalable que permita mejorar la eficiencia en la gestión de accesos y credenciales.

Desde el valor teórico, este estudio enriquece el conocimiento sobre la administración de identidades al enfocarse en su aplicación concreta dentro del sector retail, un entorno caracterizado por una alta rotación de personal y la coexistencia de Múltiples plataformas digitales. Si bien la literatura académica existente ha abordado la gestión de identidades en marcos organizacionales generales, son escasos los trabajos que profundizan en las necesidades específicas de este sector, donde la agilidad operativa y el control de accesos revisten una importancia crítica. En este sentido, Montoya y Restrepo (2012) subrayan que: la gestión de identidades y control de acceso desde una perspectiva organizacional debe considerar el entorno específico y la estructura operativa de la organización para garantizar su efectividad (p. 26). Esta afirmación sustenta la pertinencia de la presente investigación, al abordar una problemática particular que demanda soluciones adaptadas al contexto dinámico del retail. Yopan et al., (2020), destaca que la crisis de identidad organizacional puede afectar la continuidad del negocio y generar pérdidas económicas. En este sentido, el estudio contribuirá a la identificación de factores clave que deben considerarse al diseñar e implementar un sistema de gestión de identidades en entornos empresariales dinámicos.

Finalmente, la utilidad metodológica del estudio radica en la aplicación de un enfoque basado en el análisis comparativo de alternativas tecnológicas, lo que permitirá generar un modelo adaptable a diferentes contextos organizacionales. La validación del modelo propuesto mediante una matriz de valoración garantizará que su diseño se ajuste a las necesidades específicas de la empresa, proporcionando criterios objetivos para la selección de herramientas de administración de identidades. De acuerdo con Quecedo y Castaño (2002), la evaluación de

soluciones de identidad en función de su escalabilidad, costo y compatibilidad facilita la toma de decisiones estratégicas en las organizaciones. En este sentido, la investigación se enmarca en el campo de Ciencia, Tecnología e Innovación, dentro del grupo de investigación Tecnológico Ontare, y alineada con la línea de Tecnología de la Información y Comunicaciones, asegurando su pertinencia institucional y académica.

MARCO TEÓRICO

Estado del Arte

El Estado del Arte permite analizar investigaciones previas relacionadas con la gestión de información, seguridad organizacional y planificación estratégica, identificando modelos aplicables a la administración del ciclo de vida de identidades en el sector retail. A continuación, se presentan estudios que aportan al fundamento del presente trabajo.

Brochero (2019), desarrolló una metodología de gestión de información para el sector retail basada en Business Intelligence (BI), con el objetivo de mejorar la toma de decisiones y la gestión del conocimiento en estas organizaciones. A través del diseño de un data warehouse, un cuadro de mando integral y estrategias de administración de datos se evidencia que las empresas que hacen parte del sector retail, las cuales utilizan tecnologías accesibles como redes sociales y comercio electrónico, pero carecen de una gestión estructurada de información, lo que limita la optimización de sus procesos. Aunque el concepto de Inteligencia de Negocios (Business Intelligence, BI) no es ampliamente conocido en el sector MIPYME, las empresas expresan interés en su adopción siempre que las herramientas se adaptan a sus capacidades y requerimientos operativos. Este hallazgo, reportado por Brochero (2019), evidencia que muchas organizaciones carecen de estrategias estructuradas de gestión de información, lo cual limita la eficiencia en sus procesos decisionales. En consecuencia, se hace necesario formular estrategias alineadas con la realidad organizacional de cada empresa, particularmente en aquellas del sector retail que presentan alta rotación de personal y múltiples plataformas digitales. Este enfoque resulta crucial para evaluar alternativas tecnológicas orientadas a fortalecer la seguridad de la información y la administración efectiva del ciclo de vida de identidades (Brochero, 2019).

Flórez (2019), llevó a cabo un estudio con el objetivo de implementar un sistema de digitalización de documentos en la empresa ENTER SAC, alineado con el cumplimiento del

Decreto Legislativo 1310 y la Resolución de Secretaría de Gobierno Digital N° 001-2017PCM/SEGD. A través del diseño de un Programa de Gestión Documental, se establecen lineamientos para la organización de archivos de gestión, resaltando la importancia de los documentos como elementos probatorios en la administración pública y privada. Los resultados demostraron que la digitalización documental mejora los tiempos de respuesta, optimiza los procesos internos y garantiza la trazabilidad de la información dentro de las organizaciones, además de contribuir con la sostenibilidad ambiental. Esta investigación aporta al presente estudio al evidenciar cómo la implementación de modelos de gestión de información permite optimizar la administración de datos sensibles, lo que guarda relación con la necesidad de un sistema estructurado de gestión del ciclo de vida de identidades, asegurando mayor control sobre el acceso y la seguridad de la información en el sector retail.

Momblanc y Castro (2020), realizaron un estudio con el objetivo de explorar la relación entre la gestión documental y el control interno, determinando que una administración eficiente de la documentación influye directamente en el cumplimiento de los objetivos estratégicos de una organización, la transparencia administrativa y la toma de decisiones basadas en información confiable. Los resultados del análisis evidenciaron que el adecuado manejo de documentos archivísticos, especialmente aquellos con valor probatorio, es esencial para garantizar la rendición de cuentas y la seguridad de la información, así como para mitigar riesgos relacionados con la administración de datos estratégicos o confidenciales. Esta investigación destaca la importancia de implementar sistemas de control estructurados para la gestión de información, lo que se relaciona con la necesidad de un modelo de gestión del ciclo de vida de identidades, permitiendo optimizar la administración de accesos y fortalecer la seguridad en entornos organizacionales complejos.

Minchalo (2022) tuvo como objetivo diseñar un modelo de gestión para mejorar el posicionamiento de la marca RADI en el sector retail mediante la aplicación de estrategias de

branding, con el propósito de fortalecer la identidad corporativa y generar un impacto positivo en la percepción de los consumidores. La investigación se llevó a cabo en la ciudad de Cuenca en 2022, utilizando un enfoque mixto, descriptivo y de diseño no experimental, con una muestra de 386 personas seleccionadas mediante muestreo estratificado por conveniencia. Entre los principales resultados, se identificó que la gestión estratégica del branding incide significativamente en la percepción y fidelización de los clientes, lo que permitió desarrollar una propuesta basada en estrategias de posicionamiento de marca adaptadas a la cadena retail RADI. Esta investigación estructura modelos de gestión adaptados a las necesidades del sector retail, resaltando cómo la implementación de metodologías especializadas puede optimizar procesos y generar valor empresarial. Así como el branding fortalece la identidad corporativa y mejora la percepción del consumidor, un modelo de gestión del ciclo de vida de identidades permite mejorar la seguridad, la eficiencia operativa y el cumplimiento normativo dentro de las organizaciones, asegurando una administración de accesos más eficiente y confiable.

León et al. (2022) desarrollaron un proyecto de consultoría con el objetivo de introducir y aplicar la planificación estratégica en una empresa del sector inmobiliario en una ciudad intermedia, brindando acompañamiento en la construcción de un plan de desarrollo organizacional. A lo largo del proceso, se evidencia que la mayoría de las herramientas para el análisis interno y externo de la compañía eran desconocidas para los directivos, sin embargo, mediante un proceso de pedagogía se logró generar conciencia sobre la importancia de la planificación para la toma de decisiones estratégicas. Como resultado, se diseñó un documento guía que servirá como referencia para futuras inversiones y adaptaciones a los cambios del entorno competitivo. Así como la planificación estratégica permite mejorar la dirección y sostenibilidad de una empresa, la gestión del ciclo de vida de identidades contribuye a la seguridad y eficiencia operativa al establecer un control estructurado sobre los accesos a los sistemas organizacionales.

Barajas (2023) tuvo como objetivo diagnosticar y proponer acciones correctivas para optimizar el sistema de gestión documental en la empresa MIRS LATINOAMÉRICA SAS, con el propósito de garantizar la disponibilidad, seguridad y trazabilidad de la información en la ejecución de proyectos de interventoría de malla vial y espacio público. A través de un proceso de consultoría, se identifican deficiencias en la administración documental interna de la empresa, lo que representaba riesgos legales y operacionales. Entre los principales hallazgos, se evidencia la necesidad de estructurar un sistema de gestión documental que permita el acceso ágil y seguro a la información, cumpliendo con normativas legales y optimizando la productividad organizacional. Asimismo, se resaltó la importancia de la gestión documental electrónica para mejorar la sostenibilidad y reducir la dependencia de documentos físicos. Del mismo modo que la gestión documental garantiza la integridad y trazabilidad de la información, un modelo de gestión de identidades permite gestionar de manera segura y eficiente los accesos a los sistemas empresariales, minimizando riesgos y fortaleciendo la seguridad organizacional.

Las investigaciones revisadas demuestran la importancia de estructurar modelos de gestión para optimizar la administración de la información, mejorar la seguridad organizacional y fortalecer la eficiencia operativa en distintos sectores. La digitalización documental, la planificación estratégica y el uso de tecnologías avanzadas destacan como herramientas clave para la gestión eficiente de datos y accesos. En este contexto, el presente estudio se nutre de estos hallazgos para diseñar un modelo de gestión del ciclo de vida de identidades, asegurando un enfoque integral que responda a las necesidades del sector retail en términos de seguridad, eficiencia y cumplimiento normativo.

Marco Conceptual

La gestión del ciclo de vida de identidades (Identity Lifecycle Management - ILM) es un componente fundamental dentro de la administración de accesos en las organizaciones,

garantizando que los usuarios autorizados cuenten con los permisos adecuados para desempeñar sus funciones sin comprometer la seguridad de la información. De acuerdo con Altamirano (2019), un sistema ILM bien estructurado permite centralizar el control de accesos, optimizando la eficiencia operativa y mitigando riesgos de seguridad. En este sentido, el presente estudio se basa en teorías y modelos aplicados a la gestión de identidades, la seguridad de la información y el cumplimiento normativo en entornos empresariales, con un enfoque particular en el sector retail.

Teorías sobre gestión de identidades y accesos

Uno de los marcos teóricos más relevantes en la administración de identidades es la Teoría de Control de Accesos Basados en Roles (RBAC, por sus siglas en inglés), propuesta por (Ferraiolo & Kuhn, 1992). Esta teoría establece que los permisos dentro de un sistema deben asignarse según el rol que desempeña cada usuario en la organización, reduciendo la complejidad de la administración manual de accesorios. Sandhu et al. (1996) ampliaron este modelo incorporando principios de segregación de funciones, lo que permite evitar conflictos de intereses y accesos indebidos. (Role-Based Access Control Models, 1996).

Por otro lado, el modelo Control de acceso basado en atributos (ABAC), introducen un enfoque más flexible, donde los permisos no solo dependen de los roles, sino de atributos específicos del usuario, como ubicación, dispositivo utilizado o nivel de seguridad requerido. Este modelo es altamente adaptable a entornos dinámicos como el sector retail, donde las responsabilidades de los empleados pueden cambiar con frecuencia (Microsoft, 2024).

Además, la Teoría del Principio del Mínimo Privilegio, formulada por Saltzer y Schroeder (1974), establece que cada usuario debe tener solo los permisos estrictamente necesarios para realizar sus tareas. Esta teoría es esencial para reducir la superficie de ataque en sistemas de información y evitar accesos no autorizados a datos críticos.

Modelos de gestión del ciclo de vida de identidades

El modelo de Gestión del Ciclo de Vida de Identidades (ILM) propuesto por O'Neill (2018) establece que el ciclo de una identidad digital dentro de una organización atraviesa diversas fases: creación, asignación de permisos, monitoreo, modificación y eliminación. Este modelo enfatiza la necesidad de implementar sistemas automatizados que permitan una administración eficiente de identidades, reduciendo errores humanos y garantizando la trazabilidad de accesos (O'Neill, 2018).

Por otro lado, el modelo de Gestión de Identidades y Accesos (IAM) de NIST (National Institute of Standards and Technology, 2020) define tres pilares fundamentales para la administración segura de identidades: autenticación, autorización y auditoría. Este enfoque permite garantizar que los usuarios sean correctamente identificados antes de concederles acceso a sistemas empresariales y que cada acción realizada sea registrada para futuras auditorías (IBM, 2024).

La gestión del ciclo de vida de identidades está directamente relacionada con la seguridad de la información, ya que un acceso inadecuado a sistemas puede comprometer la integridad, confidencialidad y disponibilidad de los datos. Según Whitman y Mattord (2018), los incidentes de seguridad suelen estar asociados a errores en la administración de credenciales y permisos, lo que subraya la necesidad de implementar controles robustos en la gestión de identidades.

En este sentido, la aplicación de la Teoría de la Defensa en Profundidad, formulada por Stallings (2019), establece que los sistemas de seguridad deben contar con múltiples capas de protección, incluyendo autenticación multifactorial, monitoreo continuo y restricciones de acceso basadas en riesgos. Estas estrategias permiten minimizar los impactos de accesos no autorizados dentro de la organización (Universidad Pontificia Comillas, 2023).

El cumplimiento normativo es un eje central en la administración de identidades, ya que las organizaciones deben garantizar que el acceso a la información cumpla con las regulaciones

internacionales. La norma (ISO/IEC 27001, 2022), establece los principios de seguridad de la información que deben adoptarse en empresas para proteger sus activos digitales. De acuerdo con la NTC-ISO 9001 (2015), la implementación de estándares ISO en la gestión de identidades reduce la exposición a riesgos legales y operacionales.

En el ámbito europeo, la directiva NIS2 (Network and Information SecurityDirectiva 2, 2022) obliga a las empresas a fortalecer sus controles de ciberseguridad, incluyendo la adopción de sistemas de gestión de identidades robustos para prevenir ataques informáticos. En América Latina, la normativa de protección de datos personales en países como Colombia y México exige la implementación de medidas de seguridad que garantizan el control de accesos a la información empresarial (NIS2, 2022).

Impacto de la gestión de identidades en la eficiencia operativa

La administración eficiente del ciclo de vida de identidades también tiene un impacto significativo en la productividad empresarial. Según SINFOPAC (2024), la implementación de un sistema automatizado de gestión de identidades permite reducir hasta un 30 % el tiempo dedicado a la asignación y revocación de permisos en empresas con alta rotación de personal.

Asimismo, el uso de inteligencia artificial en la gestión de identidades, como lo plantea Hacking (2024), facilita la detección de accesos anómalos en tiempo real, permitiendo una respuesta inmediata ante incidentes de seguridad. Este enfoque es clave en el sector retail, donde las empresas manejan grandes volúmenes de datos y requieren soluciones escalables para gestionar identidades digitales.

El análisis de las teorías y modelos revisados demuestra que la gestión del ciclo de vida de identidades es un componente crítico en la seguridad y eficiencia operativa de las organizaciones. La adopción de enfoques como RBAC, ABAC y Zero Trust Security, junto con la aplicación de estándares normativos como ISO/IEC 27001 y NIS2, permite establecer sistemas de gestión de identidades más seguros y confiables. Este marco teórico servirá como base para

el desarrollo del modelo propuesto en la investigación, asegurando su alineación con las necesidades del sector retail y garantizando una administración eficiente de accesos en entornos digitales complejos (Gaítan, 2022).

Marco institucional

La empresa objeto de estudio es una compañía del sector retail ubicada en la ciudad de Bogotá, Colombia, cuya actividad económica se encuentra clasificada bajo el Código CIIU 4663, correspondiente a “Comercio al por mayor de materiales de construcción, artículos de ferretería, pinturas, productos de vidrio, equipo y materiales de fontanería y calefacción”. Esta organización se dedica a la comercialización de productos de consumo masivo, con presencia en múltiples puntos de venta y una infraestructura tecnológica que respalda sus operaciones en diversas plataformas digitales.

Dentro de su estructura organizacional, la empresa cuenta con diversas áreas funcionales, entre las que destacan: operaciones, tecnología de la información, recursos humanos, finanzas, mercadeo y logística. Debido al crecimiento exponencial de su fuerza laboral y la integración de múltiples sistemas de información, la gestión de identidades y accesos ha cobrado especial relevancia. La compañía opera con una alta rotación de personal, lo que genera desafíos en la administración de credenciales y permisos dentro de los sistemas corporativos.

Los principales productos y procesos de la empresa incluyen la venta de productos de consumo, la administración de inventarios, la gestión de proveedores y la atención al cliente en diversos canales de comercialización. Dada la naturaleza de su operación, la seguridad de la información se convierte en un factor clave para evitar accesos indebidos, fraudes internos y vulnerabilidades a la privacidad de los datos.

En términos de gestión tecnológica, la organización ha adoptado múltiples plataformas para la administración de transacciones, gestión de clientes y control de inventarios. No obstante,

la ausencia de un sistema centralizado para la gestión del ciclo de vida de identidades ha ocasionado inconsistencias en la asignación y revocación de permisos, generando riesgos operativos y problemas de cumplimiento normativo.

El presente estudio se enfoca en diseñar un modelo de gestión del ciclo de vida de identidades que responda a las necesidades específicas de la empresa, garantizando un equilibrio entre seguridad, eficiencia operativa y cumplimiento normativo. Este modelo permitirá establecer mecanismos automatizados para la administración de accesos, minimizando errores humanos y optimizando los procesos de autenticación y autorización dentro de la organización.

La implementación de este modelo contribuirá a fortalecer la seguridad de la información, mejorar la trazabilidad en la gestión de accesorios y reducir la carga administrativa del área de tecnología. Asimismo, se alineará con las mejores prácticas del sector, asegurando que la empresa adopte estándares internacionales en la protección de datos y la administración de identidades digitales.

METODOLOGÍA

Enfoque, alcance y diseño de la investigación

Enfoque de la investigación

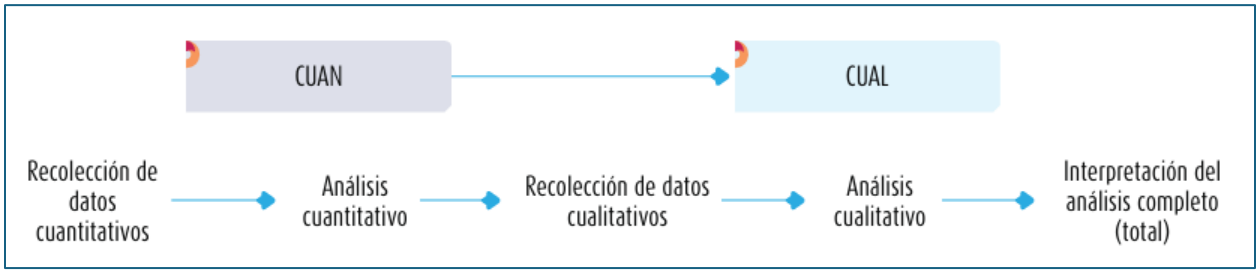
El estudio adopta un enfoque mixto, el cual combina elementos cuantitativos y cualitativos con el propósito de enriquecer la comprensión del fenómeno analizado. Desde la perspectiva cuantitativa, se busca medir la eficiencia, seguridad y cumplimiento normativo de dos alternativas tecnológicas para la gestión del ciclo de vida de identidades en una empresa del sector retail. Este componente permitirá analizar datos numéricos mediante técnicas estadísticas que facilitarán la comparación objetiva entre las soluciones propuestas. En paralelo, el enfoque cualitativo aportará profundidad y contexto a través de cuestionario de preguntas abiertas, capturando la percepción del personal respecto a la experiencia de uso, los desafíos operativos y la aceptación organizacional del modelo propuesto.

Según Hernández-Sampieri et al. (2014), el enfoque mixto permite una integración metodológica que proporciona una visión más completa del objeto de estudio, superando las limitaciones propias de una sola perspectiva. Este tipo de enfoque es especialmente útil cuando se aborda un problema complejo que implica dimensiones técnicas, organizacionales y humanas, como ocurre en la administración del ciclo de vida de identidades. Asimismo, el enfoque mixto contribuye a formular con mayor claridad el planteamiento del problema, producir datos más ricos y variados, y apoyar con mayor solidez las inferencias científicas.

Además, el estudio opta por un diseño de integración secuencial, en el cual los resultados del análisis cualitativo complementan los resultados obtenidos en la fase cuantitativa. Esta secuencia permite fundamentar la propuesta del modelo de gestión con base en evidencia empírica contextualizada, facilitando la toma de decisiones en escenarios reales. De acuerdo con la clasificación tipológica de los métodos mixtos, esta investigación se enmarca en un diseño explicativo secuencial (DEXPLIS), donde los datos cuantitativos son recogidos y analizados en

primera instancia, seguidos de la fase cualitativa para explicar o interpretar con mayor profundidad los resultados obtenidos (Hernández-Sampieri et al., 2014, p. 18).

Figura. 1 *Esquema del diseño explicativo secuencial (DEXPLIS).*



Fuente. Tomado de (Hernández-Sampieri et al., 2014, p. 554).

Alcance de la investigación

El alcance del estudio se caracteriza por ser descriptivo y correlacional. En primer lugar, se realiza una caracterización detallada de los procesos actuales de gestión de identidades en la organización, lo cual permite describir las prácticas, herramientas y dificultades existentes en este campo. Esta etapa facilita comprender cómo se llevan a cabo la creación, modificación y revocación de accesorios, así como identificar los puntos críticos que afectan la seguridad y la eficiencia operativa.

Por otra parte, el componente correlacional se evidencia en la comparación de variables técnicas y estratégicas entre las alternativas tecnológicas seleccionadas. Como señala Hernández-Sampieri et al. (2014), este tipo de estudio busca establecer relaciones entre variables en un momento dado, sin pretender explicar causas, pero permitiendo observar asociaciones significativas entre criterios como funcionalidad, escalabilidad y compatibilidad con sistemas existentes. El estudio no pretende manipular las variables, sino analizar su comportamiento y relación en el contexto organizacional específico.

Diseño de la investigación

El diseño metodológico adoptado es de tipo no experimental, con carácter transversal y alcance aplicado. Se trata de un estudio donde no se manipulan deliberadamente las variables, sino que se observan en su contexto natural. Según Hernández-Sampieri et al. (2014), la investigación no experimental se justifica cuando se desea describir y analizar fenómenos tal como ocurren, sin intervención directa del investigador en la configuración de los datos.

Este diseño es además transversal, ya que la recolección de datos se realizará en un único momento del tiempo, permitiendo capturar una “fotografía” de la situación actual del sistema de gestión de identidades y su evaluación con respecto a las soluciones tecnológicas disponibles. Esta temporalidad permite reducir costos y facilitar el análisis de las percepciones de los participantes, así como la comparación entre sistemas bajo condiciones similares.

Finalmente, el diseño se clasifica como aplicado, dado que su propósito no es únicamente teórico, sino que busca generar un modelo de gestión adaptable que responda a las necesidades específicas de una empresa del sector retail. Como lo indican Hernández-Sampieri et al. (2014), este tipo de diseño se orienta a intervenir en la realidad organizacional mediante propuestas concretas, lo que resulta coherente con los objetivos de esta investigación, centrados en la evaluación y formulación de alternativas viables para la administración del ciclo de vida de identidades.

Definición de variables

En toda investigación aplicada que aspire a generar conocimiento útil y contextualizado para la toma de decisiones, la definición de variables cumple un papel esencial, ya que permite precisar qué dimensiones del fenómeno se observarán, medidas y analizadas a lo largo del estudio. Tal como lo indican Hernández-Sampieri et al. (2014), una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse. En el presente estudio, las variables se centran en aspectos técnicos, organizacionales y normativos vinculados

con la gestión del ciclo de vida de identidades digitales dentro del sector retail. Estas variables están interrelacionadas, por lo que su análisis se desarrollará bajo un enfoque de interdependencia, sin establecer relaciones de causa y efecto propias de estudios experimentales.

Dado que se trata de un diseño no experimental y de carácter aplicado, la operacionalización de las variables se enfocará en describir sus dimensiones clave, identificar indicadores medibles y establecer métodos de recolección que permitan analizar su comportamiento en el entorno organizacional. En coherencia con la metodología propuesta, se establecerán definiciones conceptuales basadas en literatura científica especializada, así como definiciones operacionales que guíen el uso de instrumentos de medición como cuestionario, fichas comparativas y matrices de valoración.

Definición conceptual

La definición conceptual de las variables seleccionadas parte de teorías reconocidas en los campos de la ciberseguridad, la gestión organizacional y la normativa sobre protección de datos. Cada variable se ha delimitado en función de su pertinencia para los objetivos del estudio, de manera que permitan evaluar tanto los beneficios esperados como los desafíos operativos derivados de la implementación de un modelo de gestión de identidades en la empresa analizada. Hernández-Sampieri et al. (2014) recomiendan definir claramente los conceptos a estudiar, ya que esto facilita la formulación de preguntas, la construcción de instrumentos y el análisis de resultados.

Definición operacional

La definición operacional de las variables establece los criterios específicos que permitirán su medición o evaluación a partir de instrumentos diseñados para este estudio. En este caso, se utilizarán cuestionario de preguntas abiertas dirigidas a personal clave de la organización, análisis documental de las soluciones tecnológicas seleccionadas y una matriz de valoración que

ponderará criterios estratégicos y técnicos. La operacionalización también contempla la validación del modelo propuesto mediante criterios como trazabilidad, automatización, compatibilidad y alineación con estándares internacionales como ISO/IEC 27001 y NIS2.

A continuación, se presentan las variables con sus respectivas definiciones conceptuales, operacionales y dimensiones clave:

Tabla 1 *Definición conceptual y operativa de las variables del estudio sobre gestión del ciclo de vida de identidades en el sector retail*

Variable	Definición conceptual	Definición operacional	Dimensiones
Ciclo de vida de identidades	Conjunto de procesos que controlan la creación, modificación, monitoreo y eliminación de credenciales y permisos de usuarios en sistemas digitales.	Evaluación de procesos actuales mediante ficha comparativa, con énfasis en automatización, trazabilidad y asignación de roles.	Automatización, trazabilidad, asignación de roles
Seguridad de la información	Estado en el cual la información se encuentra protegida frente a accesos no autorizados, alteración, destrucción o divulgación no consentida.	Identificación de brechas de seguridad existentes y prácticas actuales de protección de datos, evaluadas con base en entrevistas y documentación técnica.	Confidencialidad, integridad, disponibilidad
Eficiencia operativa	Capacidad de una organización para ejecutar procesos internos optimizando el uso de recursos, tiempo y esfuerzo.	Medición de carga operativa, tiempos de respuesta y frecuencia de errores en los procesos actuales de gestión de identidades.	Reducción de errores, agilidad, simplificación
Cumplimiento normativo	Grado en que las prácticas organizacionales se ajustan a normas legales y estándares técnicos nacionales o internacionales sobre seguridad y privacidad.	Revisión de políticas internas, auditorías existentes y alineación con estándares como ISO/IEC 27001 y NIS2.	Auditoría, controles técnicos, políticas organizacionales
Usuario	Individuo que interactúa con los sistemas informáticos mediante credenciales asignadas, cuya conducta incide en el control de accesos y la seguridad digital.	Análisis de comportamientos y patrones de uso mediante entrevistas semiestructuradas, con énfasis en el rol del usuario en el inicio y cierre del ciclo de acceso.	Conducta de acceso, hábitos de autenticación, cumplimiento de políticas

Fuente. Elaboración propia a partir de Hernández-Sampieri et al. (2014).

Población y muestra

La población objeto de estudio está constituida por los colaboradores pertenecientes a las áreas de tecnología, recursos humanos y seguridad de la información de una empresa del sector retail localizada en la ciudad de Bogotá, Colombia. Estos profesionales desempeñan funciones estratégicas relacionadas con la gestión de accesos, la administración de credenciales digitales y el cumplimiento de normativas de seguridad de la información.

Dado que la población es reducida y corresponde a un grupo especializado de actores clave en el ciclo de vida de las identidades digitales, se ha optado por aplicar un muestreo por conveniencia, específicamente a través de un censo dirigido. Este método permite trabajar con la totalidad de los individuos directamente involucrados en los procesos objeto de análisis, lo que facilita una recolección de datos exhaustiva y alineada con los objetivos específicos del estudio.

Se estima que la muestra estará compuesta por un grupo de entre 10 y 15 participantes, cuya selección se fundamenta en su nivel de responsabilidad, experiencia directa con sistemas de gestión de identidades y conocimiento sobre las normativas de seguridad de la información vigentes. Esta estrategia asegura la pertinencia de los datos obtenidos y contribuye a una caracterización precisa de la situación actual, así como a la evaluación fundamentada del modelo propuesto.

La población está conformada por miembros del área de tecnología, recursos humanos y seguridad de la información de una empresa del sector retail en Bogotá, quienes participan activamente en la gestión de identidades digitales. Debido a su reducido tamaño y naturaleza especializada, se emplea un muestreo por conveniencia mediante censo, lo cual permite abordar a todos los sujetos clave sin recurrir a técnicas probabilísticas, dado que “en poblaciones pequeñas resulta más eficaz trabajar con su totalidad” (Hernández-Sampieri et al., 2014, p. 176).

Selección de métodos e instrumentos para la recolección de información

En concordancia con el enfoque descriptivo aplicado en esta investigación, la selección de métodos e instrumentos debe responder a criterios de pertinencia, validez y coherencia con los objetivos formulados y las variables definidas. Tal como lo indica Hernández-Sampieri et al. (2014), la adecuación de los instrumentos a las características del estudio garantiza la calidad de los datos obtenidos, así como la posibilidad de interpretar con rigor los hallazgos. En este sentido, se optará por instrumentos que permitan captar tanto aspectos cualitativos como cuantitativos, brindando una visión comprensiva de la problemática.

Para la recolección de datos primarios se emplearán tres instrumentos principales. En primer lugar, cuestionario de preguntas abiertas dirigidas a personal clave de las áreas de tecnología y seguridad de la información. Este cuestionario busca explorar, desde una perspectiva experiencial, los procesos actuales de gestión de identidades, las dificultades enfrentadas, las necesidades operativas y los criterios valorados en la adopción de soluciones tecnológicas.

En segundo lugar, se diseñará una ficha de análisis comparativo que permitirá evaluar de forma sistemática dos sistemas tecnológicos de gestión del ciclo de vida de identidades. Esta herramienta considera criterios como funcionalidad, escalabilidad, costos, compatibilidad, soporte y cumplimiento normativo, facilitando una evaluación técnica alineada con el contexto organizacional del sector retail.

Finalmente, se construirá una matriz de valoración con ponderaciones estratégicas y operativas para validar el modelo propuesto. Esta matriz integrará criterios como alineación con necesidades, grado de automatización, facilidad de implementación, sostenibilidad y aceptación interna. La triangulación entre estos instrumentos permitirá robustecer el análisis y garantizar la pertinencia de las recomendaciones.

Con base en lo anterior, los instrumentos se han diseñado a partir de referentes metodológicos y necesidades concretas de la organización, asegurando su funcionalidad en la medición de las

variables definidas. Todos los instrumentos se anexarán al final del documento para su consulta y validación.

Técnicas de análisis de datos

Según Hernández-Sampieri et al., (2014), el análisis de los datos constituye una etapa clave en la investigación científica, pues permite transformar la información recolectada en conocimiento empírico verificable.

En este estudio, que se enmarca en un enfoque mixto de carácter predominantemente cualitativo con componentes descriptivos, se combinarán diversas técnicas analíticas. Para los datos cualitativos derivados del cuestionario de preguntas abiertas, se empleará el análisis temático, técnica que permite identificar patrones, categorías y significados recurrentes en los discursos de los participantes. Esta técnica facilita una comprensión profunda de las percepciones y experiencias del personal respecto a la gestión del ciclo de vida de identidades y los sistemas tecnológicos asociados.

Por otra parte, la información recolectada mediante la ficha comparativa de soluciones tecnológicas se someterá a un análisis documental estructurado, el cual permitirá valorar objetivamente las características funcionales, técnicas y operativas de cada sistema. Este análisis se orientará a determinar ventajas, limitaciones y niveles de ajuste a las necesidades de la empresa.

Finalmente, los datos provenientes de la matriz de valoración serán analizados mediante estadística descriptiva, calculando ponderaciones promedio y determinando la viabilidad del modelo propuesto con base en la sumatoria de los valores ponderados por criterio. Este proceso permitirá una evaluación cuantitativa de la adecuación del modelo a los requerimientos técnicos, estratégicos y operativos de la organización.

Para mayor claridad metodológica, la siguiente tabla sintetiza los instrumentos aplicados, las técnicas de análisis asociadas y su respectiva finalidad:

Tabla 2 *Técnicas de análisis aplicadas a los instrumentos de recolección de información*

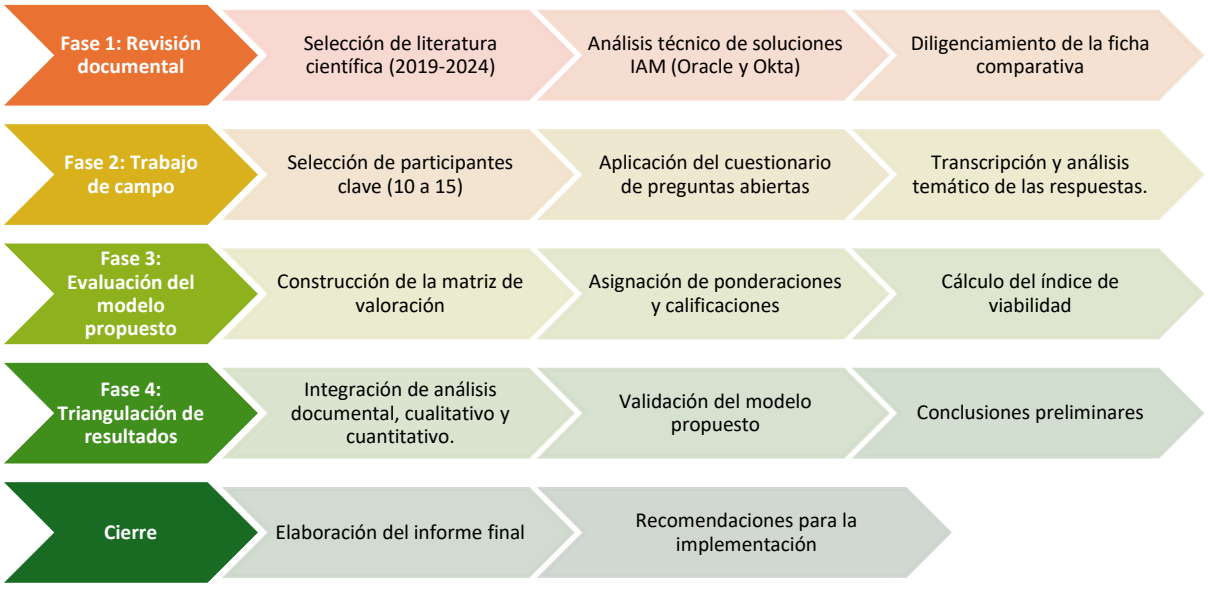
Instrumento	Técnica de análisis	Finalidad metodológica
Cuestionario de preguntas abiertas	Análisis temático	Identificar patrones discursivos, necesidades, desafíos y percepciones del equipo.
Ficha comparativa de soluciones	Análisis documental estructurado	Comparar funcionalidades y criterios técnicos de los sistemas seleccionados.
Matriz de valoración del modelo	Estadística descriptiva	Determinar la viabilidad del modelo según criterios cuantitativos definidos.

Fuente. Elaboración propia con base en Hernández-Sampieri et al. (2014).

Procedimiento de la investigación

El desarrollo metodológico de este estudio se estructura en una secuencia de fases que responden al enfoque mixto adoptado, el cual integra elementos cuantitativos y cualitativos con el propósito de fortalecer la comprensión integral del fenómeno. En coherencia con el diseño explicativo secuencial (DEXPLIS), propuesto por Hernández-Sampieri et al. (2014), primero se ejecutará la recolección y análisis de los datos cuantitativos y, posteriormente, se complementará con información cualitativa que permita interpretar y contextualizar los hallazgos.

Figura. 2 *Procedimiento de la Investigación.*



Fuente. Elaboración propia.

ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

A continuación, se desarrolla cada uno de los objetivos específicos propuestos:

Beneficios y desafíos asociados a la implementación de un sistema de gestión del ciclo de vida de identidades en la empresa.

Se realizo la encuesta a diez colaboradores de los equipos de tecnología, ciberseguridad y gestión de accesos. El cuestionario, compuesto por once preguntas abiertas agrupadas en cuatro bloques gestión actual de identidades, percepción de riesgos y eficiencia, cumplimiento normativo e interés en soluciones tecnológicas, permitió obtener testimonios sobre las prácticas actuales, los obstáculos más frecuentes y las expectativas del equipo ante una posible automatización. A partir de estas conversaciones, se elaboró un análisis cualitativo que vincula las opiniones recolectadas con las variables de estudio, de modo que se identifiquen tanto los patrones compartidos como las diferencias significativas.

A continuación, se presentan los datos esenciales de los diez profesionales que participaron en las entrevistas semiestructuradas. Esta información facilita la comprensión de su perfil laboral, antigüedad en la organización y tiempo dedicado a cada sesión, aspectos que enriquecen el análisis cualitativo de sus aportes.

Tabla 3 *Perfil de los colaboradores entrevistados.*

Nombre	Cargo	Antigüedad
Anónimo	Analista de gestión de accesos	2 años
William F. Zorro Salamanca	Analista de Gestión de Identidades y Accesos	4 años
Óscar A. López Díaz	Analista de Gestión de Identidades	6 años
Juan N. Riaño Erazo	Analista de Ciberseguridad	8 meses
Kevin A. Ortiz Villa	Técnico en Gestión de Acceso	2 años
Julieth L. Correa	Analista de Gestión de Identidades	7 años
Duvar A. Cuéllar Caicedo	Analista de Ciberseguridad	2 años
Dixon F. Murillo Montoya	Coordinador de Gestión de Identidades	31 años
Delcy García Rojas	Analista de Ciberseguridad	29 años
Carlos A. D. Ovalle	Técnico en Gestión de Identidades	1 año

Fuente: Elaboración propia a partir del cuestionario realizadas.

La figura 1, muestra a través de una nube de palabras, los términos y conceptos que más se repitieron en las diez encuestas de preguntas abiertas, lo que nos permite visualizar de un vistazo los temas que preocupan y ocupan al personal en su trabajo diario.

Figura 1 *Nube de palabras de los términos más frecuentes en las entrevistas semiestructuradas.*

Nota. Elaboración propia a partir de las transcripciones de entrevistas semiestructuradas, Universidad EAN – abril de 2025. Fuente: Tomado de Atlas. Ti.

Estos resultados refuerzan la idea de que el modelo a proponer debe centrarse en ofrecer una gestión de identidades altamente automatizada y trazable, que reduzca errores humanos, mejore la seguridad y la eficiencia operativa, y facilite el cumplimiento normativo.

La Tabla 4, clasifica las opiniones de los encuestaos según las cuatro variables de estudio y sus dimensiones. Por ejemplo, en Ciclo de vida de identidades, se evidencia el deseo de automatización y trazabilidad, así como procesos manuales de asignación masiva de accesos.

En Seguridad de la información, se visualizó preocupación tanto por la confidencialidad (accesos no retirados, fugas internas) como por mecanismos de auditoría y logs que intentan paliar esos riesgos.

Tabla 4 *Resumen de respuestas agrupadas por variable y dimensión.*

Variable	Dimensión	Respuesta extraída de la encuesta
Ciclo de vida de identidades	Automatización	"La idea es poder tener un gestor que nos ayuden a automatizar la asignación de los accesos y no tener tanta intervención manual." (William F. Zorro) "Debe ser un aplicativo con la capacidad de integrarse con múltiples soluciones…" (Óscar A. López)
	Trazabilidad	"Trazabilidad, gobierno y funcionalidad." (Anonimo) "Auditoría, lineamientos de seguridad y trazabilidad de acciones realizadas…" (Juan N. Riaño)
	Asignación y revocación de accesos	"Actualmente la creación de usuario se realiza por medio del CMD por scripts de forma masiva, y de igual forma con la eliminación…" (Kevin A. Ortiz) "Se valida con el área de Gestión Humana el archivo de ingresos, retiros y ausentismos…" (Óscar A. López)
Seguridad de la información	Confidencialidad	"Problemas de disponibilidad y confidencialidad ya que puede haber accesos en aplicaciones que no se retiraron…" (W. Zorro) "Posible fuga de Información por personal interno." (Delcy G. Rojas)
	Disponibilidad	"Auditoria, logs en las aplicaciones, inactivación de usuarios retirados entre otros." (Dixon F. Murillo) "Mensualmente se llevan a cabo auditorias para que las personas ya retiradas de la compañía tengas sus accesos bloqueados…" (Kevin A. Ortiz)
Eficiencia operativa	Reducción de errores	"Mucho, ya que como el proceso es manual el tiempo de ejecución es tardío y por temas de ingresos masivos se pueden asignar permisos por equivocación…" (W. Zorro) "Un promedio medio ocurre estas novedades ya sea por error humano…" (Julieth L.)
	Agilidad en procesos	"Es una parte fundamental del área… debe garantizar que los usuarios tengan los accesos… en los tiempos indicados." (Anonimo)

Variable	Dimensión	Respuesta extraída de la encuesta
		"Mejora la eficiencia en el acoplamiento de nuevo personal al área…" (Juan N. Riaño)
	Simplificación administrativa	"Cuando nos llegan las solicitudes… crearlos o eliminarlos directamente en la aplicación." (Julieth L.) "Se generan solicitudes en la plataforma de gestión de tickets…" (Juan N. Riaño)
Cumplimiento normativo	Auditoría	• "¿Se realizan auditorías de accesos? Anual." (Anónimo) "Sí, en el momento se tienen auditorias manuales y en algunos sistemas automáticas…" (W. Zorro) "Se realizan auditorias por parte de la revisoría fiscal… cada 6 meses a 1 año." (C. Ovalle)
	Controles técnicos	• "Controles SOX y certificación de accesos." (Anonimo) "Se realizan flujos de aprobación con al menos dos personas…" (W. Zorro)
Usuario	Integridad	"Riesgo de errores humanos en la asignación de accesos, lo que podría permitir que un usuario obtenga roles y privilegios que no correspondan…" (Óscar A. López) "Puede existir fuga de información, duplicidad de datos." (Duvar A. Cuéllar)
	Políticas organizacionales	"Todas las solicitudes deben venir de los jefes establecidos… no se atienden solicitudes que no estén bajo este flujo." (Julieth L.) "Políticas de gestión de identidades y accesos desde el área de Seguridad de la Información." (Delcy G.)

Fuente: Elaboración propia a partir del cuestionario realizadas.

La encuesta revelar una necesidad de automatización y trazabilidad en la gestión de identidades, en contraste con los actuales procesos manuales que ocasionan demoras y errores frecuentes. A pesar de contar con controles SOX y auditorías periódicas, muchos de estos son manuales y no logran mitigar por completo los riesgos de seguridad como fugas de información y excesivos privilegios. De igual forma, se constató un impacto negativo en la eficiencia operativa, pues los colaboradores enfatizaron la urgencia de agilizar y simplificar la administración de

accesos para no entorpecer sus labores diarias. Adicionalmente, las políticas y auditorías vigentes se perciben como insuficientes, lo que recalca la necesidad de implementar un modelo integrado de gestión de identidades con flujos de aprobación claros y parámetros de gobernanza definidos.

Factores críticos de éxito y las barreras en la adopción de sistemas de administración de identidades en empresas del sector retail.

Para identificar qué impulsa o frena la implementación de un IAM (Identity and Access Management) en empresas del sector retail, se analizaron las respuestas de los diez entrevistados agrupadas en dos grandes categorías: los factores críticos de éxito, aquellos elementos sin los cuales la solución difícilmente cumpliría con las expectativas y las barreras los obstáculos más frecuentes que, de no superarse, pueden condenar al proyecto al fracaso o a una adopción muy limitada.

La Tabla 5, presenta los factores y barreras que se presentaron con mayor fuerza de las encuestas:

Tabla 5 *Factores críticos de éxito y barreras en la adopción de sistemas de gestión de identidades (IAM) en el sector retail.*

FACTORES CRÍTICOS DE ÉXITO	BARRERAS EN LA ADOPCIÓN
Automatización completa	**Procesos manuales arraigados**
"La idea es poder tener un gestor que nos ayude a automatizar la asignación de accesos y no tener tanta intervención manual." (W. Zorro)	"Mucho, ya que como el proceso es manual el tiempo de ejecución es tardío…" (W. Zorro)
Integración con sistemas existentes	**Legado tecnológico**
"Debe ser un aplicativo con la capacidad de integrarse con múltiples soluciones…" (Ó. López)	"Se debe ingresar en cada sistema directamente…" (W. Zorro)
Trazabilidad y gobernanza claras	**Falta de gobierno definido**

"Trazabilidad, gobierno y funcionalidad." (Anónimo)	"En este momento no se tiene definido un gobierno…" (Ó. López)
Escalabilidad y flexibilidad	**Resistencia al cambio**
"Que sea flexible y, si en algún momento queda obsoleto…, se pueda mover con facilidad." (W. Zorro)	"El error humano y los elevados tiempos de ejecución dificultan la migración." (J. Correa)
Soporte y comunidad activa	**Costo y presupuesto limitado**
"Soporte técnico y comunidad de usuarios." (ficha comparativa)	"Los costos de licenciamiento e implementación son muy altos." (general)
Mandato y patrocinio ejecutivo	**Deficiencia de habilidades internas**
"Todas las solicitudes deben venir de los jefes establecidos…" (J. Correa)	"Las personas no están suficientemente capacitadas en seguridad de la información." (K. Ortiz)

Fuente: Elaboración propia a partir del cuestionario realizadas.

Los factores críticos de éxito coinciden en la necesidad de una solución que ofrezca automatización, integración y gobernanza sólida, pero sólo logrará una adopción real si cuenta con patrocinio ejecutivo, soporte técnico y margen para crecer. Por el contrario, las barreras más persistentes son los procesos manuales consolidados, el legado tecnológico que dificulta la conectividad, la falta de un gobierno formal y la resistencia al cambio. Adicionalmente, los costos y la carencia de competencias internas ponen en riesgo los beneficios esperados. Estos hallazgos orientan la fase de diseño del modelo, enfatizando la importancia de incluir un plan de gestión de cambio, capacitación continua y un mecanismo claro de gobernanza para asegurar que la propuesta no sólo sea técnicamente viable, sino también cultural y financieramente sostenible**.**

Evaluación de dos sistemas de gestión del ciclo de vida de identidades disponibles en el mercado, comparando su funcionalidad, escalabilidad, costos y compatibilidad con la empresa.

La ficha comparativa se llevó a cabo una revisión documental rigurosa de artículos científicos, white papers y documentación técnica publicada a partir de 2019, complementada

con manuales de producto y guías de usuario de Oracle Identity Management y Okta Identity Governance. A partir de esta base teórica se definieron criterios de análisis directamente vinculados a los objetivos del estudio: funcionalidad (creación, modificación y revocación de accesos), nivel de automatización, escalabilidad y adaptabilidad, compatibilidad con sistemas existentes, costos de licenciamiento e implementación, características de seguridad (MFA, cifrado y registros de auditoría), cumplimiento de estándares internacionales (ISO/IEC 27001, NIS2, GDPR), facilidad de uso y curva de aprendizaje, y calidad de soporte y comunidad de usuarios. Estos criterios orientaron el diseño de la tabla 6, comparativa y garantizaron una valoración consistente y alineada con las necesidades de una empresa del sector retail.

Tabla 6 *Ficha comparativa de alternativas tecnológicas.*

Criterio de evaluación	Sistema A: Oracle Identity Management	Sistema B: Okta Identity Governance
Funcionalidad	• Amplio catálogo de workflows de creación, modificación y revocación. • Personalización avanzada de flujos por rol. • Gestión de identidades híbrida (on-prem + cloud)	• Funciones básicas de creación, modificación y revocación. • Flujos preconfigurados muy intuitivos. • Fuerte enfoque cloud-native, menos personalización profunda
Oracle IM destaca en escenarios que requieren flujos de trabajo altamente específicos y entornos híbridos (on-prem + cloud), pero su despliegue y configuración son más laboriosos. Okta, en cambio, ofrece automatismos “out-of-the-box” que permiten poner en marcha la solución en semanas y adaptarse rápidamente a cambios operativos.		
Automatización del ciclo de vida	• Alto nivel de automatización, pero requiere desarrollo de conectores y scripts específicos. • Excelente para entornos complejos	• Automaciones “out-of-the-box” con catálogos de integraciones instantáneas. • Menor tiempo de puesta en marcha
Escalabilidad y adaptabilidad	• Altamente escalable en infraestructuras propias y nubes privadas.	• Escala automáticamente en la nube (SaaS).

Criterio de evaluación	Sistema A: Oracle Identity Management	Sistema B: Okta Identity Governance
	• Se adapta a grandes volúmenes, pero su diseño es más monolítico.	• Diseñado para añadir usuarios y aplicaciones de forma inmediata.
Compatibilidad con sistemas existentes	• Integra muy bien con el stack Oracle (DB, middleware, ERP). • Conectores para SAP, Microsoft Active Directory, etc., pero puede requerir ajustes.	• Más de 200 conectores listos para apps SaaS y on-prem (Salesforce, Office 365, AWS, etc.) • APIs REST fáciles de usar
La arquitectura SaaS de Okta garantiza un crecimiento prácticamente ilimitado con un coste marginal muy bajo, así como conectores inmediatos para las principales aplicaciones del retail. Oracle IM, aunque escalable, puede exigir recursos de infraestructura y ajustes mayores para integrar nuevas apps.		
Costos de licenciamiento e implementación	• Modelo de licencias perpetuas + mantenimiento anual. • Costes de infraestructura on-prem elevados	• Suscripción por usuario activo (pay-as-you-grow). • Costes iniciales reducidos; puede resultar más barato en despliegues cloud
Okta suele tener un coste inicial más bajo y flexible, con facturación por usuario activo; Oracle IM, por su modelo de licencias perpetuas y mantenimiento, exige una inversión mayor al inicio.		
Seguridad (MFA, cifrado, registros de auditoría)	• MFA integrada, cifrado en reposo y en tránsito. • Auditorías uy detalladas con logs de baja latencia.	• MFA adaptativa con análisis de riesgo en tiempo real. • Cifrado robusto y registros de auditoría centralizados
Cumplimiento de estándares (ISO, NIS2, GDPR…)	• Certificaciones ISO/IEC 27001, SOC 2, NIST SP 800-53. • Alineado con NIS2, GDPR y SOX	• Certificaciones SOC 2, ISO 27001, GDPR ready. • Cumple NIS2 y regulaciones de privacidad de datos europeas y latinoamericanas.
Ambos cumplen con los principales estándares, si bien Oracle IM lleva años madurando en entornos regulados y ofrece registros de auditoría de muy alta granularidad. Okta aporta un motor de riesgo en tiempo real y MFA adaptativo que refuerza la seguridad sin comprometer la experiencia de usuario.		
Facilidad de uso y curva de aprendizaje	• Interfaz robusta pero compleja; curva de adopción más larga.	• Dashboard muy intuitivo; administración self-service para usuarios finales.

Criterio de evaluación	Sistema A: Oracle Identity Management	Sistema B: Okta Identity Governance
	• Requiere formación especializada.	• Rápida adopción por parte de equipos de TI.
Soporte técnico y comunidad de usuarios	• Soporte 24×7 Enterprise con SLA garantizados. • Comunidad más reducida, centrada en clientes Oracle.	• Soporte 24×7 comunitario y profesional; documentación y foros muy activos. • Actualizaciones periódicas sin interrupción
Evaluación general del sistema	• Ideal para grandes corporaciones con infraestructuras híbridas y necesidades de personalización extrema, aunque con un coste y tiempo de despliegue más elevados.	• Perfecto para organizaciones cloud-first del sector retail que necesiten agilidad, rapidez de implementación y un TCO más bajo a corto y medio plazo.
Okta se alinea mejor con equipos de TI de retail que buscan reducir el “time-to-value” y contar con un onboarding sencillo, mientras que Oracle IM exige perfiles más especializados y formación dedicada.		

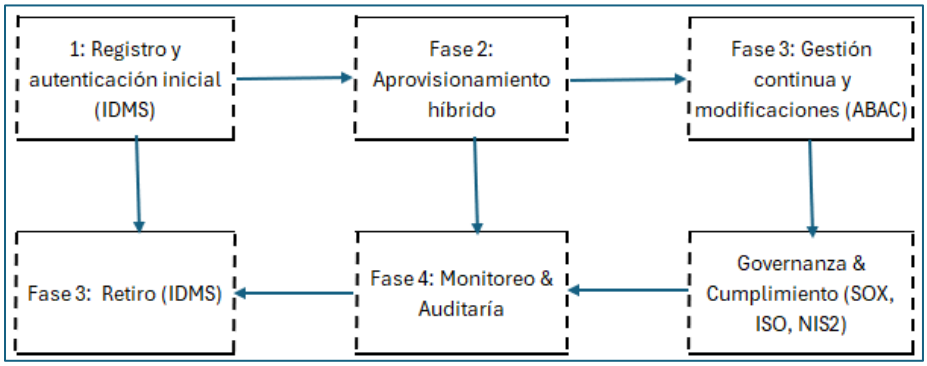
Fuente. Elaboración propia, tomando información de (Thompson, 2023), (Okta, 2023), (Okta, 2024), (ISO/IEC 27001:2022, 2022), (Directiva NIS 2, 2023).

La tabla comparativa, permite identificar que para una empresa de retail consciente de la alta rotación de personal y la necesidad de integración continua con plataformas SaaS, Okta Identity Governance representa la opción más ágil y costo-efectiva. Sin embargo, si la organización ya cuenta con un ecosistema Oracle muy consolidado y requiere personalización profunda de flujos de identidad, Oracle Identity Management aporta la robustez y el detalle de auditoría que justifican su inversión adicional. Estos hallazgos serán la base para el diseño final del modelo en el siguiente objetivo, buscando combinar las fortalezas de ambas soluciones según el contexto de la empresa.

Formular de un modelo de gestión del ciclo de vida de identidades adaptado a la empresa objeto de estudio, basado en la evaluación de alternativas.

Se propone un modelo integral que recoge lo mejor de las dos soluciones evaluadas (Oracle Identity Management y Okta Identity Governance), alineado con los requerimientos de la empresa retail estudiada. El diseño se articula en cinco fases principales, cada una soportada por componentes tecnológicos y de gobernanza que garantizan automatización, trazabilidad, seguridad y cumplimiento normativo.

Figura 2 *Modelo de integrado de gestión del ciclo de vida de identidades.*



Fuente: Elaboración propia, basada en O'Neill (2018) y NIST (2020). Nota. El esquema presenta las seis fases del modelo (desde el registro inicial hasta la validación piloto) y el módulo de gobernanza, mostrando la interdependencia entre procesos tecnológicos y políticas de cumplimiento.

Desarrollo operativo del modelo de gestión del ciclo de vida de identidades

A continuación, se detalle cada una de las fases que componen el modelo integrado de gestión del ciclo de vida de identidades, desde el registro inicial hasta la validación piloto "in-vivo". Para cada etapa se especifican los flujos, las tecnologías empleadas, los controles y validaciones, los roles responsables y las métricas clave que permitirán medir su desempeño y robustez. Esta visión operacional facilita la comprensión de cómo se articulan los componentes

técnicos y de gobernanza para lograr automatización, trazabilidad, seguridad y cumplimiento normativo.

Figura 3 *Desarrollo del modelo de gestión del ciclo de vida de identidades.*

Fase 1: Registro y autenticación inicial

- Fuente única de datos (“IdP Master”)

  Tecnología: Oracle Directory Services + Okta Universal Directory.

  Flujo:

  1. Importación automática de datos de RR. HH. (CSV/HRIS) hacia Oracle LDAP.
  2. Provisioning bidireccional: Okta sincroniza usuarios nuevos del LDAP.

  Validaciones:

  3. Integridad de atributos obligatorios (e-mail, cargo, departamento).
  4. Check ABAC: IF departamento == “TI” THEN role ∈ {Analista, Admin}.

  MFA inicial (Okta Adaptive MFA) para primer acceso.

Roles involucrados

Rol	Responsabilidad	Herramienta
Administrador HR	Sube / actualiza CSV de personal	HRIS → Oracle LDAP
Equipo IAM	Configura flujos de importación y validación	Okta Universal Dir.
Usuario final	Completa MFA y verifica perfil	Okta portal

Métricas clave

- Tiempo medio desde alta en HRIS a cuenta activa en Okta: < 15 min.
- % de cuentas con errores de atributos obligatorios: < 2%

Fase 2: Aprovisionamiento híbrido

- Motor de automatismos

  Okta Workflows para aplicaciones SaaS (Salesforce, Office 365).

  Oracle IDM para sistemas on-prem (SAP, base de datos internas).
- Asignación de roles RBAC + ABAC

  Plantillas de roles predefinidos: {“Vendedor”, “Analista TI”, “Gerente”}.

  Reglas dinámicas ABAC.
- Notificaciones

  Correo + Slack automático tras cada nuevo provisioning.

Métricas clave

- % de operaciones completadas sin intervención manual: > 90 %.
- Tasa de errores en scripts Oracle: < 1 %.

Fase 3: Gestión continua y modificaciones

- Portal self-service Okta

  Permitido para cambios de departamento, solicitudes de acceso temporal.

  Flujos de aprobación en cadena (min. 2 aprobadores para permisos críticos).
- Enriquecimiento de perfiles

Atributos adicionales: proyecto, nivel de riesgo, equipo de trabajo.
Evaluación de riesgo en tiempo real (Okta Risk Engine).

Métricas clave

- Tiempo medio de aprobación de solicitudes: < 2 h.
- % de solicitudes de acceso completadas vía self-service: > 70 %.

Fase 4: Monitoreo, auditoría y respuesta

- Registro detallado
  Logs de baja latencia (Oracle): entrada/salida de sesiones, cambios de roles.
  Logs en Okta: eventos de MFA, intentos de acceso fallidos, anomalías detectadas.
- Dashboard unificado (Splunk / Elastic Stack)
  Alertas en tiempo real si:
    - 5 intentos fallidos de MFA en 5 min.
    - Asignación de roll con nivel de riesgo “alto” sin 2* aprobación.
- Informes periódicos
  Semanal: incidentes de seguridad y aperturas de tickets.
  Mensual: cumplimiento de SLA de provisionamiento.

Métricas clave

- Número de alertas críticas vs. falsas alarmas: < 5 %.
- Tiempo medio de respuesta a incidente IAM: < 30 min.

Fase 5: Retiro y desprovisionamiento

- Automatismos basados en eventos
  Evento empleadoDesvinculado en HRIS dispara API a Okta y Oracle.
  Eliminación / suspensión de accesos en < 5 min.
- Reportes de validación
  Comparativa mensual de usuarios activos vs. lista de HRIS.

Métricas clave

- % de cuentas inactivadas en plazo: > 95 %.
- Casos de accesos “zombie” (extrabajadores con acceso): = 0.

Fase 6: Validación piloto “in-vivo”

- Objetivo: Testear el modelo con un grupo reducido de usuarios finales para recabar feedback real y ajustar parámetros antes de la implantación masiva.
- Alcance: Selección de 10–15 usuarios representativos (diferentes roles y ubicaciones) dentro de la empresa retail.
- Actividades:
  1. Despliegue controlado de las fases 1–5 en un entorno de pre-producción.
  2. Monitoreo de métricas clave (tiempos de provisioning, errores, tasa de adopción self-service).
  3. Recolección de sugerencias cualitativas (encuestas cortas y entrevistas de satisfacción).

4. Ajustes iterativos de flujos ABAC/RBAC, umbrales de alertas y experiencias de portal.

Módulo transversal: Gobernanza y cumplimiento

- Flujos SOX
  Configuración de aprobaciones duales para cambios sensibles.
- Patrocinio ejecutivo
  Comité trimestral de revisión de métricas IAM.
- Políticas y documentación
  Manuales internos, playbooks de incidentes, política de contraseñas.
- Alineaciones normativas
  Plantillas de reporte ISO/IEC 27001 y NIS2 incluidas en el dashboard.

Fuente. Elaboración propia. Nota. Detalla cada fase con sus flujos principales, herramientas clave, roles responsables y métricas de éxito, ofreciendo una visión operativa para su implementación y monitoreo.

A continuación, se muestra la Tabla 7, que sintetiza de manera concisa cómo cada criterio clave del estudio se ve reflejado en las distintas fases y componentes del modelo propuesto. Esta visión resumida permite verificar de un vistazo que el diseño atiende a los requerimientos de automatización, escalabilidad, seguridad, compatibilidad, cumplimiento, usabilidad y gobernanza definidos en los objetivos de la investigación.

Tabla 7 *Desarrollo del modelo de gestión del ciclo de vida de identidades.*

Criterio	Modelo
Automatización	Okta Workflows + Oracle scripts; > 90 % sin intervención
Escalabilidad	SaaS autoescala; Oracle admite clusters on-prem
Seguridad & trazabilidad	MFA adaptativo, logs Oracle, Okta Risk Engine
Compatibilidad	> 200 conectores + APIs REST
Cumplimiento	Workflows SOX; reportes ISO & NIS2
UX & adopción	Portal self-service; formación; patrocinio ejecutivo
Gobernanza	Aprobaciones duales; comité ejecutivo

Fuente. Elaboración propia.

Validar la viabilidad del modelo propuesto mediante una matriz de valoración que permita determinar su alineación con las necesidades de la empresa.

La Tabla 8, sintetiza la evaluación cuantitativa del modelo de gestión del ciclo de vida de identidades propuesto, mediante una matriz de valoración construida con criterios clave identificados en el estudio (alineación operativa, automatización, cumplimiento normativo, facilidad de implementación, costos, aceptación interna, escalabilidad y sostenibilidad). Cada criterio recibió un peso según su importancia estratégica y una calificación de 1 a 5 basada en la percepción del equipo de TI, lo que permitió calcular un valor ponderado que cuantifica la viabilidad global de la solución.

Tabla 8 *Matriz de valoración del modelo propuesto (con calificaciones y valor ponderado).*

Criterio evaluado	Peso (%)	Calificación (1–5)	Valor ponderado (Peso × Calif.)
Alineación con necesidades operativas	25%	4	**1,00**
Nivel de automatización del proceso	15%	5	**0,75**
Cumplimiento con normativas y estándares	15%	4	**0,60**
Facilidad de implementación	10%	4	**0,40**
Costos asociados	10%	3	**0,30**
Aceptación por parte del equipo de TI	10%	4	**0,40**
Escalabilidad del modelo	10%	5	**0,50**
Sostenibilidad en el tiempo	5%	4	**0,20**
Total	**100%**		**4,15**

Fuente. Elaboración propia.

Con un puntaje agregado de 4,15 sobre 5, el modelo demuestra una sólida viabilidad, destacándose especialmente en automatización y escalabilidad. Este resultado valida que la combinación de las mejores capacidades de Oracle IM y Okta satisface de manera efectiva las prioridades operativas y de seguridad del retail. Asimismo, señala áreas de mejora principalmente en la optimización de costos, que deberán abordarse durante la fase piloto para garantizar una implantación exitosa.

CONCLUSIONES

La problemática de la gestión del ciclo de vida de identidades en una empresa del sector retail, identificando beneficios, desafíos y validando un modelo integral que combina las fortalezas de Oracle Identity Management y Okta Identity Governance. En primer lugar, la implementación de un sistema automatizado y trazable redujo significativamente los errores humanos y los tiempos de provisión, tal como plantean Ferraiolo y Kuhn (1992), en su fundamentación de RBAC, y concuerda con los principios de defensa en profundidad de Stallings (2019). Asimismo, el diseño híbrido propuesto permitió la escalabilidad automática en la nube y la integración con sistemas legacy, ofreciendo un “time-to-value” reducido sin sacrificar la personalización profunda para entornos críticos (NIST, 2020).

Desde la perspectiva de la seguridad de la información, el uso de MFA adaptativo y análisis de riesgo en tiempo real reforzó la confidencialidad e integridad de los datos, respaldando las recomendaciones de ISO/IEC 27001 (2022) y las directrices de la NIS2 (2022), sobre auditoría continua. Este enfoque dinámico se alinea con las tendencias de identidad cero-confianza descritas por Hacking (2024), que promueven controles de acceso basados en contexto y atributos (ABAC) para minimizar vectores de ataque.

En términos operativos y culturales, el módulo de gobierno y el plan de gestión de cambio con patrocinio ejecutivo y capacitación continua— resultaron determinantes para superar la resistencia interna (Montoya & Restrepo, 2012). La validación piloto “in-vivo” confirmó la aceptabilidad del portal self-service y la eficacia de los workflows, recuperando retroalimentación que permitió ajustar los umbrales de alerta y optimizar los flujos ABAC/RBAC antes de la adopción masiva.

Finalmente, la puntuación global de viabilidad 4,15 sobre 5, demuestra que el modelo propuesto satisface de manera equilibrada las exigencias de automatización, cumplimento normativo, usabilidad y sostenibilidad, aunque identifica la necesidad de mejorar la gestión de

costos operativos. En conjunto, estos hallazgos evidencian que una estrategia de gestión de identidades bien diseñada no solo mitiga riesgos de seguridad, sino que también impulsa la eficiencia y la agilidad organizacional, contribuyendo de manera significativa a la resiliencia y competitividad de las empresas retail.

REFERENCIAS

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances, 21*(2). https://www.redalyc.org/journal/6378/637869113010/html/

Anaya, F. (1 de enero de 2024). *La gestión del riesgo en torno a la mayor vulnerabilidad y el vector más explotado: la identidad.* https://www.redseguridad.com/especialidades-tic/gestion-y-gobierno-ti/la-gestion-del-riesgo-en-torno-a-la-mayor-vulnerabilidad-y-el-vector-mas-explotado-la-identidad_20240131.html

Barajas, E. (2023). *Propuesta de mejora para la gestión documental del área de proyectos de la empresa MIRS Latinoamerica S.A.S.* Bogotá: Universidad de los Andes. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/48933b7b-ea0e-4ccf-8c6b-dd631d03d11b/content

Berdugo, J., & Cardona, J. (12 de diciembre de 2022). *Autenticación, autorización y acceso a través del uso de una identidad digital descentralizada (DID).* https://repositorio.uniandes.edu.co/entities/publication/07b75371-232d-404d-bdbc-9119b85302a7

Brochero, D. (2019). *Diseño de una metodología de gestión de información para el sector mipyme a través del uso de business intelligence.* Bogotá: Pontificía Universidad Javeriana. https://repository.javeriana.edu.co/bitstream/handle/10554/49994/TRABAJO%20DE%20GRADO%20FINAL.pdf?sequence=1&isAllowed=y

Camacho, A. (2024). *Diseño de un modelo de gestión de incidentes de T.I. para la empresa social MEDICAL DATA 2024.* Girardot: Universidad Piloto de Colombía. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/14031/Proyecto%20de%20Grado%20-%202024.pdf?sequence=1&isAllowed=y

Directiva NIS 2. (2023). *¿Qué es la Directiva NIS 2?* https://www.nis-2-directive.com/

Ferraiolo, D., & Kuhn, R. (1992). Role-Based Access Controls. *15th National Computer Security Conference, 13*(16), 554-563. https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased-access-controls/final/docs/ferraiolo-kuhn-92.pdf

Flores, W. (2023). *Factores para la adopción de servicios de Cloud Computing y sus.* Guayaquil – Ecuador: Universidad Tecnológica Empresarial de Guayaquil.

Flórez, R. (2019). *Implementación del modelo de gestión documental digital para mejorar la calidad de servicio en la empresa ENTER SAC.* Jesús María. Lima, Perú: Repositorio.

Universidad Peruana de ciencias informáticas. https://doi.org/http://repositorio.upci.edu.pe/handle/upci/235

Gaítan, J. (2022). *Análisis del modelo de seguridad Zero Trust y las consideraciones generales aplicables a cualquier organización pública en Colombia.* Fusagasugá: Escuela Nacional Abierta y a Distancia - UNAD. https://repository.unad.edu.co/bitstream/10596/48929/1/jlgaitanb.pdf

Hacking, E. (15 de noviembre de 2024). *Cómo la IA está transformando la gestión de identidades y acceso (IAM) y la seguridad de la identidad.*

IBM. (26 de marzo de 2024). *¿Qué es la gestión de identidades y accesos (IAM)?* https://www.ibm.com/es-es/topics/identity-access-management

ISO/IEC 27001. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* https://www.iso.org/es/norma/27001

ISO/IEC 27001:2022. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad.* Sistemas de gestión de la seguridad de la información: https://www.iso.org/standard/27001

Keshet, Y. (26 de marzo de 2024). *The Identity Underground Report: visión profunda de las brechas de seguridad de identidad más críticas.* https://www.silverfort.com/es/blog/the-identity-underground-report-deep-insight-into-the-most-critical-identity-security-gaps/

León, W., Peñaranda, D., & Vargas, H. (2022). *Replanteando la gestión estratégica en constructora de ciudad intermedia.* Universidad de los Andes. https://repositorio.uniandes.edu.co/server/api/core/bitstreams/ed1986d9-3fa6-480c-966d-eff562b77d8c/content

Microsoft. (01 de abril de 2024). *¿Qué es el control de acceso basado en atributos de Azure (Azure ABAC)?* https://learn.microsoft.com/es-es/azure/role-based-access-control/conditions-overview

Minchalo, P. (2022). *Propuesta de mejora en la gestión del branding de a cadena retail "RADI" en la ciudad de cuenca.* Cuenca-Ecuador: Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/23968/1/UPS-CT010255.pdf

MinTic. (28 de octubre de 2021). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.* https://gobiernodigital.mintic.gov.co/692/articles-237908_maestro_mspi.pdf

Momblanc, L., & Castro, H. (2020). La gestión documental y el control interno: un binomio indispensable. *Revista Del Archivo Nacional, 84*, 1-12. https://doi.org/https://www.dgan.go.cr/ran/index.php/RAN/article/view/481

Montoya, J., & Restrepo, Z. (2012). Gestión de identidades y control de acceso desde una perspectiva organizaciona. *Ing. USBMed, 3*(1), 23-34.

NIS2. (2022). *Directiva sobre redes y sistemas de información 2 (NIS2).* https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2

NTC-ISO 9001. (09 de septiembre de 2015). *Sistema de la gestión de la calidad. requisitos.* https://www.guadalupanolasalle.edu.co/sgc/ISO9001-2015-Requisitos.pdf

Okta. (2023). *What Identity Governance looks like in 2023.* https://www.okta.com/resources/webinar-what-identity-governance-looks-like-in-2023/

Okta. (7 de 11 de 2024). *¿Qué es la Red de Integración Okta?* https://workos.com/blog/what-is-the-okta-integration-network

O'Neill, D. (2018). Una buena vida para todos dentro de los límites planetarios. *Sostenibilidad de la naturaleza volumen, 1*, 88-95. https://www.nature.com/articles/s41893-018-0021-4

Quecedo, R., & Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. *Revista de Psicodidáctica, 14*, 5-39. https://www.redalyc.org/pdf/175/17501402.pdf

Rodríguez, D. (24 de febrero de 2023). *La gestión de identidades, un elemento de seguridad clave en 2023.* https://www.itdigitalsecurity.es/opinion/2023/02/la-gestion-de-identidades-un-elemento-de-seguridad-clave-en-2023

Rojas. (3 de agosto de 2023). *Diferencias entre ISO 27002 e ISO 27003 y cómo abordar estos estándares.* https://www.pmg-ssi.com/2023/08/diferencias-entre-iso-27002-e-iso-27003-y-como-abordar-estos-estandares/

Role-Based Access Control Models. (1996). *IEEE Computer, 29*(2), 38-47. https://csrc.nist.gov/csrc/media/projects/role-based-access-control/documents/sandhu96.pdf

Saltzer, J., & Schroeder, M. (1974). *The Protection of Information in Computer Systems.* University of Virginia, Department of Computer Science.

SINFOPAC. (30 de agosto de 2024). *¿Qué es la gestión del ciclo de vida de la identidad?*

Thompson, L. (25 de 10 de 2023). *Lanzamiento del parche proactivo de Oracle Access Management 12.2.1.4 de octubre de 2023.* Compatibilidad con Fusion Middleware:

https://blogs.oracle.com/fusionmiddlewaresupport/post/october-2023-oracle-access-management-12214-proactive-patch-released

Universidad Pontificia Comillas. (18 de diciembre de 2023). *Seguridad en Profundidad.* https://ciberseguridad.comillas.edu/seguridad-en-profundidad/

Whitman, M., & Mattord, H. (10 de marzo de 2018). *Gestión de la seguridad de la información.* https://books.google.com.co/books/about/Management_of_Information_Security.html?id=TuNhEAAAQBAJ&redir_esc=y#:~:text=Whitman/Mattord's%20MANAGEMENT%20OF%20INFORMATION,available%20in%20the%20ebook%20version.

Yopan, J., Palmero, N., & Santos, J. (2020). Cultura organizacional: De las teorías comunicativas al enfoque organizacional complejo y perspectivas antropológicas latinoamericanas. *Controversias y Concurrencias Latinoamericanas, 11*(20), 263-289.

ANEXOS

Instrumentos

1. Cuestionario de preguntas abiertas

La intención del instrumento del cuestionario es recolectar información cualitativa sobre los procesos actuales de gestión de identidades, las necesidades operativas, las dificultades percibidas y los criterios para la selección de soluciones tecnológicas dentro de la empresa del sector retail.

Anexo 1 *Estructura del cuestionario de preguntas abiertas.*

Buenas tardes.

El cuestionario de preguntas abiertas forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.

Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.

El cuestionario durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza continuar con el cuestionario?

_____

Datos generales del participante

- Cargo:
- Tiempo en la organización:
- Experiencia con sistemas de gestión de identidades:

Bloques temáticos y preguntas orientadoras

a. Situación actual de la gestión de identidades

- ¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?
- ¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?

b. Percepción sobre riesgos y eficiencia

- ¿Qué riesgos considera que existen actualmente en el acceso a la información?
- ¿Cómo impacta la gestión de identidades en la eficiencia del área?

c. Cumplimiento normativo

- ¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?
- ¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?

d. Interés en soluciones tecnológicas

- ¿Ha tenido contacto con sistemas automatizados de gestión de identidades?
- ¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?

Muchas Gracias

Fuente. Elaboración propia.

2. Ficha comparativa de alternativas tecnológicas

El desarrollo de la ficha comparativa se fundamentará en una revisión documental de artículos científicos publicados a partir del año 2019, así como en el análisis de documentación técnica y fuentes especializadas. Esta herramienta permitirá evaluar dos alternativas tecnológicas reconocidas para la gestión del ciclo de vida de identidades: Oracle Identity Management y Okta Identity Governance, seleccionadas por su amplia adopción en entornos empresariales y por su alineación con las necesidades del sector retail. La comparación se basará en criterios como

funcionalidad, automatización, escalabilidad, costos, compatibilidad, seguridad y cumplimiento normativo. Los resultados obtenidos facilitarán una toma de decisiones informadas para el diseño del modelo propuesto.

Anexo 2 *Estructura sugerida de la ficha.*

Criterio de evaluación	**Sistema A** **Oracle Identity Management**	**Sistema B** **Okta Identity Governance**
Funcionalidad (creación, modificación, revocación de accesorios)		
Automatización del ciclo de vida.		
Escalabilidad y adaptabilidad		
Compatibilidad con sistemas existentes		
Costos de licenciamiento e implementación		
Seguridad (MFA, cifrado, registros de auditoría)		
Soporte técnico y comunidad de usuarios		
Cumplimiento de estándares (ISO, NIS2)		
Facilidad de uso y curva de aprendizaje.		
Evaluación general del sistema		

Fuente. Elaboración propia.

3. Matriz de valoración del modelo propuesto

La matriz de valoración se aplica como instrumento final para evaluar la viabilidad del modelo de gestión del ciclo de vida de identidades propuesto. Esta herramienta se diligenciará en conjunto con el equipo de tecnología de la empresa del sector retail, quienes asignarán una calificación del 1 al 5 a cada criterio, según su percepción y experiencia. Cada criterio tendrá un

peso porcentual previamente definido, que refleja su relevancia estratégica, técnica u operativa dentro del contexto organizacional. A partir de esta ponderación, se calculará un valor total que permitirá determinar el nivel de viabilidad del modelo en términos de automatización, cumplimiento normativo, alineación con las necesidades operativas, facilidad de adopción y sostenibilidad. Este análisis complementará la validación técnica del modelo y guiará su posible implementación.

Anexo 3 *Estructura de la matriz.*

Criterio evaluado	Peso (%)	Calificación (1-5)	Valor ponderado
Alineación con necesidades operativas	**25 %**		
Nivel de automatización del proceso	**15 %**		
Cumplimiento con normativas y estándares	**15 %**		
Facilidad de implementación	**10 %**		
Costos asociados	**10 %**		
Aceptación por parte del equipo de TI	**10 %**		
Escalabilidad del modelo	**10 %**		
Sostenibilidad en el tiempo	**5 %**		
Total	**100 %**		**Resultado**

Fuente. Elaboración propia.

Anexo 4 Respuestas de la encuesta de respuestas abiertas

ENTREVISTA

ean universidad Acreditada en Alta Calidad

NOMBRE DEL ENTREVISTADO	Carlos Andrés David Ovalle		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	10:00 a.m.	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	10:20 a.m.
CARGO EN LA ORGANIZACIÓN	Tecnico gestion de identidades		**TIEMPO EN LA ORGANIZACIÓN**	1 año	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?

SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Diariamente llegan a un buzón de correo las solicitudes de los usuarios que se deben crear, al igual que los usuarios que se deben inactivar por terminación de contrato. Se debe ingresar aplicativo por aplicativo y crear o inactivar respectivamente.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesos?	Muy frecuente, ya que este proceso requiere de mucha interacción humana lo cual hace que se generen mayores posibilidades de error en cada paso.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Existen muchos riesgos ya que no se tiene un control o sistema que unifique y permita la vigilancia de los permisos asignados a todos los usuarios de la compañía, lo que hace que la operación sea muy riesgosa.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	El impacto es significativo ya que se entiende que la gestión de identidades es uno de los pilares fundamentales para que todas las personas de la empresa puedan desarrollar sus funciones de la manera más eficiente.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Certificaciones de acceso, se miden a nivel de cargos y permisos asociados al mismo.
¿Se realizan auditorías de accesos? ¿Con qué frecuencia?	Se realizan auditorias por parte de la revisoría fiscal y demás entidades, con una frecuencia aproximada de 6 meses a un año.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Si, una vez trabajé con el gestor de identidades de Oracle (OIM)
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	La minimización de tareas manuales y optimización de procesos, lo que generaría mayor eficiencia y productividad en la compañía.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Carlos Andrés David Ovalle

Documento de identidad: 1000352646

Correo electrónico: carlosjorge7913@gmail.com

Firma: Carlos David

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Delcy Garcia Rojas		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	12:03	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	12:28
CARGO EN LA ORGANIZACIÓN	Analista Ciberseguridad		**TIEMPO EN LA ORGANIZACIÓN**	29 Años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	SI	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Se realiza el proceso en la aplicación de certificados digitales
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	No estan frecuente.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Posible fuga de Información por personal interno.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Proceso muy manual, posibles errores en la asignación de permisos, demora en los procesos,
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Políticas de gestión de identidades y accesos desde el área de seguridad de la Información. Manual de gobierno para el control de identidades y accesos a la información, Directriz de seguridad para el control de identidades y accesos a la información.
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Una vez al año.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	No
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	1. Gestión del ciclo de vida de Identidades, (gestión de roles y atributos) 2. Control de acceso basado en roles. 3. Gestión de privilegios mínimos. 4. Registro detallado de actividades, reportes, alertas y monitoreo.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Daley García Rgas

Documento de identidad: 52.049.328-3ta

Correo electrónico: gddagr@gmail.com.

Firma:

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	DIXON FERNANDO MURILLO MONTOYA		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	3:16 PM	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	
CARGO EN LA ORGANIZACIÓN	COORDINADOR DE GESTION DE IDENTIDADES		**TIEMPO EN LA ORGANIZACIÓN**	31 AÑOS	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Las diferentes áreas de la organización envían una solicitud de creación o inactivación de usuarios a través de correo electrónico. Se gestiona la solicitud y se responde el correo.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesos?	Es bastante frecuente teniendo en cuenta que el proceso de gestión de accesos es muy manual.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	AL no existir un gobierno establecido en el proceso de gestión de accesos que defina las políticas de segregación, se corre el riego de accesos a información no autorizada.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	El impacto es considerable teniendo en cuenta que todo se hacer de forma manual.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Auditorias, logs en las aplicaciones, inactivación de usuarios retirados entre otros
¿Se realizan auditorías de accesos? ¿Con qué frecuencia?	Si, por demanda mínimo una vez al año
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Si
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Automatización, segregación, auditorias, escalabilidad, disminución de la operación, disminución de la asignación de accesos no autorizados.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Dixon Fernando Ximenez Montoya

Documento de identidad: 79708718

Correo electrónico: mzdixfdo@gmail.com

Firma:

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Duvar Alejandro Cuellar Caicedo		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	11:30	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	
CARGO EN LA ORGANIZACIÓN	Analisa de Ciberseguirdad		**TIEMPO EN LA ORGANIZACIÓN**	2 años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Esto se realiza por AD, aplicaciones CORE, asignación de Licencias en cada una de las plataformas que requiera para sus funciones y una BD donde se depuran en modo de perfiles las funciones o roles de los usuarios.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	Los errores son frecuentes debido a la depuración de la información o que sus cargos no se ajustan con los roles que se parametrizan en el perfil predefinido.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Puede existir fuga de información, duplicidad de datos.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Reprocesos en la gestión, aumento de incidentes dentro de la operación.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Auditorías internas.
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Anualmente
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	No
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Principalmente que se integrable o compatible con los aplicativos que requiere el usuario, que sea autogestiónale en aspectos de contraseñas para usuario final, Ofrezca crecimiento y mejora continua en sus servicio y adaptativo a las nuevas Tecnologias.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Duvan Alejandro Cruz Ibr

Documento de identidad: 1012465995

Correo electrónico: dlopez-99@hotmail.com

Firma:

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Julieth Lorena Correa		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	03:00 pm	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	04:00 pm
CARGO EN LA ORGANIZACIÓN	Analista de gestión de identidades		**TIEMPO EN LA ORGANIZACIÓN**	7 años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Cuando nos llegan las solicitudes actualmente tenemos que ingresar a los aplicativos que se manejan en la compañía y crearlos o eliminarlos directamente en la aplicación.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	Un promedio medio ocurre estas novedades ya sea por error humano o inconsistencias en las solicitudes.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Existen varios riesgos sobre la información como los accesos que no están autorizados, incluso con las credenciales que son otorgadas ya que teniendo un gestor estas credenciales ya les llegan directamente a los usuarios.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Siempre el impacto a la gestión de accesos el alto ya que ayuda en la gestión que es entregada a los usuarios, la automatización de los accesos, prevenir un menor riesgo dentro de la asignación de los accesos.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Todas las solicitudes deben de venir por parte de los jefes establecidos para aprobar los accesos, no se atienden solicitudes que no estén bajo este flujo de correo.
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Si, se realizan auditorias en los accesos esporádicamente por parte de auditoría, cada mes se realizaban.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Si he tenido experiencia con estos sistemas.
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Una característica seria fortalecer o implementar la autenticación por doble factor

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Julieth Lorena Correa Tryjillo

Documento de identidad: 1019309158

Correo electrónico: julieth1correa@gmail.com

Firma: Lorena Correa

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Kevin Augusto Ortiz Villa		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	3:00 pm	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	3:30 pm
CARGO EN LA ORGANIZACIÓN	Técnico en Gestion de acceso		**TIEMPO EN LA ORGANIZACIÓN**	2 anos	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?

SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Actualmente la creación de usuario se realiza por medio del CMD por scripts de forma masiva, y de igual forma con la eliminación de los usuarios
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	No muy a menudo ya que los pasos de creación están debidamente marcados, pero como todo hay errores humanos
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	En mi experiencia Laboral en el área considero que la primera falla de seguridad son las personas poco capacitadas en la compañía en el tema de seguridad de la información, ya sea por el tema de compartir contraseñas y usuarios para poder realizar operación que otros no, hasta el problema de autorizar accesos a usuarios sin haber pasado por una rama de riegos
¿Cómo impacta la gestión de identidades en la eficiencia del área?	El impacto es critico ya que por un acceso no asignado se pueden perder ventas y negociaciones o pagos oportunos Los cuales causan grandes traumatismos a las compañías
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Se implementan revisiones periódicas del acceso de las personas, que hayan sido modificados por personas externa al área
¿Se realizan auditorías de accesos? ¿Con qué frecuencia?	Mensualmente se llevan a cabo auditorias para que las personas ya retiradas de la compañía tengas sus accesos bloqueados, para evitar fugas de información
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Si, con el gestor de identidades de Oracle
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Auditoria, Segregación de Roles, permitir integración con aplicaciones y aplicaciones legadas, flujos de aprobación y automatización de procesos.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Kevin Augusto Ortiz Villa

Documento de identidad: 1.030.642.115

Correo electrónico: Kevin.Ortiz.V1@gmail.com

Firma:

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Juan Nicolas Riaño Erazo		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	11:37	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	11:59
CARGO EN LA ORGANIZACIÓN	Analista de Ciberseguridad		**TIEMPO EN LA ORGANIZACIÓN**	8 Meses	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Se genera una solicitud en la plataforma de gestión de tickets para solicitar la creación o eliminación.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	Frecuentemente, las actividades de los usuarios no suelen estar definidas completamente.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Considero que no hay un filtrado de roles en las plataformas de fabricantes lo cual puede ser sobre permisivo en algunos casos, sumando a la falta de monitoreo en las acciones de roles privilegiados no administradores suponen un riesgo alto para la gestión de información.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Mejora la eficiencia en el acoplamiento de nuevo personal al área y reduce los riesgos potenciales relacionados a permisos excesivos.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Auditoria, lineamientos de seguridad y trazabilidad de acciones realizadas sobre y para usuarios.
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Relacionados a la asignación de accesos, y algunos factores puntuales definidos por auditoria de forma anual.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	No.
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Integración con las diferentes nubes o fuentes. Capacidades granulares de automatización. Gestión centralizada. Roles basados en accesos. Integraciones relacionadas a alertamiento y monitoreo, así como a seguridad y cumplimiento.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

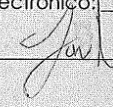
Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Juan Nicolas Riaño Erazo

Documento de identidad: 1019139157

Correo electrónico: nicolas0360@hotmail.com

Firma: 

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	Oscar Andres Lopez Diaz		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	12:15PM	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	12:41PM
CARGO EN LA ORGANIZACIÓN	Analista de Gestion de Identidades		**TIEMPO EN LA ORGANIZACIÓN**	6 años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Se valida con el área de Gestión Humana el archivo de ingresos, retiros y ausentismos, para identificar a los usuarios a los que se debe retirar o crear acceso. Posteriormente, se ingresa directamente a cada aplicativo para realizar los cambios, creaciones o inactivaciones correspondientes.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	Debido a la naturaleza manual de las acciones, es muy común que se cometan errores humanos al momento de gestionar los cambios.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Riesgo de errores humanos en la asignación de accesos, lo que podría permitir que un usuario obtenga roles y privilegios que no correspondan a su cargo. lo que deriva en acceso a información sensible
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Al ser un proceso manual, la asignación de accesos según el rol del usuario puede tomar mucho tiempo, lo que afecta directamente la eficiencia del área.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	En este momento, no se tiene definido un gobierno, por lo que los accesos se están garantizando según el cargo del usuario y los permisos asociados a este.
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Dado que no se tiene definido un modelo de gobierno, las auditorías de accesos se realizan semanalmente, cruzando la información de los permisos asociados al cargo con los accesos que el usuario tiene actualmente.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Contacto inicial con el Oracle Identity Manager
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	Debe ser un aplicativo con la capacidad de integrarse con múltiples soluciones, permitiendo la implementación de automatizaciones en la gestión de accesos. Además, debe contar con alta disponibilidad para ejecutar tareas masivas de manera eficiente, asegurando que no consuman demasiado tiempo.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Oscar Andrés López

Documento de identidad: 80195174

Correo electrónico: osukaru1@gmail.com

Firma: 

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO	William Felipe Zorro Salamanca		**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**	02:30 pm	**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	03:00 pm
CARGO EN LA ORGANIZACIÓN	Analista de Gestion Identidades y Accesos		**TIEMPO EN LA ORGANIZACIÓN**	4 años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	X	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	Se debe ingresar en cada sistema directamente y gestionar desde allí la acción que se requiere.
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesos?	Mucho, ya que como el proceso es manual el tiempo de ejecución es tardío y por temas de ingresos masivos se pueden asignar permisos por equivocación a los usuarios.
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Problemas de disponibilidad y confidencialidad ya que puede haber accesos en aplicaciones que no fueron retirados a los usuarios.
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Es parte fundamental de la compañía, ya que desde allí parte la organización e implementación de la metodología que tenemos en la empresa para entregar los diferentes accesos a los usuarios.
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Se realizan flujos de aprobación con el fin de que sean mínimo dos personas que participen en la justificación de la asignación de los accesos, y si es un permiso que con lleve un riesgo mayor es revisado por la respectiva área encargada en la compañía para mirar los diferentes vectores de riesgos y revisar algún flujo que permita realizar un mayor control de ese permiso, ya sea por medio de auditorías manuales o automáticas estar revisando las acciones realizadas por lo usuario que tienen el acceso.
¿Se realizan auditorías de accesos? ¿Con qué frecuencia?	Si, en el momento se tienen auditorias manuales y en algunos sistemas automáticas, sin embargo, la mayoría al ser manuales dependemos del tiempo que se emplea para realizarla, para lo cual en algunos sistemas toman demasiado tiempo y tienden a realizarse muy de vez en cuando, tanto que algunos se realizan cuando sucede alguna novedad.
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	Si, la idea es poder tener un gestor que nos ayuden a automatizar la asignación de los accesos y no tener tanta intervención manual.
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo?	El tema de tener diferentes complementos que con lleven a poder conectar los sistemas que estén en la compañía, que sea flexible al tiempo en cuanto a que si en algún momento quede obsoleto por temas de soporte se pueda mover con facilidad a otra solución. Que permita tener diferentes controles para asignación de accesos,

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: William felipe Zorro Salamanca

Documento de identidad: 1051590499

Correo electrónico: fsalamank@gmail.com

Firma: William Felipe Zorro Salamanca

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.

ENTREVISTA

NOMBRE DEL ENTREVISTADO			**REALIZADO POR**	Nestor Julian Ortiz Gutierrez	
FECHA DE LA ENTREVISTA	30/04/2025	**HORA DE INICIO DE LA ENTREVISTA**		**HORA DE FINALIZACIÓN DE LA ENTREVISTA**	
CARGO EN LA ORGANIZACIÓN	Analista de gestion de accesos		**TIEMPO EN LA ORGANIZACIÓN**	2 años	

DESCRIPCIÓN DE LA ENTREVISTA

Esta entrevista forma parte de un proyecto académico de la Universidad EAN, cuyo objetivo es conocer los procesos actuales de gestión de identidades en la empresa, así como las necesidades y retos relacionados con la seguridad, eficiencia y cumplimiento normativo.
Su participación es voluntaria y no tendrá ningún efecto sobre su situación laboral. La información recopilada se tratará de forma confidencial y anónima, y se utilizará únicamente con fines investigativos.
La entrevista durará entre 20 y 30 minutos. Puede abstenerse de responder cualquier pregunta o retirarse en cualquier momento.

¿Autoriza Continuar con la Entrevista?			
SI	x	**NO**	

A). Situación actual de la gestión de identidades	
¿Qué procesos siguen actualmente para crear o eliminar usuarios en los sistemas?	
¿Qué tan frecuentes ocurren errores o inconsistencias en la asignación de accesorios?	
B). Percepción sobre riesgos y eficiencia	
¿Qué riesgos considera que existen actualmente en el acceso a la información?	Asignacion de provilegios o permisos no autorizados, trazabilidad de cambio y asignaciones
¿Cómo impacta la gestión de identidades en la eficiencia del área?	Es una parte fundamenta del area y la compañia ya que la gestion de identidades debe garantizar que los usuario tengas los accesos corespondan para el desempeño de sus funciones en los tiempos indicados
C). Cumplimiento normativo	
¿Qué controles están implementados para garantizar el cumplimiento de las normas de seguridad?	Controles sox y certificacion de accesos
¿Se realizan auditorías de accesorios? ¿Con qué frecuencia?	Anual
D). Interés en soluciones tecnológicas	
¿Ha tenido contacto con sistemas automatizados de gestión de identidades?	He tenido contacto con adminstradores de identidades como OIM y IDM
¿Qué características consideran imprescindibles en una solución tecnológica de este tipo	Trazabilidad, gobierno y funcionabilidad.

Cierre de la Encuesta y Autorización para el Tratamiento de Datos Personales

Agradecemos su participación voluntaria en esta encuesta. Su aporte es fundamental para el desarrollo de este proyecto académico, y la información suministrada será tratada con total confidencialidad y utilizada exclusivamente con fines investigativos.

Datos del participante:

Nombres y apellidos: Yerson Calderon Moreno

Documento de identidad: 1024519118

Correo electrónico: yerson.calderon1986@gmail.com

Firma: Yerson C.

Autorización para el tratamiento de datos personales

En cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 sobre protección de datos personales en Colombia, autorizo de manera libre, previa, expresa y voluntaria para que realice el tratamiento de mis datos personales con la finalidad de gestionar la información recolectada en el marco del presente proyecto académico.