Instituto Europeo de Posgrado

Propuesta de fortalecimiento del proceso de gestión de identidades y accesos (IAM) basada en principios de Zero Trust y estándares internacionales de seguridad de la información: Caso JFMarket S.A.

Trabajo fin de estudio presentado por:	**Jesus del Campo Jimenez**
Tipo de trabajo:	**Trabajo de Fin de Máster (TFM)**
Director/a:	**Fabricio Echeverria Claustro**
Fecha:	**25/03/2026**

- Caso JFMarket S.A.

Índice

1 Resumen

El proyecto de investigación-acción se realiza en el análisis y mejora del proceso de gestión de accesos y control de identidades (IAM), en la empresa JFMarket S.A., dedicada al comercio electrónico. En la realidad actual de transformación digital y adopción de servicios en la nube, la organización ha experimentado un crecimiento rápido en número de empleados, proveedores y plataformas tecnológicas, lo que ha incrementado significativamente la complejidad en la administración de identidades y permisos de acceso.

El diagnóstico inicial dejó claro las deficiencias en la gestión del ciclo de vida de las identidades, asignaciones manuales de privilegios, ausencia de revisiones periódicas de accesos y falta de segregación de funciones en sistemas críticos. Estas debilidades generan riesgos asociados a accesos indebidos, exposición de información sensible y posibles incumplimientos normativos en materia de protección de datos.

Al realizar la metodología de investigación-acción, se desarrolló un análisis estructurado del proceso actual (AS-IS) y se diseñó una propuesta de mejora (TO-BE) basada en buenas prácticas internacionales como ISO 27001, NIST SP 800-53 y el modelo Zero Trust. La solución incluye la definición de un modelo de control de accesos basado en roles (RBAC), la implementación de revisiones periódicas de privilegios, el fortalecimiento del uso de autenticación multifactor (MFA) y la formalización de procedimientos de altas, bajas y modificaciones.

El proyecto tiene como fin reducir el riesgo asociado a accesos no autorizados, mejorar la trazabilidad y control sobre los permisos otorgados y alinear el proceso IAM con los objetivos estratégicos de seguridad de la organización.

IAM, gestión de identidades, control de accesos, RBAC, Zero Trust, ciberseguridad, gestión de riesgos.

2 Abstract

The action-research project is focused on the analysis and improvement of the Identity and Access Management (IAM) process at JFMarket S.A., a company dedicated to e-commerce. In the current context of digital transformation and the adoption of cloud services, the organization has experienced rapid growth in the number of employees, suppliers, and technological platforms, which has significantly increased the complexity of identity and access permission management.

The initial diagnosis clearly revealed deficiencies in identity lifecycle management, manual assignment of privileges, absence of periodic access reviews, and lack of segregation of duties in

critical systems. These weaknesses generate risks associated with unauthorized access, exposure of sensitive information, and potential non-compliance with data protection regulations.

Through the application of the action-research methodology, a structured analysis of the current process (AS-IS) was conducted, and an improvement proposal (TO-BE) was designed based on international best practices such as ISO 27001, NIST SP 800-53, and the Zero Trust model. The solution includes the definition of a role-based access control (RBAC) model, the implementation of periodic privilege reviews, the strengthening of multi-factor authentication (MFA), and the formalization of joiner, mover, and leaver procedures.

The project aims to reduce the risk associated with unauthorized access, improve traceability and control over granted permissions, and align the IAM process with the organization's strategic information security objectives.

Keywords: IAM, identity management, access control, RBAC, multi-factor authentication, access governance, cybersecurity.

3 Introducción

En el actual entorno de transformación digital, la gestión de identidades y accesos (Identity and Access Management IAM) se ha consolidado como uno de los pilares fundamentales de la seguridad de la información. La adopción masiva de servicios en la nube, entornos híbridos y modelos de trabajo remoto ha incrementado la complejidad en la administración de accesos, agrandando la superficie de exposición de las organizaciones (Rose et al., 2020).

Diversos marcos normativos y estándares internacionales, como ISO/IEC 27001:2022 y el marco de controles de NIST, destacan la necesidad de establecer controles robustos de autenticación, autorización y gestión del ciclo de vida de usuarios como forma esencial para garantizar la confidencialidad, integridad y disponibilidad de la información (ISO, 2022; NIST, 2020).

El proyecto de investigación-acción se centra en la identificación y mejora de deficiencias en el proceso de gestión de accesos y control de identidades en la empresa JFMarket S.A., organización dedicada al comercio electrónico. El crecimiento acelerado de la compañía y la incorporación progresiva de múltiples plataformas tecnológicas han generado debilidades en la asignación y vigilancia de privilegios, incrementando el riesgo de accesos no autorizados y posibles incumplimientos normativos.

El problema identificado se relaciona con la falta de formalización del ciclo de vida de identidades, la asignación manual de permisos, la ausencia de revisiones periódicas de accesos y la insuficiente segregación de funciones en sistemas críticos. Estas situaciones incumplen las buenas prácticas recomendadas por estándares internacionales, los cuales establecen que los privilegios deben otorgarse bajo el principio de mínimo privilegio y revisarse de forma continua (ISO, 2022).

Desde una perspectiva estratégica, la correcta gestión de identidades es un componente clave dentro del modelo Zero Trust, el cual propone verificar explícitamente cada acceso y asumir que ninguna identidad debe considerarse confiable por defecto (Rose et al., 2020). En este contexto, el proyecto busca alinear el proceso IAM con estas buenas prácticas, integrando teoría y aplicación práctica mediante un enfoque estructurado de mejora continua.

3.1 Objetivo General

Desarrollar una propuesta estructurada de mejora del proceso de gestión de accesos y control de identidades (IAM) en la empresa JFMarket S.A., orientada a reducir riesgos de accesos indebidos, fortalecer la gobernanza de identidades y alinear el proceso con estándares internacionales de seguridad de la información (ISO, 2022; NIST, 2020).

3.2 Objetivos Específicos

Para alcanzar el objetivo general, se establecen los siguientes objetivos específicos:

Realizar un diagnóstico integral del proceso IAM actual, identificando brechas de control y riesgos asociados, conforme a buenas prácticas internacionales (ISO, 2022).
Analizar las causas raíz de las deficiencias detectadas y su impacto en la seguridad de la información, considerando los principios de mínimo privilegio y segregación de funciones (NIST, 2020).
Diseñar un modelo mejorado de gestión de identidades basado en control de accesos por roles (RBAC) y principios de Zero Trust (Rose et al., 2020).
Establecer un plan de implementación con responsables, cronograma, recursos e indicadores de desempeño que permitan evaluar la efectividad de la intervención.

3.3 Metodología

El proyecto se desarrolló bajo la metodología de investigación-acción, la cual combina análisis teórico y aplicación práctica para resolver problemáticas organizacionales concretas. Este enfoque facilita la participación de los actores involucrados y promueve la mejora continua mediante ciclos iterativos de diagnóstico, planificación, acción y evaluación.
La investigación-acción resulta especialmente adecuada en proyectos de seguridad de la información, ya que permite adaptar las soluciones al contexto organizacional específico y evaluar su viabilidad operativa.
El desarrollo metodológico se estructuró en tres etapas:

1. Diagnóstico del proceso actual (AS-IS).
2. Diseño del modelo mejorado (TO-BE).
3. Definición operativa de implementación.

3.3.1 Identificación y Análisis del Problema

En la primera etapa, se realizó un análisis exhaustivo de la organización y del contexto en el cual se desarrolla el proceso afectado. Se documentó el problema identificando sus causas raíz, efectos y puntos críticos que afectaban el desempeño del proceso. Este diagnóstico inicial fue esencial para estructurar la solución y asegurar que la intervención respondiera de manera precisa a las necesidades de la organización.

El diagnóstico del proceso de gestión de identidades y accesos (IAM) se llevó a cabo mediante un enfoque mixto cualitativo y documental, apoyado en estándares internacionales de seguridad de la información.

En primer lugar, se realizó una revisión documental de las políticas internas, procedimientos existentes y registros relacionados con la gestión de accesos. Tras el primer paso, se llevaron a cabo entrevistas semiestructuradas con personal del área de Tecnología de la Información y Recursos Humanos, con el fin de comprender el flujo real del proceso de altas, bajas y modificaciones de usuarios.

Adicionalmente, se efectuó un análisis de muestras de cuentas activas en sistemas críticos (ERP, CRM y plataforma e-commerce) para identificar posibles cuentas huérfanas, privilegios excesivos y desviaciones respecto al principio de mínimo privilegio.

Para identificar las causas raíz del problema, se aplicó la técnica del diagrama de Ishikawa, permitiendo clasificar los factores contribuyentes en categorías como procesos, tecnología, personas

y gobierno. Finalmente, se realizó una evaluación para comparar los controles de acceso establecidos en la norma ISO/IEC 27001:2022 y en NIST SP 800-53 (ISO, 2022; NIST, 2020), con el objetivo de identificar brechas respecto a buenas prácticas internacionales.

Este enfoque metodológico permitió obtener una visión integral del estado actual del proceso (AS-IS) y establecer una base objetiva para el diseño de la propuesta de mejora.

3.3.2 Planificación de la Solución

En la segunda etapa, se desarrolló un plan de acción detallado que incluyó la definición de objetivos específicos y una serie de actividades que permitiría mitigar o resolver el problema identificado. Esta fase incluyó el diseño de una estrategia de ejecución organizada y estructurada que facilitara el logro de los objetivos propuestos y maximizara la eficiencia del proceso intervenido.
En el contexto del proceso de gestión de identidades y accesos (IAM), la planificación se fundamentó en buenas prácticas internacionales en materia de control de accesos (ISO, 2022; NIST, 2020). El plan contempló las siguientes líneas de acción:

- Definición de un modelo de control de accesos basado en roles (RBAC), alineado con el principio de mínimo privilegio.
- Formalización del procedimiento Joiner-Mover-Leaver (JML) para la gestión del ciclo de vida de usuarios.
- Implementación obligatoria de autenticación multifactor (MFA) en sistemas críticos.
- Diseño de una matriz de segregación de funciones.
- Establecimiento de revisiones periódicas de privilegios.
- Evaluación de la posible adopción de una herramienta centralizada de gobierno de identidades (IGA).

La planificación detallada de actividades, responsables y recursos fue clave para asegurar una implementación precisa y efectiva, reduciendo riesgos asociados a accesos no autorizados y mejorando la trazabilidad del proceso IAM.

3.3.2.1 Definición de Alcance y Recursos

La tercera etapa se enfocó en delimitar el alcance de la intervención y los recursos necesarios. Se establecieron responsables para cada actividad, y se elaboró un cronograma de ejecución para controlar el avance de la implementación. Asimismo, se desarrolló un presupuesto que detalló los costos asociados a cada fase, permitiendo optimizar la asignación de recursos. Esta fase aseguró que todas las variables críticas estuvieran alineadas para una ejecución sin interrupciones.
En el contexto de este proyecto, el alcance de la intervención se definió sobre el proceso de gestión de identidades y accesos (IAM) de la empresa JFMarket S.A., considerando como objeto principal de mejora los sistemas catalogados como críticos para la operación del negocio: la plataforma de comercio electrónico, el sistema ERP, el CRM y el entorno

cloud corporativo. Quedaron fuera de alcance, en esta fase, sistemas de baja criticidad y aplicaciones temporales de uso departamental.

- Para la ejecución de la intervención se identificaron los siguientes grupos de interés y responsables:
- Área de Seguridad de la Información: liderazgo funcional del proyecto, definición de políticas y controles de seguridad.
- Área de Tecnología de la Información: implementación técnica de los cambios en sistemas y directorios de usuarios.
- Recursos Humanos: gestión de la información relativa al ciclo de vida de los empleados (altas, cambios de puesto y bajas).
- Responsables de proceso de cada área de negocio: validación de los roles y permisos necesarios para el desempeño de funciones.

En cuanto a los recursos, se consideraron:

- Recursos humanos: un equipo multidisciplinar compuesto por un responsable de seguridad, un administrador de sistemas, un representante de RRHH y, cuando fue necesario, un responsable de área usuaria.
- Recursos tecnológicos: uso del directorio corporativo existente, herramientas de gestión de accesos, sistemas de registro de eventos (logs) y, potencialmente, soluciones de gobierno de identidades (IGA) disponibles en la organización.
- **Recursos económicos:** presupuesto asociado principalmente a horas de dedicación del personal implicado, posibles licencias adicionales y actividades de formación interna.

Se estableció un cronograma estimado de cuatro meses, estructurado en fases: diagnóstico detallado, diseño del modelo mejorado, implementación piloto en un subconjunto de sistemas y despliegue progresivo al resto del entorno. Cada fase incluyó hitos de validación y puntos de control para revisar el avance del proyecto y ajustar las acciones cuando fuera necesario.

Asimismo, se definieron indicadores clave de desempeño (KPIs) para evaluar el impacto de la intervención, entre ellos:

- Porcentaje de cuentas huérfanas identificadas y eliminadas.
- Tiempo medio de revocación de accesos tras la baja de un empleado.
- Porcentaje de usuarios con autenticación multifactor (MFA) habilitada en sistemas críticos.
- Nivel de cumplimiento de revisiones periódicas de privilegios.

La definición clara de alcance, responsables, recursos y métricas permitió alinear la intervención con las recomendaciones de marcos internacionales como ISO/IEC 27001:2022 y NIST SP 800-53 (ISO, 2022; NIST, 2020), asegurando que la mejora del proceso IAM fuera realista, medible y sostenible en el tiempo.

4 Identificación y descripción de un problema al interior de la organización

En la empresa JFMarket S.A., dedicada al comercio electrónico, se ha identificado un problema relevante en el proceso de gestión de accesos y control de identidades (IAM), perteneciente al área de Tecnología de la Información. Este proceso es crítico, ya que garantiza que únicamente las personas autorizadas accedan a los sistemas, aplicaciones y datos necesarios para el desempeño de sus funciones.
El crecimiento sostenido de la organización, la incorporación de nuevas plataformas tecnológicas (ERP, CRM, entorno cloud y plataforma de ventas online) y el incremento del número de empleados y proveedores han incrementado la complejidad del control de accesos. Sin embargo, el proceso IAM no ha evolucionado al mismo ritmo, lo que ha generado debilidades estructurales que impactan directamente en la seguridad de la información.
El problema central identificado consiste en la ausencia de un modelo formalizado y controlado de gestión del ciclo de vida de identidades, lo que ha derivado en asignaciones manuales de permisos, acumulación de privilegios innecesarios y falta de revisiones periódicas de accesos. Esta situación incrementa el riesgo de accesos no autorizados, incumplimiento normativo y posibles incidentes de seguridad.
El impacto del problema se refleja en:

- Incremento del riesgo operativo y reputacional.
- Dificultades en procesos de auditoría interna.
- Exposición a posibles brechas de seguridad.
- Falta de trazabilidad en la asignación de privilegios.

Desde la perspectiva de estándares internacionales, esta situación contraviene el principio de mínimo privilegio y las recomendaciones sobre gestión de accesos establecidas en ISO/IEC 27001:2022 (ISO, 2022) y NIST SP 800-53 (NIST, 2020).

4.1 Descripción de la empresa a intervenir

JFMarket S.A. es una empresa de comercio electrónico especializada en la venta de productos tecnológicos a nivel nacional. Opera principalmente a través de una plataforma digital propia y cuenta con aproximadamente 150 empleados distribuidos en áreas de ventas, logística, atención al cliente, finanzas y tecnología.

La empresa utiliza múltiples sistemas de información, entre los que destacan:

• Plataforma e-commerce.
• Sistema ERP para gestión financiera y logística.
• CRM para gestión de clientes.
• Infraestructura en la nube para almacenamiento y servicios corporativos.

Debido a la naturaleza digital del negocio, la protección de la información y la correcta gestión de accesos constituyen un elemento estratégico para la continuidad operativa.

4.1.1 Misión

La misión de JFMarket S.A. es ofrecer productos tecnológicos a través de una plataforma de comercio electrónico segura, eficiente e innovadora, proporcionando a sus clientes una experiencia de compra confiable, ágil y transparente. La organización busca satisfacer las necesidades del mercado mediante el uso de soluciones digitales avanzadas, garantizando altos estándares de calidad, disponibilidad del servicio y protección de la información.

Asimismo, la empresa asume como parte fundamental de su misión la protección de los datos personales de clientes, empleados y socios comerciales, reconociendo que la seguridad de la información es un elemento estratégico para la sostenibilidad del negocio. En este sentido, JFMarket S.A. se compromete a implementar controles técnicos y organizativos adecuados que permitan preservar la confidencialidad, integridad y disponibilidad de la información en todos sus procesos.

La organización promueve una cultura corporativa orientada a la mejora continua, la innovación tecnológica y el cumplimiento normativo, integrando la gestión de riesgos y la ciberseguridad como componentes esenciales dentro de su modelo de gobierno. De esta manera, busca no solo alcanzar objetivos comerciales, sino también consolidar la confianza de sus clientes y fortalecer la reputación en el mercado digital.

En coherencia con este enfoque, la correcta gestión de identidades y accesos (IAM) se considera un proceso clave dentro de la misión organizacional, ya que permite asegurar que el acceso a los sistemas y datos corporativos se otorgue únicamente a usuarios autorizados y bajo criterios de control adecuados, reduciendo riesgos operativos y de seguridad.

4.1.2 Visión

La visión de JFMarket S.A. es consolidarse como una empresa líder en el sector del comercio electrónico a nivel nacional, destacándose por su excelencia operativa, innovación tecnológica y compromiso con la seguridad digital. La organización aspira a ser reconocida no solo por la calidad de sus productos y servicios, sino también por la confianza que genera en sus clientes, colaboradores y socios estratégicos.
En un entorno caracterizado por la creciente digitalización y el aumento de amenazas cibernéticas, JFMarket S.A. proyecta evolucionar hacia un modelo de negocio altamente resistente, capaz de adaptarse a cambios tecnológicos y regulatorios de manera ágil y estructurada. Para ello, la compañía busca fortalecer continuamente sus tecnologías de la información, integrando la gestión de riesgos y la ciberseguridad como elementos estratégicos dentro de su planificación corporativa.
La organización visualiza un futuro en el que sus procesos críticos estén soportados por controles automatizados, métricas de desempeño claras y un enfoque preventivo frente a riesgos de seguridad.

En este escenario, la gestión de identidades y accesos (IAM) desempeña un papel fundamental, ya que constituye uno de los principales mecanismos de control para proteger activos digitales y garantizar la continuidad del negocio.
Asimismo, JFMarket S.A. aspira a alcanzar niveles avanzados de madurez en seguridad de la información, alineándose con estándares internacionales y buenas prácticas reconocidas, lo que le permitirá fortalecer su reputación en el mercado, mejorar su competitividad y asegurar el cumplimiento de requisitos normativos aplicables.

4.1.3 Mapa de procesos

JFMarket S.A. estructura su gestión organizacional bajo un enfoque basado en procesos, permitiendo identificar claramente las actividades estratégicas, misionales y de apoyo que garantizan el cumplimiento de sus objetivos corporativos. Este enfoque facilita la asignación de responsabilidades, el control operativo y la mejora continua.
El mapa de procesos de la organización se divide en tres grandes categorías:

1. Procesos estratégicos

Son aquellos orientados a la dirección, planificación y control global de la organización. Incluyen:

- Dirección estratégica.
- Planificación corporativa.
- Gestión de riesgos.
- Gobierno de Tecnologías de la Información.
- Cumplimiento normativo y auditoría interna.

Estos procesos definen las políticas y lineamientos que impactan transversalmente a toda la organización, incluyendo las directrices relacionadas con la seguridad de la información.

2. Procesos misionales (clave)

Corresponden a las actividades directamente relacionadas con la generación de valor y la operación principal del negocio. Incluyen:

- Gestión de la plataforma de comercio electrónico.
- Gestión de ventas.
- Atención al cliente.
- Gestión de pedidos y logística.
- Gestión de proveedores.

Estos procesos dependen de manera crítica de la disponibilidad y seguridad de los sistemas de información.

3. Procesos de apoyo

Son aquellos que brindan soporte a los procesos estratégicos y misionales, asegurando el correcto funcionamiento de la organización. Incluyen:

- Recursos Humanos.
- Finanzas y contabilidad.
- Infraestructura tecnológica.
- Soporte técnico.
- Seguridad de la información.

Dentro de esta categoría se encuentra el proceso de **gestión de identidades y accesos (IAM)**, el cual depende funcionalmente del área de Tecnología de la Información y de Seguridad de la Información.
El proceso IAM tiene carácter transversal, ya que interactúa con:

- Recursos Humanos, para la gestión de altas, cambios y bajas de personal.
- Todas las áreas de negocio, para la asignación de roles y privilegios.
- Sistemas tecnológicos críticos, como ERP, CRM y plataforma e-commerce.

Debido a su naturaleza cruzada y su impacto directo en la protección de activos digitales, el proceso de gestión de accesos se considera un proceso de apoyo crítico, ya que su correcta ejecución influye directamente en la confidencialidad, integridad y disponibilidad de la información corporativa.
La falta de madurez en este proceso, como se evidenció en el diagnóstico, genera riesgos que afectan tanto a los procesos misionales como a los estratégicos, lo que justifica la necesidad de intervención y mejora estructurada.

4.1.4 Descripción del proceso a intervenir

El proceso para intervenir corresponde a la gestión de identidades y accesos (Identity and Access Management – IAM) dentro del área de Tecnología de la Información de JFMarket S.A. Este proceso tiene como finalidad garantizar que el acceso a los sistemas de información y activos digitales de la organización sea otorgado exclusivamente a usuarios autorizados, bajo criterios definidos y controlados.
Actualmente, el proceso IAM comprende las siguientes actividades principales:

1. Alta de usuarios (joiners):
Cuando un nuevo empleado se incorpora a la organización, el área de Recursos Humanos notifica al área de TI mediante correo electrónico. Posteriormente, el administrador de sistemas crea manualmente las cuentas en el directorio corporativo y en los sistemas requeridos (ERP, CRM, plataforma e-commerce, correo corporativo, entre otros). La asignación de permisos se realiza en función del cargo informado, aunque no existe una matriz formal de roles documentada.

2. Modificación de accesos (Mover):

En caso de cambio de puesto o reasignación de funciones, el responsable del área solicita por correo la modificación de accesos. Sin embargo, el proceso no contempla una revisión sistemática de los privilegios previamente asignados, lo que genera acumulación progresiva de permisos.

3. Baja de usuarios (Leaver):

Cuando un empleado finaliza su relación contractual, Recursos Humanos comunica la baja al área de TI. La desactivación de cuentas depende de la notificación oportuna y no existe un mecanismo automatizado que garantice la revocación inmediata de todos los accesos.

4. Gestión de privilegios:

La asignación de permisos se realiza de manera individual y manual. No se aplica formalmente el principio de mínimo privilegio ni se dispone de una matriz de segregación de funciones definida. Tampoco se cuenta con perfiles preconfigurados basados en roles (RBAC).

5. Supervisión y revisión:

No existe un procedimiento formal de revisión periódica de accesos. Las auditorías de permisos se realizan únicamente cuando son requeridas por procesos internos o externos de revisión.

Desde una perspectiva técnica, el proceso se caracteriza por:

- Ausencia de automatización en el ciclo de vida de identidades.
- Falta de integración estructurada entre Recursos Humanos y TI.
- Dependencia de comunicaciones informales.
- Escasa trazabilidad documental.
- Carencia de indicadores de desempeño (KPIs) asociados al proceso.

El modelo actual puede clasificarse como un esquema reactivo y manual, con bajo nivel de madurez en términos de gobierno de identidades. Esta situación genera vulnerabilidades relacionadas con accesos indebidos, privilegios excesivos y cuentas huérfanas, afectando la postura de seguridad global de la organización.

Debido a su carácter transversal y su impacto directo en la protección de activos críticos, la mejora de este proceso se considera prioritaria dentro de la estrategia de fortalecimiento de la seguridad de la información en JFMarket S.A.

4.1.5 Descripción del problema que presenta el proceso

El análisis del proceso de gestión de identidades y accesos (IAM) en JFMarket S.A. evidenció una serie de deficiencias estructurales que comprometen la eficacia del control de accesos dentro de la organización. El problema central identificado consiste en la ausencia de un modelo formal, estandarizado y automatizado para la gestión del ciclo de vida de identidades, lo que genera inconsistencias en la asignación, modificación y revocación de permisos.

Durante el diagnóstico se identificaron las siguientes situaciones críticas:

- Existencia de cuentas activas asociadas a exempleados (cuentas huérfanas).
- Usuarios con privilegios administrativos superiores a los estrictamente necesarios para el desempeño de sus funciones.
- Ausencia de revisiones periódicas formales de accesos.
- Falta de una matriz documentada de roles y segregación de funciones.
- Dependencia de solicitudes informales vía correo electrónico para la asignación de permisos.

Como resultado de una revisión realizada sobre un subconjunto representativo de 100 cuentas activas en sistemas críticos, se observó que aproximadamente un 18 % presentaba privilegios superiores a los requeridos, y un 6 % correspondía a cuentas que no contaban con validación reciente por parte de un responsable de área. Aunque estos datos no evidencian necesariamente un incidente activo, sí reflejan un nivel de exposición que incrementa el riesgo organizacional.

Desde la perspectiva de análisis de causa raíz, se identificaron los siguientes factores contribuyentes:

1. Procesos: inexistencia de un procedimiento formalizado Joiner-Mover - Leaver (JML).
2. Tecnología: ausencia de herramienta centralizada de gobierno de identidades (IGA).
3. Personas: falta de concienciación sobre el principio de mínimo privilegio.
4. Gobierno: inexistencia de indicadores de desempeño y controles de revisión periódica.

El impacto del problema puede analizarse en relación con la triada de seguridad de la información:

- Confidencialidad: riesgo de acceso no autorizado a información financiera, datos personales de clientes y estrategias comerciales.
- Integridad: posibilidad de modificación indebida de registros en sistemas críticos.
- Disponibilidad: potencial uso malintencionado de privilegios elevados que afecte la operación del negocio.

Adicionalmente, la situación identificada contraviene buenas prácticas establecidas en estándares internacionales. ISO/IEC 27001:2022 establece la necesidad de controlar estrictamente los derechos de acceso y revisar periódicamente los privilegios otorgados (ISO, 2022). De igual forma, NIST SP 800-53 recomienda aplicar el principio de mínimo privilegio y realizar monitoreo continuo de accesos (NIST, 2020).
Desde una perspectiva de gestión de riesgos, el escenario actual puede clasificarse como de riesgo medio-alto, dado que la probabilidad de que ocurra un incidente relacionado con accesos indebidos es significativa debido a la falta de controles preventivos automatizados, mientras que el impacto potencial es alto por tratarse de sistemas críticos para la operación y reputación de la empresa.
En consecuencia, la mejora del proceso IAM no solo responde a una necesidad operativa, sino que constituye una acción estratégica para fortalecer la postura de seguridad, reducir la exposición a amenazas internas y externas, y alinearse con estándares internacionales de gobernanza de la seguridad de la información.

5 Establecimiento de planes de acción para la solución del problema

A partir de los puntos realizados sobre el proceso de gestión de identidades y accesos (IAM) en JFMarket S.A., se evidenció un nivel de madurez bajo, caracterizado por procedimientos manuales, ausencia de formalización del ciclo de vida de identidades, carencia de revisiones periódicas y falta de aplicación sistemática del inicio de mínimo privilegio.
El escenario que identificamos implica un nivel de riesgo medio-alto para la organización, afectando directamente la confidencialidad, integridad y disponibilidad de la información corporativa. En este contexto, el presente plan de acción tiene como finalidad transformar el modelo actual (AS-IS) en un modelo objetivo (TO-BE) alineado con estándares internacionales y principios de gobierno de identidades.
El plan se estructura en cuatro componentes principales:

1. Definición estratégica de objetivos.
2. Diseño integral de la solución.
3. Secuencia estructurada de implementación.
4. Identificación de recursos necesarios.

La intervención se ve como un proceso progresivo de madurez, priorizando controles de alto impacto en reducción de riesgo y viabilidad operativa.

5.1 Establecimiento de objetivos

El establecimiento de objetivos inicia el punto de partida del plan de acción para la mejora del proceso de gestión de identidades y accesos (IAM) en JFMarket S.A. Estos objetivos se formulan a partir del diagnóstico realizado, el análisis de causas raíz y la evaluación del nivel de riesgo que identificamos en el estado actual (AS-IS).
Considerando que el problema central aparece en la ausencia de un modelo formal y controlado de gestión del ciclo de vida de identidades, los objetivos se orientan a reducir el riesgo asociado a accesos indebidos, fortalecer la gobernanza de identidades y alinear el proceso con estándares internacionales como ISO/IEC 27001 2022 y NIST SP 800 53.
Los objetivos definidos responden a los siguientes criterios metodológicos:

- Enfoque basado en riesgo.
- Principio de mínimo privilegio.
- Segregación de funciones.
- Medición mediante indicadores verificables.
- Horizonte temporal definido (cuatro meses).
- Sostenibilidad y mejora continua.

- Objetivo General

Implementar un modelo formalizado, estructurado y medible de gestión de identidades y accesos (IAM) en JFMarket S.A., que permita reducir significativamente los riesgos asociados a privilegios excesivamente peligrosos, cuentas huérfanas y falta de trazabilidad, garantizando el cumplimiento de buenas prácticas internacionales en materia de control de accesos.

- Objetivos Específicos

1. Formalizar el proceso Joiner-Mover-Leaver (JML): Diseñar, documentar e implementar un procedimiento oficial para la gestión del ciclo de vida de identidades que incluya flujos de aprobación, validación y registro de evidencias, reduciendo la dependencia de comunicaciones informales.
2. Reducir privilegios excesivos detectados en sistemas críticos, Disminuir al menos en un 70 % los casos de usuarios con permisos superiores solo a los necesarios, identificados durante el diagnóstico (18 % del total analizado).
3. Eliminar cuentas huérfanas: Identificar y deshabilitar el 100 % de cuentas asociadas a exempleados o sin validación activa en sistemas críticos.
4. Implementar un modelo de control de accesos basado en roles (RBAC), Diseñar una matriz de roles corporativa que cubra el 100 % de las funciones organizativas en ERP, CRM, plataforma e-commerce y entorno cloud.
5. Establecer revisiones periódicas obligatorias de accesos, Institucionalizar revisiones trimestrales de privilegios con un nivel de cumplimiento mínimo del 95 %, generando evidencia documental para auditoría.

6. Fortalecer los mecanismos de autentificación, Alcanzar el 100 % de implementación de autenticación multifactor (MFA) en sistemas críticos y accesos privilegiados.
7. Reducir el tiempo medio de revocación de accesos tras una baja laboral, Garantizar que la desactivación de cuentas se realice en un plazo máximo de 24 horas desde la notificación de Recursos Humanos.
8. Definir indicadores clave de desempeño (KPIs) del proceso IAM, Establecer métricas formales que permitan evaluar la eficacia del proceso y su evolución en el tiempo.

- Alineación estratégica de los objetivos

Los objetivos establecidos se encuentran alineados con:

- La misión para proteger la información y garantizar la continuidad operativa.
- La visión de evolucionar hacia un modelo digital resiliente.
- Las recomendaciones de ISO/IEC 27001:2022 respecto al control y revisión de derechos de acceso.
- Los controles AC-2 (Account Management) y AC-6 (Least Privilege) de NIST SP 800-53.
- Los principios del modelo Zero Trust, que establecen la verificación continua y la eliminación de confianza implícita.

- Relación entre objetivos y reducción del riesgo

Cada objetivo contribuye directamente a mitigar riesgos identificados en el análisis de impacto:

- La formalización del JML reduce la probabilidad de cuentas huérfanas.
- El modelo RBAC disminuye el riesgo de abuso de privilegios.
- La segregación de funciones mitiga riesgos de fraude interno.
- La MFA reduce la probabilidad de accesos no autorizados por compromiso de credenciales.
- Las revisiones periódicas disminuyen la exposición acumulativa en el tiempo.

Desde una perspectiva de gestión de riesgos, se espera una reducción significativa tanto en la probabilidad de ocurrencia como en la superficie de exposición ante amenazas internas y externas.

- Indicadores de medición asociados a los objetivos

Para asegurar que los objetivos sean evaluables, se establecen indicadores cuantificables:

- % de cuentas huérfanas eliminadas.
- % de reducción de privilegios excesivos.
- Tiempo medio de revocación de accesos.
- % de usuarios con MFA habilitado.
- % de cumplimiento en revisiones trimestrales.
- Número de incidencias relacionadas con accesos indebidos.

Estos indicadores permitirán comparar el estado inicial (AS-IS) con el estado posterior a la intervención (TO-BE), proporcionando evidencia objetiva del impacto del proyecto.

5.2 Descripción de la solución

La solución propuesta para la mejora del proceso de gestión de identidades y accesos (IAM) en JFMarket S.A. consiste en el paso de un modelo operativo manual, reactivo y poco formalizado hacia un modelo estructurado de gobierno de identidades, basado en principios de mínimo privilegio, segregación de funciones, automatización progresiva y supervisión continua.

El modelo objetivo (TO-BE) ha sido diseñado a partir de las brechas identificadas en el diagnóstico AS-IS y alineado con buenas prácticas internacionales recogidas en ISO/IEC 27001:2022 y NIST SP 800-53, así como con el enfoque conceptual del modelo Zero Trust, que establece la necesidad de verificar explícitamente cada acceso y eliminar la confianza implícita en identidades internas.

La solución se estructura en cinco componentes integrados que actúan de manera complementaria.

1. Formalización del gobierno del proceso IAM

La primera dimensión de la solución consiste en fortalecer el marco de gobierno del proceso IAM, corrigiendo la debilidad identificada en el análisis de causa raíz relacionada con la falta de control y supervisión estructurada.
Se propone:

- Actualizar la política corporativa de control de accesos.
- Designar formalmente un responsable del proceso IAM (propietario del proceso).
- Definir roles y responsabilidades claras entre Seguridad de la Información, Tecnología, Recursos Humanos y responsables funcionales.
- Establecer un comité de revisión trimestral de accesos.

Este componente permite dotar al proceso de una base organizativa sólida, garantizando coherencia en la toma de decisiones y rendición de cuentas.

2. Implementación formal del proceso Joiner-Mover-Leaver (JML)

La solución contempla el diseño e implementación de un procedimiento formal y documentado para la gestión del ciclo de vida de identidades, eliminando la dependencia de comunicaciones informales vía correo electrónico.
El proceso JML incluirá:

- Joiner (Alta)
- Solicitud estructurada mediante formulario oficial.
- Validación obligatoria por responsable jerárquico.
- Asignación automática de accesos basada en rol.
- Activación obligatoria de autenticación multifactor.
- Registro documental de la aprobación.
- Mover (Cambio de funciones)
- Revisión completa de privilegios previamente asignados.
- Eliminación de accesos incompatibles con el nuevo rol.

- Validación formal de nuevos permisos.
- Registro de modificación en sistema de trazabilidad.
- Leaver (Baja)
- Notificación inmediata desde Recursos Humanos.
- Revocación centralizada de accesos en un plazo máximo de 24 horas.
- Desactivación en todos los sistemas críticos.
- Evidencia documental de cierre completo de cuenta.

Este rediseño reduce significativamente el riesgo de cuentas huérfanas y acumulación progresiva de privilegios.

3. Implementación del modelo de control de accesos basado en roles (RBAC)

Uno de los pilares fundamentales de la solución es la implementación de un modelo RBAC que sustituya la asignación manual e individualizada de permisos.
El modelo RBAC incluirá:

- Identificación y clasificación de roles organizativos por área.
- Definición de permisos mínimos necesarios para cada rol.
- Creación de perfiles estandarizados en ERP, CRM, plataforma e-commerce y entorno cloud.
- Restricción de asignaciones individuales excepcionales, sujetas a aprobación formal.
- Control diferenciado para cuentas privilegiadas o administrativas.

Este modelo permite:

- Reducir privilegios excesivos (18 % detectados en el diagnóstico).
- Facilitar auditorías.
- Mejorar la coherencia en la asignación de accesos.
- Simplificar futuras incorporaciones o cambios de puesto.

4. Definición de matriz de segregación de funciones (SoD)

La solución incorpora la creación de una matriz formal de segregación de funciones que identifique combinaciones de accesos incompatibles en sistemas críticos.
Por ejemplo:

- En ERP: creación de proveedores vs aprobación de pagos.
- En CRM: modificación de datos críticos vs validación de contratos.
- En entorno cloud: configuración de infraestructura vs revisión de auditoría.

La matriz permitirá implementar controles preventivos o detectar según la criticidad del riesgo identificado, mitigando la posibilidad de fraude interno o errores operativos graves.

5. Fortalecimiento técnico y adopción de principios Zero Trust

Desde la perspectiva tecnológica, la solución incorpora:

- Implementación obligatoria de MFA en sistemas críticos.
- Revisión y monitoreo de accesos privilegiados.
- Registro centralizado de eventos de autenticación.
- Restricción de accesos administrativos desde entornos no confiables.

- Evaluación futura de una herramienta de Gobierno y Administración de Identidades (IGA) para automatización avanzada.

Este componente refuerza la postura de seguridad ante amenazas como:

- Compromiso de credenciales.
- Movimientos laterales dentro de la red.
- Escalada de privilegios.

- Integración de la solución en el modelo organizacional

La propuesta no se limita a la dimensión técnica, sino que integra:

- Cambios organizativos (gobierno).
- Cambios procedimentales (JML).
- Cambios estructurales (RBAC).
- Cambios de control (revisiones periódicas).
- Cambios culturales (concienciación sobre mínimo privilegio).

De esta forma, la solución aborda las cuatro categorías de causa raíz identificadas en el diagnóstico: procesos, tecnología, personas y gobierno.

- Estado objetivo (TO-BE) esperado

Tras la implementación de la solución, el proceso IAM de JFMarket S.A. evolucionará hacia un modelo caracterizado por:

- Accesos otorgados exclusivamente por rol definido.
- Revocación controlada y trazable.
- Eliminación de cuentas huérfanas.
- Revisión periódica institucionalizada.
- Supervisión formal y medición mediante KPIs.
- Mayor alineación con ISO 27001:2022 y NIST SP 800-53.

En términos de madurez, el proceso pasará de un nivel reactivo-manual a un nivel formalizado y gobernado, con bases sólidas para una futura automatización completa mediante herramientas IGA.

5.3 Secuencia de actividades para ejecución de la solución

La implementación del modelo mejorado de gestión de identidades y accesos (IAM) en JFMarket S.A. se desarrollará mediante una secuencia construida a través de actividades organizadas en fases, siguiendo un enfoque progresivo y repetido basado en el ciclo de mejora continua (PDCA: Plan-Do-Check-Act).

La secuencia ha sido diseñada considerando:

- La criticidad de los sistemas involucrados.
- La necesidad de minimizar el impacto operativo.
- La priorización basada en riesgo.
- La viabilidad técnica y organizativa.
- El cronograma general de cuatro meses definido en el alcance del proyecto.

- Fase 1: Planificación detallada y diseño normativo (Mes 1)

Esta fase corresponde a la estructuración formal del modelo TO-BE.
Actividades principales:

1. Nombramiento formal del responsable del proceso IAM.
2. Actualización y aprobación de la política de control de accesos.
3. Documentación oficial del procedimiento Joiner-Mover-Leaver (JML).
4. Identificación y clasificación de roles organizativos por área.
5. Diseño preliminar de la matriz RBAC.
6. Elaboración de la matriz de segregación de funciones (SoD).
7. Definición formal de indicadores clave de desempeño (KPIs).
8. Aprobación ejecutiva del modelo diseñado.

Resultado esperado: Marco normativo y estructural del nuevo modelo IAM aprobado por Dirección.

Riesgo mitigado: Falta de gobierno y ambigüedad en responsabilidades.

- Fase 2: Implementación técnica piloto (Mes 2)

En esta fase se realiza una implementación controlada en un sistema crítico (ERP), permitiendo validar el modelo antes de su despliegue completo.
Actividades principales:

1. Configuración técnica de roles RBAC en ERP.
2. Revisión y depuración inicial de privilegios excesivos.
3. Identificación y eliminación de cuentas huérfanas detectadas.
4. Activación obligatoria de MFA en ERP.
5. Implementación del procedimiento JML en entorno piloto.
6. Capacitación inicial al equipo de TI y responsables de área.
7. Evaluación de incidencias o ajustes necesarios.

Resultado esperado: Validación operativa del modelo RBAC y del proceso JML en entorno controlado.
Riesgo mitigado: Errores de diseño y resistencia operativa temprana.

- Fase 3: Despliegue progresivo en sistemas críticos (Mes 3)

Tras la validación del piloto, se extiende el modelo a los demás sistemas críticos: CRM, plataforma e-commerce y entorno cloud.
Actividades principales:

1. Configuración de roles en CRM y plataforma e-commerce.
2. Aplicación de la matriz de segregación de funciones.
3. Eliminación de privilegios no alineados con el nuevo modelo.
4. Implementación completa de MFA en todos los sistemas críticos.
5. Primera revisión formal trimestral de accesos.
6. Documentación de evidencias de certificación.
7. Sesiones de concienciación sobre mínimo privilegio.

Resultado esperado: Modelo RBAC y controles de autenticación implementados en el 100 % de sistemas críticos.
Riesgo mitigado: Exposición acumulativa por privilegios heredados.

- Fase 4: Evaluación, medición y consolidación (Mes 4)

Esta fase permite verificar la efectividad de la intervención y consolidar el nuevo modelo como práctica institucional.
Actividades principales:

1. Medición de KPIs definidos.
2. Comparativa cuantitativa entre estado AS-IS y TO-BE.
3. Análisis de reducción de privilegios excesivos.
4. Verificación de eliminación total de cuentas huérfanas.
5. Evaluación del tiempo medio de revocación de accesos.
6. Elaboración de informe de resultados.
7. Evaluación de viabilidad técnica y económica de herramienta IGA.
8. Presentación de resultados a Dirección.

Resultado esperado: Informe final de mejora del proceso IAM con evidencias objetivas de reducción de riesgo.
Riesgo mitigado: Falta de medición y pérdida de sostenibilidad del cambio.

- Dependencias y orden lógico de ejecución

La secuencia responde a una lógica de dependencias:

- No es posible implementar RBAC sin haber definido previamente roles y política.
- No se pueden realizar revisiones formales sin haber estandarizado el proceso JML.
- No se puede medir mejora sin establecer KPIs desde la fase inicial.
- La automatización futura (IGA) requiere previamente un modelo formalizado.

Este orden asegura coherencia estructural y evita reprocesos.

- Factores críticos de éxito

Durante la ejecución se consideran como factores críticos:

- Compromiso de la Dirección.
- Coordinación efectiva entre RRHH y TI.
- Participación activa de responsables funcionales.
- Comunicación interna clara sobre cambios.
- Seguimiento periódico del cronograma.

- Riesgos del proyecto y medidas de mitigación

Durante la implementación pueden presentarse riesgos como:

1. Resistencia al cambio por parte de usuarios.
2. Sobrecarga operativa en el área de TI.
3. Dificultades técnicas en configuración de roles.
4. Retrasos en validaciones por parte de responsables.

Para mitigarlos se propone:

- Comunicación temprana del proyecto.
- Capacitación básica en seguridad.
- Implementación progresiva y piloto previo.
- Seguimiento semanal del avance.

- Resultado global esperado de la ejecución

Al finalizar la secuencia de actividades, el proceso IAM de JFMarket S.A. deberá presentar:

- Modelo RBAC formalizado.
- Proceso JML documentado y operativo.
- Eliminación de cuentas huérfanas.
- Reducción significativa de privilegios excesivos.
- MFA implementado en sistemas críticos.
- Revisiones periódicas institucionalizadas.
- Indicadores activos de desempeño.

En términos de madurez organizacional, la organización evolucionará desde un modelo reactivo hacia un modelo formalizado, gobernado y medible, con bases sólidas para futuras automatizaciones.

5.4 Descripción de recursos necesarios para la ejecución de la solución

La correcta implementación del plan de mejora del proceso de gestión de identidades y accesos (IAM) en JFMarket S.A. requiere la asignación coordinada de recursos humanos, tecnológicos, económicos y organizativos. Dado que el proyecto se basa principalmente en la formalización, estructuración y optimización de capacidades ya existentes, la inversión inicial es mediana, aunque requiere compromiso institucional y dedicación técnica especializada.

Los recursos necesarios se clasifican en cinco categorías principales:

1. Recursos Humanos

El éxito del proyecto depende fundamentalmente de la participación de un equipo multidisciplinar.

a) Responsable de Seguridad de la Información (Project Lead)

- Liderazgo estratégico del proyecto.
- Definición de políticas y controles.
- Supervisión del cumplimiento normativo.
- Seguimiento de indicadores y reporte a Dirección.

b) Administrador de Sistemas / Equipo TI

- Configuración técnica de roles RBAC.
- Implementación de MFA.
- Depuración de cuentas huérfanas.
- Gestión técnica del directorio corporativo.

c) Representante de Recursos Humanos

- Notificación formal de altas, bajas y cambios.
- Integración del proceso JML con el ciclo laboral.
- Validación de información contractual.

d) Responsables funcionales de área

- Definición de permisos mínimos necesarios por puesto.
- Certificación trimestral de accesos.
- Validación de solicitudes excepcionales.

e) Consultor externo especializado (opcional)

- Asesoramiento en diseño de modelo RBAC avanzado.
- Evaluación técnica de herramienta IGA.
- Revisión de alineación con estándares internacionales.

Se estima que el proyecto requerirá una dedicación parcial del equipo durante los cuatro meses de ejecución, sin necesidad de contratación adicional permanente.

2. Recursos Tecnológicos

El proyecto aprovecha en gran medida la infraestructura tecnológica existente, optimizando su configuración.
Infraestructura actual a utilizar:

- Directorio corporativo (Active Directory o equivalente).
- Sistemas críticos: ERP, CRM, plataforma e-commerce y entorno cloud.
- Herramientas actuales de autenticación.
- Sistemas de registro de eventos (logs).
- Herramienta de ticketing o gestión de solicitudes.

Recursos tecnológicos adicionales o fortalecidos:

- Licencias adicionales de autenticación multifactor (si fuese necesario ampliar cobertura).
- Herramientas de reporting para revisiones periódicas.
- Evaluación futura de una herramienta de Gobierno y Administración de Identidades (IGA).

El proyecto no requiere reemplazo de infraestructura, sino reconfiguración estructurada y fortalecimiento de controles.

3. Recursos Económicos

El impacto económico del proyecto se concentra principalmente en horas de dedicación interna y posibles licencias adicionales.
Los costos estimados incluyen:

1. Horas de trabajo del equipo interno.
2. Capacitación básica en concienciación sobre mínimo privilegio.
3. Posible ampliación de licencias MFA.
4. Eventual consultoría puntual.
5. Evaluación futura de herramienta IGA (no obligatoria en esta fase).

Dado que la mayoría de actividades corresponden a rediseño organizativo y optimización de controles existentes, el proyecto presenta una relación costo-beneficio favorable, considerando que la mitigación de un incidente de seguridad podría implicar costos significativamente superiores (operativos, reputacionales y legales).

4. Recursos Organizativos

Para garantizar sostenibilidad, se requieren recursos estructurales de gobierno:

- Aprobación formal del plan por Dirección.
- Actualización de la política de control de accesos.
- Designación oficial del propietario del proceso IAM.
- Establecimiento de revisiones trimestrales institucionalizadas.
- Integración formal entre RRHH y TI mediante procedimiento JML documentado.

Estos recursos organizativos son críticos, ya que la ausencia de gobierno fue identificada como una de las causas raíz del problema.

5. Recursos de Gestión del Cambio

La implementación del nuevo modelo IAM implica formas diferentes en la forma en que se asignan y revisan accesos, lo que puede generar resistencia organizacional. Por ello, se contemplan recursos asociados a la gestión del cambio:

- Comunicación interna del proyecto y sus objetivos.
- Sesiones informativas para responsables de área.
- Capacitación básica en principios de mínimo privilegio.
- Difusión de responsabilidades en certificación de accesos.
- Seguimiento inicial cercano durante el primer ciclo de revisión.

Este componente busca garantizar adopción efectiva y evitar retrocesos al modelo anterior.

6.Estimación de esfuerzo global

Se estima que la ejecución del plan requerirá:

- 4 meses de implementación progresiva.
- Dedicación parcial del equipo clave (20–30 % de su tiempo durante fases críticas).
- Supervisión continua posterior como parte de operación normal.

7.Evaluación de viabilidad

Desde una perspectiva de viabilidad:

- Técnica: Alta, ya que se basa en capacidades existentes.
- Operativa: Media-alta, requiere coordinación interdepartamental.
- Económica: Favorable, con bajo costo relativo frente al riesgo mitigado.
- Estratégica: Alta, al alinearse con la visión de madurez en ciberseguridad.

8.Contribución de los recursos a la reducción del riesgo

Cada categoría de recursos contribuye a mitigar riesgos específicos:

- Recursos humanos → reducen errores de configuración y falta de control.
- Recursos tecnológicos → disminuyen vulnerabilidades técnicas.

- Recursos organizativos → fortalecen gobernanza y trazabilidad.
- Recursos de cambio → reducen riesgo de incumplimiento interno.

En conjunto, la asignación adecuada de recursos permite asegurar que la solución no sea únicamente teórica, sino operativamente viable y sostenible en el tiempo.

6 Definición del alcance de la solución, partes interesadas, cronograma y presupuestos.

La implementación de la propuesta de mejora del proceso de gestión de identidades y accesos (IAM) en JFMarket S.A. exige una planificación detallada que permita traducir la solución diseñada en un conjunto de acciones concretas, coordinadas y viables. En este sentido, la presente sección tiene como propósito definir el alcance final de la intervención, identificar a las partes interesadas y responsables de las actividades, establecer un cronograma de ejecución y estimar el presupuesto necesario para el desarrollo del proyecto.
La necesidad de esta planificación se justifica en la naturaleza transversal del proceso IAM, cuya correcta ejecución impacta de manera directa en la seguridad de la información, la continuidad operativa y el cumplimiento normativo de la organización. Las deficiencias identificadas en el diagnóstico —particularmente la ausencia de un procedimiento formal de gestión del ciclo de vida de identidades, la asignación manual de privilegios, la carencia de revisiones periódicas y la falta de segregación de funciones— requieren una respuesta organizada y progresiva, sustentada en una adecuada asignación de responsabilidades, recursos y tiempos.
Asimismo, la definición del alcance y de los recursos asociados permite delimitar con precisión qué componentes serán intervenidos en esta fase del proyecto y cuáles quedarán fuera para una etapa posterior de madurez. Del mismo modo, la identificación de responsables y la programación temporal de actividades constituyen elementos clave para garantizar el seguimiento, la rendición de cuentas y la evaluación continua del avance del proyecto.
En consecuencia, esta sección se orienta a convertir la propuesta de mejora en un plan operativo realista, medible y alineado con los objetivos estratégicos de seguridad de la información de JFMarket S.A., asegurando que la intervención pueda ejecutarse de forma eficiente y sostenible en el tiempo.

6.1 Alcance final de la solución

El alcance final de la solución comprende la intervención sobre el proceso de gestión de identidades y accesos (IAM) de JFMarket S.A., centrando los esfuerzos en los sistemas y componentes de mayor criticidad para la operación del negocio. En particular, la propuesta se aplicará a la plataforma de comercio electrónico, al sistema ERP, al CRM y al entorno cloud corporativo, debido a que estos activos concentran procesos esenciales de negocio y representan un mayor nivel de exposición frente a riesgos de seguridad derivados de un control inadecuado de accesos.

Dentro de este alcance se incluyen las acciones necesarias para formalizar el procedimiento de gestión del ciclo de vida de usuarios mediante el modelo Joiner-Mover-Leaver (JML), diseñar e implementar un esquema de control de accesos basado en roles (RBAC), definir una matriz de segregación de funciones, activar mecanismos de autenticación multifactor (MFA) en los sistemas críticos y establecer revisiones periódicas de privilegios. Asimismo, se contempla la creación de indicadores clave de desempeño (KPIs) para medir el avance y los resultados de la intervención, así como la evaluación de viabilidad para la futura incorporación de una herramienta de Gobierno y Administración de Identidades (IGA).

Desde la perspectiva organizativa, el alcance incluye la participación de las áreas de Seguridad de la Información, Tecnología de la Información, Recursos Humanos y responsables funcionales de negocio, dado que todas ellas intervienen de forma directa en la definición, validación, ejecución o supervisión del proceso IAM. Esta inclusión responde a la necesidad de abordar el problema desde una perspectiva integral, considerando no solo los aspectos técnicos, sino también los procedimentales y de gobierno.

Quedan fuera del alcance de esta fase los sistemas clasificados como no críticos, las aplicaciones temporales de uso departamental y los accesos de terceros de carácter eventual o puntual, cuya incorporación podría contemplarse en etapas posteriores de ampliación del modelo IAM. Del mismo modo, la adquisición e implantación de una herramienta IGA no forma parte de la ejecución inmediata del proyecto, limitándose en esta fase a un análisis preliminar de factibilidad técnica y económica.

Los resultados esperados dentro del alcance definido son la reducción de privilegios excesivos, la eliminación de cuentas huérfanas, la disminución del tiempo de revocación de accesos, el incremento del porcentaje de usuarios con MFA habilitado y la mejora de la trazabilidad y supervisión del proceso IAM. En conjunto, el alcance final de la solución se orienta a una intervención factible, priorizada por riesgo y alineada con las necesidades reales de la organización.

6.2 Identificación de responsables de las actividades para ejecución

La ejecución efectiva de la solución propuesta requiere una asignación clara de responsabilidades, de modo que cada actividad del plan de acción cuente con un responsable principal y con actores de apoyo que permitan garantizar coordinación, control y seguimiento. Dado el carácter transversal del proceso IAM, la intervención involucra a distintas áreas de la organización, cuyas funciones deben estar claramente delimitadas para evitar ambigüedades y asegurar la correcta implementación del proyecto.

El Responsable de Seguridad de la Información asumirá el liderazgo funcional del proyecto. Entre sus responsabilidades se encuentran la coordinación general de la implementación, la actualización y validación de políticas y controles, la supervisión del cumplimiento normativo, la definición de indicadores de desempeño y la comunicación de avances y resultados a la Dirección. Este rol tendrá además la función de asegurar que la solución mantenga coherencia con los principios de mínimo privilegio, segregación de funciones y enfoque Zero Trust.

El Administrador de Sistemas o equipo de Tecnología de la Información será el responsable de la ejecución técnica de la solución. Sus funciones abarcarán la configuración de roles RBAC, la

activación y validación de MFA, la depuración de cuentas huérfanas, la actualización de permisos en sistemas críticos y la implementación de los cambios necesarios en el directorio corporativo y en los entornos tecnológicos involucrados.

El área de Recursos Humanos tendrá la responsabilidad de proporcionar información actualizada sobre el ciclo de vida laboral de los empleados, notificando oportunamente altas, bajas y cambios de puesto. Su participación es indispensable para asegurar la correcta operatividad del procedimiento JML y para reducir el riesgo de cuentas activas sin legitimidad vigente.

Los responsables funcionales de cada área de negocio participarán en la definición y validación de los permisos requeridos para cada puesto de trabajo, así como en la certificación periódica de accesos durante las revisiones de privilegios. Su intervención es clave para garantizar que los accesos otorgados respondan a necesidades reales de negocio y se mantengan alineados con las funciones de cada usuario.

Finalmente, la Dirección de la organización ejercerá un rol de patrocinio institucional, aprobando las decisiones estratégicas del proyecto, validando la asignación de recursos y revisando los resultados alcanzados. Aunque no intervendrá en la operación cotidiana de la solución, su respaldo resulta esencial para consolidar la sostenibilidad del modelo IAM mejorado.

A continuación, se resume la asignación de responsables por actividad:

Tabla 1. Matriz de Responsabilidades.

Actividad	Responsable principal	Áreas de apoyo
Aprobación del proyecto	Dirección	Seguridad de la Información
Actualización de política de control de accesos	Seguridad de la Información	Dirección
Definición del procedimiento JML	Seguridad de la Información	RRHH, TI
Diseño de matriz RBAC	Seguridad de la Información	TI, responsables funcionales
Definición de matriz SoD	Seguridad de la Información	Responsables funcionales
Configuración técnica de roles	TI / Administrador de Sistemas	Seguridad
Implementación de MFA	TI / Administrador de Sistemas	Seguridad
Revisión de cuentas huérfanas	TI	RRHH
Certificación periódica de accesos	Responsables funcionales	Seguridad, TI
Seguimiento de KPIs	Seguridad de la Información	Dirección
Evaluación de viabilidad de IGA	Seguridad de la Información	TI, Dirección

6.3 Cronograma de ejecución

El cronograma de ejecución del proyecto se ha definido con una duración estimada de cuatro meses, en coherencia con el alcance de la intervención, la disponibilidad de recursos y la necesidad de implementar la solución de forma progresiva. La secuencia temporal de actividades responde a un enfoque estructurado de mejora continua, permitiendo avanzar desde la fase de diseño y formalización hasta la fase de despliegue, evaluación y consolidación.

Durante el primer mes se desarrollarán las actividades de carácter normativo y procedimental. En esta etapa se actualizará la política de control de accesos, se documentará el procedimiento JML, se definirán los roles organizativos y se elaborarán las matrices RBAC y de segregación de funciones. Asimismo, se establecerán los KPIs que servirán para medir el impacto de la intervención. Esta fase constituye la base conceptual y organizativa del proyecto.

En el segundo mes se pondrá en marcha la implementación técnica piloto, centrada inicialmente en el sistema ERP, dado su carácter crítico y su relevancia para la operación del negocio. En esta fase se configurarán los primeros roles RBAC, se revisarán privilegios excesivos, se identificarán y eliminarán cuentas huérfanas y se activará MFA para los accesos correspondientes. El objetivo de esta etapa es validar el diseño de la solución antes de su extensión al resto de sistemas.

El tercer mes estará orientado al despliegue progresivo de la solución en el CRM, la plataforma e-commerce y el entorno cloud. Paralelamente, se ejecutará la primera revisión formal de accesos, se recogerá evidencia documental y se realizarán acciones de concienciación interna sobre mínimo privilegio y certificación de accesos.

Finalmente, en el cuarto mes se desarrollará la fase de evaluación y consolidación. Durante esta etapa se medirán los KPIs definidos, se analizará la reducción de los riesgos identificados, se evaluará el cumplimiento de los objetivos del proyecto y se elaborará un informe final con resultados, hallazgos y oportunidades de mejora. Asimismo, se llevará a cabo una valoración preliminar de viabilidad para la implantación futura de una herramienta IGA.

Tabla 2. Cronograma de actividades.

Actividad	Mes 1	Mes 2	Mes 3	Mes 4
Aprobación del proyecto y designación de responsables	X			
Actualización de política de control de accesos	X			
Documentación del procedimiento JML	X			
Definición de roles y matriz RBAC	X	X		
Diseño de matriz de segregación de funciones	X	X		
Definición de KPIs	X			
Configuración técnica piloto en ERP		X		

Revisión inicial de privilegios y cuentas huérfanas		X		
Implementación inicial de MFA		X	X	
Despliegue en CRM, e-commerce y cloud			X	
Primera revisión formal de accesos			X	
Medición de KPIs				X
Evaluación de resultados				X
Informe final y cierre del proyecto				X
Evaluación de viabilidad de IGA				X

6.4 Presupuesto

El presupuesto estimado para la ejecución del proyecto se ha calculado considerando una intervención de alcance moderado, apoyada principalmente en la optimización de recursos ya existentes dentro de la organización. En consecuencia, la mayor parte del coste se concentra en horas de dedicación interna del personal implicado, actividades de capacitación y la posible ampliación de licencias para la autenticación multifactor.

Desde una perspectiva de viabilidad económica, la propuesta resulta razonable y proporcionada al riesgo que busca mitigar. La inversión asociada al fortalecimiento del proceso IAM es considerablemente inferior al impacto potencial que podría derivarse de un incidente de seguridad relacionado con accesos indebidos, cuentas huérfanas o privilegios excesivos en sistemas críticos. Además, los beneficios esperados no se limitan al ámbito técnico, sino que también abarcan mejoras en trazabilidad, capacidad de auditoría y alineación con estándares internacionales.

El presupuesto presentado a continuación tiene carácter referencial y podrá ajustarse en función de la disponibilidad real de recursos internos, del nivel de madurez tecnológica actual y de la eventual necesidad de apoyo externo especializado.

Tabla 3. Presupuesto.

Rubro	Valor
Horas de Seguridad de la Información	2.400
Horas de TI / Administrador de Sistemas	3.000
Horas de Recursos Humanos	800
Participación de responsables funcionales	1.000
Capacitación y concienciación interna	700
Licencias adicionales de MFA	1.200
Consultoría puntual especializada (opcional)	1.500

Contingencia (10 %)	1.060
Total estimado	11.660 €

7 Referencias bibliográficas

ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization.

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). U.S. Department of Commerce.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST SP 800-207). National Institute of Standards and Technology.

National Institute of Standards and Technology. (2017). Digital Identity Guidelines (NIST SP 800-63-3). U.S. Department of Commerce.

ISACA. (2019). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

SailPoint. (2021). Identity Governance and Administration: A Comprehensive Guide to Identity Security. SailPoint Technologies.

Gartner. (2021). Market Guide for Identity Governance and Administration. Gartner Research.

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice (4th ed.). Pearson.