UNIVERSIDAD NACIONAL DE CHIMBORAZO
FACULTAD DE INGENIERIA
CARRERA ELECTRONICA Y TELECOMUNICACIONES

Desarrollo de un Prototipo para la Administración Centralizada de Identidades y Dispositivos en la Nube mediante Herramientas Microsoft en los Laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH

Trabajo de Titulación para optar al título de Ingeniero en Electrónica y Telecomunicaciones

Autor:
Rosales Orbes, Bryan Javier

Tutor:
MgSc. Alejandra del Pilar Pozo Jara

Riobamba, Ecuador. 2026

DERECHOS DE AUTORÍA

Yo, **Bryan Javier Rosales Orbes**, con cédula de ciudadanía **1003770672**, autor del trabajo de investigación titulado: **Desarrollo de un Prototipo para la Administración Centralizada de Identidades y Dispositivos en la Nube mediante Herramientas Microsoft en los Laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH,** certifico que la producción, ideas, opiniones, criterios, contenidos y conclusiones expuestas son de mí exclusiva responsabilidad.

Asimismo, cedo a la Universidad Nacional de Chimborazo, en forma no exclusiva, los derechos para su uso, comunicación pública, distribución, divulgación y/o reproducción total o parcial, por medio físico o digital; en esta cesión se entiende que el cesionario no podrá obtener beneficios económicos. La posible reclamación de terceros respecto de los derechos de autor (a) de la obra referida, será de mi entera responsabilidad; librando a la Universidad Nacional de Chimborazo de posibles obligaciones.

En Riobamba, 05 de enero de 2026.

Bryan Javier Rosales Orbes
C.I: 1003770672

DICTAMEN FAVORABLE DEL PROFESOR TUTOR

Quien suscribe, Mgs. Alejandra del Pilar Pozo Jara, catedrática adscrita de la Facultad de Ingeniería por medio del presente documento certifico haber asesorado y revisado el desarrollo del trabajo de investigación **"Desarrollo de un Prototipo para la Administración Centralizada de Identidades y Dispositivos en la Nube mediante Herramientas Microsoft en los Laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH"**, bajo la autoría de Bryan Javier Rosales Orbes; por lo que se autoriza ejecutar los trámites legales para su sustentación.

En todo cuanto informo en honor a la verdad; en Riobamba, a los 5 días del mes de enero del año 2026.

Mgs. Alejandra del Pilar Pozo

TUTOR

CERTIFICADO DE LOS MIEMBROS DEL TRIBUNAL

Quienes suscribimos, catedráticos designados Miembros del Tribunal de Grado para la evaluación del trabajo de investigación **Desarrollo de un Prototipo para la Administración Centralizada de Identidades y Dispositivos en la Nube mediante Herramientas Microsoft en los Laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH,** presentado por Bryan Javier Rosales Orbes con cédula de identidad número 1003770672, bajo la tutoría de Mgs. Alejandra del Pilar Pozo Jara; certificamos que recomendamos la APROBACIÓN de este con fines de titulación. Previamente se ha evaluado el trabajo de investigación y escuchada la sustentación por parte de su autor; no teniendo más nada que observar

De conformidad a la normativa aplicable firmamos, en Riobamba a los 5 días del mes de enero del año 2026.

Ing. Ciro Diego Radicelli García, PhD.
Presidente del Tribunal de Grado

Ing. Juan Carlos Cepeda Pacheco, PhD.
Miembro del Tribunal de Grado

Dr. Manuel Antonio Meneses Freire, PhD.
Miembro del Tribunal de Grado

C E R T I F I C A C I Ó N

Que, **ROSALES ORBES BRYAN JAVIER** con CC: **1003770672**, estudiante de la Carrera **ELECTRÓNICA Y TELECOMUNICACIONES**, **NO VIGENTE,** Facultad de **Ingeniería**; ha trabajado bajo mi tutoría el trabajo de investigación titulado "**Desarrollo de un Prototipo para la Administración Centralizada de Identidades y Dispositivos en la Nube mediante Herramientas Microsoft en los Laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH**", cumple con el **3% de similitud y 3% de Inteligencia Artificial**, de acuerdo al reporte del sistema Anti plagio **COMPILATIO**, porcentaje aceptado de acuerdo a la reglamentación institucional, por consiguiente autorizo continuar con el proceso.

Riobamba, 16 de diciembre de 2025

Firmado electrónicamente por:
ALEJANDRA DEL PILAR POZO JARA
Validar únicamente con FirmaEC

Mgs. Alejandra del Pilar Pozo Jara
TUTORA TRABAJO DE INVESTIGACIÓN

DEDICATORIA

El presente trabajo de titulación va dedicado con todo mi corazón principalmente a Dios por darme la sabiduría y resiliencia para afrontar cada reto que se ha presentado a lo largo de los años en esta resiliente carrera universitaria.

A mis padres, por ser mi roca, mi inspiración y mi apoyo incondicional en cada etapa de mi vida. Su sacrificio, su amor infinito y su fe en mí hicieron posible este logro. Esto es para ustedes.

A mi familia y amigos en general que me han apoyado a lo largo de este proceso para encontrar mi camino en la convicción, esfuerzo y fe, en momentos muy oscuros ellos fueron mi luz para poder continuar, el permitirse creer en mi me abrió puertas que antes no sabía que eran posibles.

También quiero realizar una mención especial para A.T y M. por ser guía esencial en mi vida, cambiar mi perspectiva y saber que todo es posible con respeto y amor, muchas gracias por los largos días compartidos y el apoyarme hasta el final de este difícil recorrido.

Finalmente me dedico este trabajo a mí mismo, porque pese a las dificultades, el cansancio y las dudas, decidí no rendirme. Hoy cierro una etapa sabiendo que cada sacrificio valió la pena.

AGRADECIMIENTO

En primer lugar, agradezco a la Universidad Nacional de Chimborazo por brindarme la formación, los recursos y el entorno académico necesarios para llevar a cabo este proyecto de tesis. Extiendo mi sincero agradecimiento a mi tutora, Mgs. Alejandra del Pilar Pozo cuya guía, orientación y compromiso fueron fundamentales para el desarrollo de este trabajo. Su paciencia, conocimientos y observaciones enriquecieron cada etapa del proceso, siendo una inspiración constante tanto en lo personal como en lo profesional.

También expreso mi agradecimiento al Dr. Antonio Meneses por su disposición y experiencia durante este proyecto cuyo acompañamiento resultó fundamental para la elaboración de este trabajo.

De igual manera, agradezco al personal de la Dirección de Tecnologías de la Información de la UNACH, especialmente al Mgs. Adrián Aldaz, por abrirme las puertas de su entorno y permitir la realización de este proyecto.

Hago extensivo mi agradecimiento a los docentes y al personal administrativo de la carrera de Electrónica y Telecomunicaciones ya que su dedicación y contribuciones académicas fueron claves para el crecimiento de mis habilidades profesionales, así como al Mgs. Juan Carlos Cepeda por su respaldo durante el proceso y por último deseo manifestar mi gratitud a mi familia, quienes con su apoyo continuo hicieron posible la finalización de esta fase académica siendo así un pilar esencial a lo largo de todo mi recorrido educativo.

ÍNDICE GENERAL

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, la administración eficiente y segura de identidades y dispositivos se ha consolidado como un elemento clave en las instituciones educativas debido al incremento del uso de tecnologías en la nube y a la necesidad de garantizar un acceso controlado a los recursos tecnológicos. Por ello, la ausencia de una plataforma centralizada puede generar dificultades en la gestión de accesos, dispositivos y políticas de seguridad en los laboratorios institucionales.

La siguiente investigación se desarrolla con el objetivo de crear un prototipo que centralice la gestión de identidades y dispositivos en la nube utilizando herramientas Microsoft como Entra ID e Intune, con el propósito de mejorar la administración y efectividad en los laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Nacional de Chimborazo (UNACH). La investigación es de tipo aplicada, descriptiva y tiene un enfoque cuasiexperimental puesto que se implementa un prototipo tecnológico orientado a resolver una problemática real, analiza una situación inicial de los procesos de gestión y la solución se despliega en un entorno virtual controlado que replica las condiciones reales del laboratorio permitiendo comparar el estado del entorno antes y después de la intervención. El prototipo integra Microsoft Entra ID para la administración de identidades e Intune para la gestión de dispositivos y se realizaron pruebas funcionales sobre equipos de laboratorio con el propósito de evaluar la aplicación de políticas, administración remota y control del entorno.

En conclusión, los resultados evidenciaron avances significativos en la gestión y organización del entorno tecnológico dado que la integración de Intune permitió aplicar configuraciones y políticas de forma centralizada mientras que Entra ID facilitó el uso de credenciales institucionales y una administración unificada de accesos, también la configuración de equipos compartidos y la restricciones específicas contribuyeron a una mayor estandarización, representando de esta manera un avance significativo frente a un escenario sin gestión centralizada y sirviendo como base para una futura implementación y optimización del modelo de administración a nivel institucional.

Palabras claves: Administración centralizada, Entra ID, Intune, nube, identidades, dispositivos

Abstract

Efficient and secure management of identities and devices has become essential for educational institutions, driven by the growing adoption of cloud-based technologies and the need to ensure controlled access to technological resources. In this context, the absence of a centralized management platform can generate significant challenges related to access control, device administration, and the enforcement of security policies within institutional laboratories. This study aimed to design and implement a prototype that centralizes cloud-based identity and device management using Microsoft tools such as Entra ID and Intune, with the goal of improving administrative efficiency and operational effectiveness in the laboratories of the Information and Communication Technologies Department at the Universidad Nacional de Chimborazo (UNACH). An applied, descriptive research methodology with a quasi-experimental design was adopted, as a technological solution was developed to address a real institutional need. The study began with an analysis of the existing management processes, followed by the deployment of the proposed prototype in a controlled virtual environment that emulated real laboratory conditions. This approach enabled a comparative assessment of the system before and after implementation. The prototype integrates Microsoft Entra ID for identity and access management and Microsoft Intune for device administration. Functional tests were conducted on laboratory equipment to evaluate policy enforcement, remote management capabilities, and environment configuration. The results revealed substantial improvements in the organization and administration of the technological environment. Intune facilitated centralized configuration and policy management, while Entra ID strengthened authentication processes using institutional credentials and unified access control. Furthermore, the implementation of shared device configurations and specific usage restrictions led to increased standardization across laboratory environments. Overall, transitioning from a non-centralized management model to a centralized, policy-driven approach significantly enhanced operational efficiency and established a robust foundation for future institutional-level adoption and optimization of the proposed administration model.

***Keywords*:** centralized administration, Entra ID, Intune, cloud computing, identities, devices.

Firmado electrónicamente por:
JENNY ALEXANDRA FREIRE RIVERA
Validar únicamente con FirmaEC

Reviewed by:
Jenny Alexandra Freire Rivera, M.Ed.
ENGLISH PROFESSOR
ID No.: 0604235036

CAPÍTULO I.

1. INTRODUCCION

Hoy en día la administración eficiente de identidades y dispositivos se ha consolidado como algo primordial para las organizaciones debido a los cambios repentinos tecnológicos a nivel mundial en donde las empresas se ven en la necesidad de implementar servicios basados en la nube [1], este cambio está lejos de parecer simplemente un movimiento de transformación digital sino también una estrategia clave para su continuidad comercial y operativa como se evidenció con la rápida adopción de estos servicios en la reciente pandemia [1] asimismo esta modalidad ha emergido como algo determinante para el suministro de servicios a través de internet proporcionando escalabilidad, versatilidad y una gestión rentable [2].

Bajo esta perspectiva los laboratorios de la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo (UNACH) presentan dificultades en los procesos de administración de identidades y accesos (IAM) en donde la infraestructura actual no dispone de una solución centralizada que posibilite una manera de administrar de manera unificada identidades, accesos y dispositivos en diversos entornos de laboratorio lo cual dificulta la implementación de políticas de gestión centralizadas y consistentes elevando así las vulnerabilidades en los mecanismos de seguridad y la exposición a ingresos no autorizados o indebidos para lo cual las soluciones en la nube han probado ser altamente ventajosas al mejorar el acceso, la sincronización y con ello la recolección integral de datos [3].

Microsoft Entra ID (MEID) que antes se llamaba Azure Active Directory (Azure AD) es la solución de gestión de identidades y accesos (IAM) basada en la nube de Microsoft [4], [5] que es un servicio de gestión de acceso e identidades basado en la nube que los trabajadores tienen la posibilidad de emplear para tener acceso a recursos externos dentro de los cuales se incluyen Microsoft 365, Azure Portal y otras aplicaciones SaaS [6]. MEID amplía las capacidades de administración de identidades y accesos de Active Directory hacia entornos multinube mediante un servicio en la nube que permite integrar inicio de sesión único, autenticación multifactorial y políticas de acceso condicional para todos los recursos empresariales híbridos [7]. Del mismo modo Microsoft Intune es una plataforma de

administración que controla el cómo los usuarios acceden a los recursos de la empresa y facilita la gestión de aplicaciones y dispositivos [8].

En vista de ello esta investigación propone el desarrollo de un prototipo para la gestión centralizada de identidades y dispositivos en la nube usando la combinación de herramientas Microsoft como Entra ID e Intune para los laboratorios de la DTIC en la UNACH esto implica que el proceso incluirá un análisis y diseños previos para identificar las características y funciones requeridas con la finalidad de crear una solución escalable que se adapte a las futuras necesidades tecnológicas de la institución y de este modo fortalecer la administración, seguridad y optimización de los recursos en el entorno académico.

1.1 Planteamiento del problema

La introducción de la era digital y la abundancia de información han provocado un incremento notable en los dispositivos interconectados que a su vez ha resultado en una gran cantidad de datos que se circulan por la red [9]. Investigaciones recientes enfatizan la relevancia de establecer un sistema centralizado de datos en la nube dentro de las instituciones educativas, indicando cómo su aplicación ayuda de manera considerable a fortalecer la seguridad, aumentar la eficiencia en las operaciones y facilitar la administración de dispositivos y accesos, particularmente en situaciones en las que varios usuarios utilizan equipos compartidos [3].

De igual manera los servicios en la nube suelen adoptarse para replicar las soluciones locales y simultáneamente ofrecer una mayor flexibilidad que los sistemas físicos o virtuales. Para reducir la amenaza de accesos no autorizados y otras vulnerabilidades al sistema es crucial garantizar que se utilice servicios de autenticación centralizados que se hayan migrado a la nube lo que permite mantener el dominio sobre las aplicaciones y los usuarios [10].

En el escenario actual los laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH no cuentan con un sistema centralizado de gestión de identidades y accesos, lo cual conlleva diversas limitaciones. Por este motivo, cada laboratorio maneja sus usuarios y dispositivos de manera independiente, careciendo de una coordinación en las políticas de seguridad, lo que al ser un ambiente académico no solo aumenta el riesgo de accesos no autorizados, sino que también complica la implementación

de estándares uniformes de protección en los distintos laboratorios, así como el resguardo de los recursos que la universidad proporciona a la comunidad académica [3]. A nivel institucional esta problemática implica un consumo innecesario de recursos económicos y humanos que podría ser redirigido a otras áreas de trabajo.

1.2 Justificación

Numerosas organizaciones que están realizando la transición hacia aplicaciones en la nube, así como aquellas que operan con una combinación de sistemas están reconociendo la importancia de implementar una gestión de red fundamentada en la nube [11], también están apuntando hacia la administración de identidades y accesos para satisfacer las exigencias regulatorias y apego normativo que establecen una gran responsabilidad a la función de gestión de seguridad, lo que se traduce a la necesidad de elaborar informes adicionales, mantener mejores registros de flujos de trabajos y procesar solicitudes [12], en consecuencia han identificado que la automatización en la gestión es un claro reductor de costos.

Ahora bien, dado que la Universidad Nacional de Chimborazo está alineada como una entidad Microsoft se busca implementar los servicios proporcionados por la compañía para abordar las limitaciones relacionados con la optimización de la administración centralizada de identidades y dispositivos aprovechando los recursos respecto a licencias existentes e incorporando las herramientas Entra ID e Intune.

En la actualidad, Microsoft Entra ID se ha integrado con gran éxito en diversas organizaciones tanto en el ámbito público como el privado a nivel global [4], gracias a la capacidad de centralización que brinda esta plataforma la información puede ser accesible desde casi cualquier ubicación que cuente con conexión a internet. De acuerdo con Microsoft [13], la compañía destina mil millones de dólares al año a la seguridad con el objetivo de salvaguardar la información de los clientes frente a amenazas cibernéticas, además investigaciones recientes indican que los servicios basados en la nube poseen la capacidad necesaria para manejar amenazas de seguridad siempre y cuando se implementen adecuadamente [1], también el almacenamiento de datos en la nube de manera centralizada reduce la posibilidad de perder la información asociada a fallos en el hardware [3] gracias a las copias de respaldo y las mecanismos de protección en estos entornos se garantiza que los

datos permanezcan seguros y accesibles fortaleciendo la robustez y la continuidad en el acceso a los datos fundamentales [3].

Considerando estos antecedentes y con el fin de atender las dificultades que presenta la DTIC en la gestión de identidades y dispositivos se plantea el desarrollo de un prototipo de administración centralizada en la nube basado en Microsoft Entra ID e Intune. La propuesta se llevará a cabo en un entorno que simule las condiciones específicas de un laboratorio donde el prototipo será aplicado a 3 dispositivos dentro de dicho entorno para lo cual el plan contempla un análisis y diseño iniciales para definir las funcionalidades que permitan optimizar el control, fortalecer la seguridad y gestionar de forma eficiente los recursos educativos además de prever su capacidad de adaptación frente a las demandas futuras de la institución.

1.3 OBJETIVOS

1.3.1 Objetivo General

Desarrollar un prototipo de administración centralizada de identidades y dispositivos en la nube utilizando herramientas Microsoft para optimizar la gestión y eficiencia en los laboratorios de la Dirección de Tecnologías de la Información y Comunicación de la UNACH.

1.3.2 Objetivos Específicos

- Analizar la situación actual de la administración de identidades y dispositivos en los Laboratorios de la Dirección de Tecnologías de la Información.
- Investigar las funcionalidades y capacidades de Microsoft Entra ID e Intune en la administración de identidades y dispositivos en la nube en un entorno académico.
- Desarrollar un prototipo de administración centralizada que integre Microsoft Entra ID e Intune para gestionar eficientemente identidades y dispositivos en los laboratorios.
- Proponer lineamientos para su futura implementación en todos los laboratorios de la dirección de Tecnologías de la información.

CAPÍTULO II.

2. MARCO TEÓRICO

2.1 Estado del arte

Las publicaciones actuales indican un cambio notable hacia modelos de gestión centralizada en la nube motivados por la necesidad de consolidar identidades, accesos y dispositivos en un solo entorno en donde investigaciones comparativas demuestran que los sistemas centralizados de gestión de identidades facilitan una implementación más uniforme de las políticas de acceso y fortalecen la capacidad de seguimiento en comparación con las arquitecturas descentralizadas [14]. Además, investigaciones recientes en el ámbito de la gestión de identidades resaltan el movimiento hacia sistemas integrados que facilitan la automatización, gobernanza de accesos y las evaluaciones de conformidad en la nube promoviendo de esta manera la implementación de estructuras de control centralizado como fundamento de la seguridad en las organizaciones [15]. Asimismo, evidencia reciente existen sobre la gestión unificada de endpoints (UEM) indican que las plataformas UEM se han convertido en alternativas fundamentales para la administración de diversos dispositivos en cuanto a seguridad, regulación y supervisión dentro de organizaciones que operan con modelos híbridos y entornos de trabajo a distancia [16].

2.2 Administración centralizada

La administración centralizada implica el manejo unificado de los recursos y servicios tecnológicos dentro de una organización abarcando dispositivos, usuarios, aplicaciones y normativas de seguridad, este método brinda a los administradores de tecnologías de la información la capacidad de supervisar completamente la infraestructura tecnológica facilitando así las labores de monitoreo, mantenimiento e implementación de políticas de seguridad, de esta manera resulta esencial para optimizar la eficiencia operativa, disminuir gastos, asegurar el cumplimiento de normativas y proteger información sensible frente a accesos no autorizados.

La también denominada gestión centralizada, en entornos tecnológicos comprende mecanismos, políticas y herramientas que permiten administrar identidades, accesos y dispositivos de manera unificada desde un punto de control central; en organizaciones que adoptan la nube o que manejan infraestructuras diversas es en donde la centralización tiene

como objetivo simplificar la operación, incrementar la seguridad y facilitar el cumplimiento de normativo lo cual ha impulsado el crecimiento de soluciones de gestión de identidades y accesos (IAM) y de plataformas de gestión de dispositivos que están integradas en la nube [17].

2.3 Gestión de identidades y accesos

La gestión de identidades y accesos (IAM) integra procesos de aprovisionamiento y des aprovisionamiento de cuentas, así como mecanismos de autenticación definidos por políticas y funciones de auditoría centralizada, como se puede observar en Figura 1, con el objetivo de controlar y verificar quien puede tener acceso a los recursos y en qué momento, todo esto conforme a las políticas previamente establecidas [18].

Es entonces que la gestión centralizada de identidades y accesos (IAM) se refiere a la recopilación de procesos y herramientas tecnológicas que se emplean para gestionar de forma centralizada a los usuarios y sus permisos para acceder a sistemas de información y aplicaciones brindando así a todos los usuarios internos como externos un acceso apropiado [17].

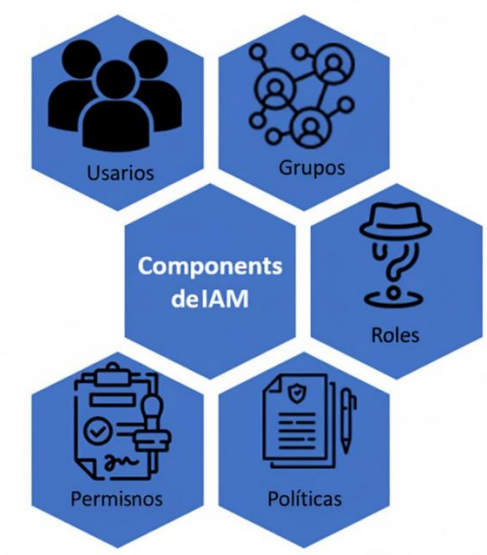


Figura 1. Componentes principales de la gestión de identidades y accesos (IAM) en entornos organizacionales, incluyendo usuarios, grupos, roles, permisos y políticas de control [15]

2.4 Gestión de dispositivos

Paralelamente la gestión centralizada de dispositivos (MDM) permite administrar la configuración, el cumplimiento, la actualización de sistemas y la distribución de aplicaciones

de los dispositivos finales desde una plataforma unifica en la cual conjunto con la administración de identidades conforman el núcleo operativo de los modelos modernos de administración centralizada [18].

La gestión de dispositivos permite a las organizaciones supervisar y mantener diversos equipos lo que abarca máquinas virtuales, dispositivos físicos/móviles y aparatos IoT por ende es un componente fundamental de cualquier organización permitiendo que los dispositivos sean seguros, estén actualizados y cumplan con las políticas establecidas por la entidad con el objetivo de proteger los datos y la red corporativa.

2.5 Computación en la nube

La computación en nube se ha transformado en un modelo fundamental para ofrecer recursos informáticos que pueden ser solicitados según las necesidades, facilitando que las organizaciones utilicen servicios de procesamiento, almacenamiento y aplicaciones mediante infraestructuras que son altamente escalables y distribuidas.

El concepto de computación en nube se refiere a la accesibilidad de recursos de procesamiento centralizados los cuales los usuarios pueden emplear para realizar una variedad de actividades recibiendo a cambio los resultados que la plataforma ha procesado, este modelo es adoptado tanto por individuos como por empresas ya que ofrece la posibilidad de contratar capacidad de cómputo sin adquirir equipamiento propio, lo que representa un ahorro significativo frente a la compra de múltiples computadoras o servidores físicos [19].

Es decir que facilita una administración eficiente de la información a un costo accesible, ofreciendo opciones de precios flexibles que se adaptan tanto a las exigencias de los usuarios como a la experiencia de los proveedores de este tipo de servicios [20].

2.5.1 Características

En términos generales para que un servicio sea considerado en la nube debe cumplir algunas características entre las cuales están el autoservicio bajo demanda, el amplio acceso a la red, la puesta en común de recursos, la elasticidad rápida y el servicio medido [21].

A continuación, se detallan dichas características:

Autoservicio bajo demanda: Capacidad del usuario final para gestionar la provisión de recursos y servicios por sí mismo sin necesidad de interacción directa con el proveedor.

Amplio acceso a la red: Oportunidad de acceder a los servicios mediante redes estándar mediante varios tipos de dispositivos, como computadoras de escritorio, laptops y dispositivos móviles.

Puesta en común de recursos: Los recursos del proveedor se agrupan para atender a múltiples usuarios y así asignarse dinámicamente según la demanda.

Servicio medido: Implementación de métodos de medición que permiten supervisar y facturar el uso de recursos como un servicio.

2.5.2 Tenant

Desde el enfoque de la arquitectura los inquilinos son elementos clave en un esquema conocido como multi-tenant. En este sistema, diversas entidades utilizan la misma infraestructura física proporcionada por un servicio en la nube, mientras que cada una preserva un entorno lógico que es totalmente independiente y seguro, por ende, esta separación asegura que las configuraciones, la información y las directrices de un inquilino no puedan ser alteradas ni visitadas por otros a pesar de compartir la misma infraestructura [22].

2.6 Microsoft Entra ID

Microsoft Entra ID Figura 2, que antes se llamaba Azure Active Directory como se observa en la Figura 3, es un servicio de gestión de identidades y accesos basados en la nube cuya función principal consiste en controlar y proteger el acceso de los usuarios autorizados para que puedan ingresar a los recursos organizacionales ya sean tanto de manera locales como en la nube y también Entra ID permite la integración con otros proveedores y aplicaciones de identidad [23].

Figura 2. Logotipo oficial de Microsoft Entra ID [6]

Entra ID proporciona a las empresas la administración de identidades, la implementación de políticas de seguridad, la autenticación de usuarios a través de técnicas avanzadas como la autenticación multifactorial y definir criterios de acceso condicional de acuerdo a requerimientos particulares [6] y evaluaciones de riesgo en tiempo real lo que fortalece la seguridad organizacional mediante decisiones basadas en contexto [15].

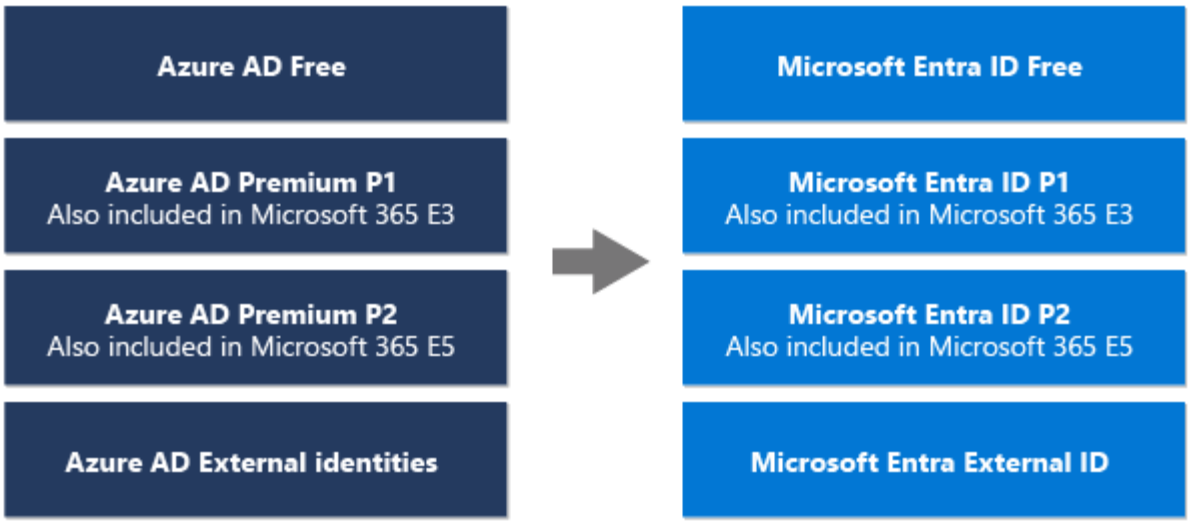


Figura 3. Comparación de las ediciones y nomenclaturas de Azure Active Directory y Microsoft Entra ID, incluyendo las versiones Free, P1, P2 y External ID dentro del ecosistema Microsoft 365 [6].

2.6.1 Licencias

Microsoft Entra ID proporciona varias versiones de licencias que se ajustan a las demandas de seguridad, manejo y cumplimiento de entidades de diversos tamaños y grados de avance tecnológico, entre las cuales se encuentran:

-Microsoft Entra ID Free: ofrece funciones esenciales como la administración de usuarios y grupos, la integración con directorios locales mediante sincronización, la disponibilidad de reportes básicos y el restablecimiento de contraseñas por parte del usuario final. Asimismo, habilita el acceso mediante inicio de sesión único a Azure, Microsoft 365 y múltiples aplicaciones SaaS comunes en el sector [6].

-Microsoft Entra ID P1: Aparte de las funciones disponibles en la versión gratuita, esta licencia ofrece a los usuarios en entornos híbridos la posibilidad de acceder tanto a recursos en la nube como locales. Esta versión también incluye capacidades de gestión más

sofisticadas, como la pertenencia dinámica a grupos, la gestión de grupos por parte del usuario, Microsoft Identity Manager y características de escritura diferida en la nube que facilitan a los usuarios locales la opción de restablecer sus contraseñas por sí mismos [6].

-Microsoft Entra ID P2: Además de las funciones disponibles de forma gratuita y en P1, la opción P2 incluye Microsoft Entra ID Protection, que facilita el acceso condicional a tus aplicaciones y datos esenciales de la empresa, basándose en el análisis de riesgos. También cuentan Privileged Identity Management que permite identificar limitar y monitorear a los administrados y su acceso a los recursos y además ofrece acceso justo a tiempo cuando se requiere [6].

2.7 Microsoft Intune: Endpoint Management

Microsoft Intune es un servicio en la nube para la gestión unificada de puntos (UEM) que facilita la administración de dispositivos, aplicaciones y configuraciones de seguridad desde un panel centralizado el cual su objetivo principal es ofrecer a las empresas un control uniforme sobre dispositivos que operan con Windows, macOS, Android y iOS, al integrar la gestión de políticas, la protección de datos y la implementación de software sin depender de la infraestructura local [5].

Figura 4. Logotipo oficial de Microsoft Intune [5]

De acuerdo a un artículo reciente, Intune (Figura 4), se considera como una herramienta clave para la administración unificada de dispositivos siendo fundamental para las empresas que desean garantizar que sus dispositivos, sistemas operativos y aplicaciones permanezcan actualizados, seguros y operativos [24].

Figura 5. Arquitectura funcional de Microsoft Intune para la administración centralizada de dispositivos, identidades, aplicaciones y políticas de seguridad en entornos organizacionales basados en la nube [5]

Es relevante señalar que Intune no ofrece un esquema de licencias que dependa únicamente de los dispositivos, en cambio, la plataforma sigue un modelo (Figura 5) asociado a las cuentas de los usuarios de manera que cada licencia faculta al propietario gestionar varios dispositivos en la empresa [25].

Por el contrario, cuando una organización necesita manejar un número elevado de dispositivos que no se asocian a un usuario específico, Microsoft Intune también ofrece un sistema denominado gestión de inscripción de dispositivos. No obstante, este enfoque está diseñado para casos donde las computadoras son parte del inventario de la empresa y requieren administración central sin conexión directa con cuentas individuales en donde un único usuario con permisos de inscripción registre hasta 1000 dispositivos lo que facilita la gestión masiva de equipos en entornos educativos, empresariales o en esta situación de laboratorios [25].

2.7.1 Licenciamiento

El licenciamiento de Microsoft Intune se estructura en diferentes planes, cada uno con características específicas orientadas a distintos escenarios de uso [26]:

Intune Plan 1: Incluye las funcionalidades estándar de administración de dispositivos, así como capacidades de generación de reportes y análisis de endpoints.

Intune Plan 2: Amplía las funciones del plan 1 al incorporar Microsoft Tunnel para VPN a nivel de aplicación en dispositivos iOS y Android además de soporte para dispositivos especializados.

Intune Suite: Integra todas las características de los planes anteriores y añade herramientas avanzadas como Remote Help, Endpoint Privilege Management y Advanced Endpoint Anaalytics.

CAPÍTULO III.

3. METODOLOGIA.

3.1 Tipo de investigación

La presente investigación es de tipo aplicada, puesto que se desarrolla un prototipo tecnológico que busca orientar a resolver un problema real relacionado con la ausencia de una administración centralizada de identidades y dispositivos en laboratorios de la Dirección de las Tecnologías de Información y Comunicación (DTIC) de la Universidad Nacional de Chimborazo. Además, es descriptiva, ya que se encarga de detallar la situación inicial de los procesos de gestión de accesos, políticas, dispositivos y seguridad informática antes de la intervención tecnológica. Finalmente, adopta un enfoque cuasiexperimental, ya que el prototipo se implementa en un entorno virtual controlado el cual replica las condiciones reales del laboratorio, sin una aleatorización ni grupo control, permitiendo así comparar los resultados obtenidos antes y después de la intervención y evaluar el efecto de la solución propuesta sobre la gestión del entorno tecnológico.

3.2 Diseño de la investigación

El diseño de la investigación se clasifica como cuasiexperimental, puesto que se fundamenta en la aplicación de un prototipo tecnológico en un entorno virtual controlado que se encarga de replicar las condiciones operativas del laboratorio, para evaluar los cambios generados tras su implementación. Este diseño permite realizar una comparación de forma directa entre lo que es el estado inicial en el que se encuentra el laboratorio y el estado posterior a lo que viene a ser la intervención.

Como se puede observar en **¡Error! No se encuentra el origen de la referencia.**, p ara la ejecución metodológica de la investigación se establecen las siguientes fases:

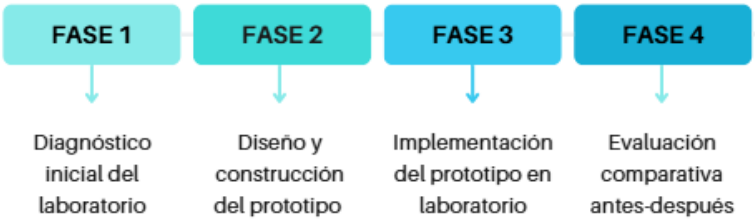


Figura 6. Fases metodológicas de la investigación para el diagnóstico, diseño, implementación y evaluación del prototipo de administración centralizada en el laboratorio

Fuente: Autor

Fase 1. Diagnóstico inicial del laboratorio

En esta primera fase se analizó la situación actual de los laboratorios de la DTIC respecto a la administración de identidades, dispositivos, políticas institucionales y niveles de seguridad. Se identificó que no existía una gestión centralizada, que los equipos permiten una instalación libre de aplicaciones y que no había una visibilidad del estado de los dispositivos ni un control desde los portales de administración de Microsoft Entra ID, los cuales constituyen el entorno técnico desde donde se gestiona lo que es la identidad, el acceso y la configuración de dispositivos dentro del ecosistema Microsoft 365. Esta fase ha permitido establecer el estado basal para lo que corresponde a parte posterior de la comparación.

Fase 2. Diseño y construcción del prototipo

En esta fase se desarrolló el prototipo de administración centralizada, utilizando herramientas de Microsoft Entra ID y Microsoft Intune. Por ello se ha configurado un entorno de prueba compuesto por tres máquinas virtuales, que permiten simular las condiciones de los equipos físicos del laboratorio y ejecutan Windows 11 Pro, lo cual es un requisito necesario para su gestión en la nube.

En este entorno se han creado grupos de seguridad, se habilitó la inscripción de dispositivos por medio de Microsoft Entra Joined, además se activó lo que es la modalidad PC Shared para equipos compartidos y se diseñaron políticas de Intune que se encuentran orientadas al control de software, restricciones de ejecutables y parámetros de seguridad.

Puesto que Entra ID e Intune operan de forma íntegra en la nube, las configuraciones aplicadas en las máquinas virtuales son idénticas a las que adoptarían los equipos reales del laboratorio si fueran inscritos en los mismos grupos de seguridad, por ello, dicho entorno de

forma virtual ha permitido construir un prototipo de forma controlada y transferible al contexto real.

Fase 3. Implementación del prototipo en laboratorio

El prototipo se aplicó en tres máquinas virtuales configuras para simular equipos de laboratorio, mediante un muestreo intencional, dado que la disponibilidad limitada de los dispositivos físicos. En cada máquina virtual se han aplicado configuraciones planificadas del prototipo, siguiendo el mismo proceso que se ejecutaría en un equipo real:

- Inscripción del dispositivo mediante en Microsoft Entra Joined
- Asignación de grupos de seguridad
- Activación de la modalidad PC Shared
- Aplicación de directivas desde Microsoft Intune
- Configuración de restricción de seguridad y control de aplicaciones

Esta fase ha permitido replicar fielmente el comportamiento que se espera en los equipos físicos del laboratorio, puesto que las soluciones en la nube de Entra ID e Intune aplicas las mismas políticas y configuraciones tantos en los dispositivos virtuales como en los dispositivos reales.

Fase 4. Evaluación comparativa antes-después

Una vez que se implementó el prototipo en el entorno virtualizado del laboratorio, se procedió a comparar el estado inicial del laboratorio con el estado obtenido tras la intervención. Se analizaron los indicadores como dispositivos registrados, políticas aplicadas, nivel de restricciones, visibilidad en consola, estado de cumplimiento y el nivel general de seguridad. Esta fase permitió identificar los cambios generados por la aplicación del prototipo y evaluar así su impacto sobre la administración tecnológica del laboratorio, teniendo en cuenta que las políticas y configuraciones aplicadas en el entorno virtual son equivalentes a las que adoptarían los dispositivos reales al ser inscritos en la plataforma de Microsoft Entra ID e Intune.

3.3 Técnicas e Instrumentos de Recolección de Datos

3.3.1 Técnicas

Para la recolección de datos se emplearon técnicas acordes con la naturaleza tecnológica y cuasiexperimental de la investigación.

a. Observación directa

Se ha realizado una observación de forma sistemática del estado inicial del laboratorio, permitiendo identificar aspectos claves para establecer la línea base comparativa:

- Las condiciones y configuraciones iniciales de los dispositivos
- Accesos disponibles para los usuarios
- Ausencia de políticas centralizadas de administración
- Libertad de instalación de software sin un control institucional

Esta observación se realizó de manera sistemática, para garantizar su comparabilidad con el estado posterior a la intervención.

b. Registro técnico

A continuación, se aplicó la técnica de registro técnico, que se encuentra fundamentada en la información generada por las plataformas Microsoft Entra ID y Microsoft Intune. Estas herramientas han permitido recopilar:

- Inscripción y estado de los dispositivos
- Grupos de seguridad configurados
- Políticas aplicadas desde Intune
- Restricciones y parámetros de seguridad establecidos
- Estados de cumplimiento
- Visibilidad del dispositivo dentro del entorno de administración

La evidencia obtenida mediante estas plataformas constituyó el insumo principal para el análisis posterior del prototipo.

c. Análisis comparativo

Así mismo, se aplicó un método de análisis comparativo, mediante la cual se contrastó el estado inicial del laboratorio con el estado posterior a la implementación. Esta revisión contrastada hizo posible reconocer los cambios alcanzados:

- Administración centralizada
- Control de accesos e identidades
- Gestión de monitoreo de dispositivos
- Niveles de seguridad y cumplimiento

El uso de los datos generados de los portales de administración de Microsoft garantizó la precisión y la fiabilidad de la comparación que se realizó de pre-post.

3.3.2 Instrumentos

Para la recolección y organización de los datos se han empleado los siguientes instrumentos:

- Capturas de pantalla, se han utilizado para documentar visualmente el estado inicial y final de la configuración en Microsoft Entra ID e Intune.
- Reportes técnicos generados por las plataformas Microsoft Entra ID e Intune, los cuales han proporcionado información verificable sobre la inscripción de los dispositivos, políticas aplicadas, estados de cumplimiento y visibilidad del entorno.
- Registro del sistema que se obtuvieron mediante los comandos ejecutados en PowerShell, empleados para validad los procesos de inscripción, las sesiones de usuario y los cambios de configuración.
- Matriz comparativa, diseñada para la organización de los indicadores pre y post intervención, facilitando el análisis estructurado de los cambios ocasionado por el prototipo.

El uso de estos instrumentos ha permitido obtener información de forma precisa, verificable y que se encuentra directamente relacionada con el comportamiento del prototipo tecnológico, garantizando así la consistencia y la validez del análisis final.

3.4 Población y Muestra

3.4.1 Población

La población de estudio estuvo integrada por los equipos informáticos, las cuentas institucionales, los recursos tecnológicos y los componentes de infraestructura que forman parte de los laboratorios de Dirección de las Tecnologías Información y Comunicación en la Universidad Nacional de Chimborazo. Este conjunto constituye el entorno donde se identificó la problemática y donde se evaluó la efectividad del prototipo desarrollado.

3.4.2 Muestra

La muestra utilizada fue de tipo no probabilístico e intencional y estuvo conformada por tres máquinas virtuales configuradas para simular las condiciones operativas de los equipos del laboratorio 404 de la DTIC. Estas máquinas virtuales se seleccionaron debido a la disponibilidad limitada de los equipos físicos y porque el trabajar con plataformas de administración en la nube como Microsoft Entra ID e Intune, los procesos de inscripción, aplicación de políticas y la gestión de la seguridad se ejecutan de forma equivalente en los dispositivos virtuales y reales.

3.4.3 Operaciones de Variables

Para este estudio se definieron dos variables clave: la variable independiente corresponde al prototipo de administración centralizada mediante Microsoft Entra ID e Intune; y la variable dependiente se relaciona con el nivel de gestión, control y seguridad de los laboratorios. La operacionalización de variables se muestra a continuación en la **¡Error! No se encuentra el origen de la referencia.**:

Tabla 1. Operacionalización de las variables del estudio para la evaluación del prototipo de administración centralizada de identidades y dispositivos en el laboratorio

Fuente: Autor

Variable	Descripción	Indicadores	Técnicas e Instrumentos
Independiente	Prototipo basado en la inscripción de dispositivos, aplicación de políticas y administración centralizada en la nube.	-Dispositivos inscritos con Entra Joined. -Grupos de seguridad creados. -Políticas aplicadas desde Intune.	-Observación directa. -Registro técnico desde los portales de Entra ID e Intune. -Comprobaciones de estado mediante comando PowerShell.

		Restricciones configuradas. -PC Shared habilitado.	-Capturas de pantalla como evidencia documentada.
Dependiente	Nivel de gestión y seguridad logrado tras la implementación del prototipo.	-Cantidad de dispositivos gestionados. -Nivel de restricciones aplicadas. -Estado de cumplimiento del dispositivo. -Visibilidad del estado en el que se encuentra el dispositivo. -Administración de la instalación del software.	-Matriz comparativa pre-post. -Evidencia documentada mediante capturas y verificaciones técnicas en lo que corresponde a PowerShell.

3.5 Hipótesis

La hipótesis plantea que la implementación del prototipo de administración centralizada basada en Microsoft Entra ID e Intune aplicado en lo que es un entorno virtualizado que se encarga de replicar las condiciones de laboratorio, mejora de forma significativa lo que es la gestión de identidades y las condiciones de laboratorio en comparación con el estado inicial.

3.6 Métodos de Análisis y Procesamiento de Datos

El análisis de los datos se realizó mediante estadística descriptiva, utilizando valores numéricos obtenidos antes y después de la implementación del prototipo. Para ello, se emplearon indicadores cuantificables tales como número de dispositivos gestionados, cantidad de políticas aplicadas, equipos configurados con PC Shared y restricciones de seguridad activas, se ha trabajado mediante Excel y SPSS.

La información se ha organizado en tablas comparativas de tipo Pre-Post, representada a través de un gráfico de líneas permitiendo visualizar de una forma objetiva los cambios generados después de la intervención en el entorno virtualizado.

De igual forma, el análisis se ha fortalecido con una interpretación de forma técnica de las variaciones identificadas en cada indicador, valorando así el efecto del prototipo en la gestión centralizada del laboratorio en donde el enfoque cuantitativo descriptivo es adecuado para estudios experimentales con muestras pequeñas, puesto que permite identificar diferencias significativas en el comportamiento de los sistemas antes y después del tratamiento sin requerir un análisis estadístico inferencial.

CAPÍTULO IV.

4. RESULTADOS Y DISCUSIÓN

4.1 Introducción a los resultados

Se presentan los resultados obtenidos, tras la implementación del prototipo de administración centralizada basada en Microsoft Entra ID e Intune, desarrollado en un entorno controlado de máquinas virtuales que replican las condiciones de los equipos del laboratorio 404 de la DTIC. Este entorno virtualizado ha constituido una unidad de análisis adecuada para evaluar los efectos del prototipo en condiciones operativas comparables al uso real en el laboratorio.

El propósito de este análisis consiste en comparar el estado inicial que vendría a ser el (pre) de los dispositivos con su estado posterior a la intervención que vendría a ser el (post), utilizando indicadores relacionados con la administración de identidades, métodos de inicio de sesión, inscripción de dispositivos, el nivel general de la seguridad y el control del software. Dicho análisis se desarrolla bajo un diseño cuasiexperimental, ya que evalúa los cambios que se obtuvieron en los mismos dispositivos tanto antes como después de la implementación del prototipo en los dispositivos virtualizados.

4.1.1 Introducción a los resultados del cuestionario CAPA

Este capítulo presenta los hallazgos obtenidos tanto del cuestionario CAPA (Conocimiento, Actitud, Práctica y Aptitud) como del análisis comparativo realizado antes y después de la implementación del prototipo de administración centralizada en el laboratorio 404.

Ya que el cuestionario CAPA opera como un insumo complementario que se encarga de recoger la percepción técnica y operativa de los administradores, sus resultados se encargan de exponer en primera instancia proporcionando así un marco interpretativo previo en lo que son aspectos técnicos del prototipo. Además, describen los resultados cuantitativos asociados a los indicadores definidos para evaluar el funcionamiento y la efectividad del sistema implementado.

4.1.2 Resultados descriptivos por dimensión

El cuestionario CAPA se aplicó a dos administradores del Departamento de Tecnologías de la Información y Comunicación (DTIC) con el objetivo de valorar su nivel de conocimiento, actitud, práctica y aptitud en relación con el uso del prototipo de administración centralizada implementado mediante Microsoft Entra ID y Microsoft Intune. Este instrumento permitió obtener percepciones directas de quienes gestionan operativamente el laboratorio, aportando así una visión complementaria a los resultados técnicos obtenidos en las fases previa y posterior a la intervención.

Es de vital importancia destacar que CAPA hace referencia las dimensiones evaluadas por el cuestionario mientras que el coeficiente Kappa corresponde a lo que es una prueba estadística empleada más adelante, útil para determinar la concordancia entre los evaluadores. Aunque ambos forman parte del análisis responden a propósitos diferentes dentro del proceso evaluativo y no deben considerar términos equivalentes.

4.1.3 Estructura y propósito del cuestionario CAPA

Los resultados del cuestionario CAPA se organizan en lo que corresponde a cuatro dimensiones clave:

- Conocimiento (K)
- Actitud (A)
- Práctica (P)
- Aptitud (AA).

Cada una de las categorías mencionadas permiten evaluar desde la percepción del administrador aspectos relacionados con los siete indicadores técnicos del prototipo: equipos registrados, configuración de grupos de seguridad, método de inicio de sesión, gestión de identidades, uso de PC Shared, control de instalación de aplicaciones y nivel global de seguridad.

El uso de ítems redactados en primera persona permite de manera más fácil identificar el grado de dominio técnico, la valoración subjetiva, la disposición para utilizar el prototipo y la capacidad operativa que los administradores consideran tener para que de esta manera el cuestionario CAPA se convierta en un complemento de forma esencial en lo

que es el análisis experimental puesto que permite integrar tanto la dimensión técnica como la dimensión humana del proceso de implementación.

Posteriormente, se incorpora el cálculo de coeficiente Kappa en donde cuyo propósito es determinar en nivel de concordancia entre las respuestas de los dos administradores y con ello estimar la consistencia interna del instrumento aplicado.

4.1.4 Escala de valoración utilizada (Likert)

Con el fin de facilitar la comprensión de los resultados obtenidos, las respuestas del cuestionario se organizaron en cuatro tablas correspondientes a las dimensiones de Conocimiento (K), Actitud (A), Práctica (P) y Aptitud (AA). Cada ítem fue valorado mediante una escala Likert de 1 a 5, definida de la siguiente manera:

1 = Totalmente en desacuerdo

2 = En desacuerdo

3 = Neutral

4 = De acuerdo

5 = Totalmente de acuerdo

La utilización de esta escala permite analizar no solo el sentido de la respuesta, sino también el grado de intensidad del acuerdo o desacuerdo. Su empleo es habitual en instrumentos tipo CAPA, ya que facilita el análisis descriptivo, el cálculo de medias y la comparación entre dimensiones evaluadas.

Las tablas de los resultados se encargan de presentar las puntuaciones por cada evaluador a los ítems que están vinculados con los siete indicadores del prototipo permitiendo identificar las tendencias de respuesta, niveles de aceptación, comprensión técnica y la percepción de la seguridad operativa.

Además, se calcularán lo que son los promedios por dimensión y se incorporará un gráfico comparativo seguido de lo que es el análisis de concordancia entre los evaluadores utilizando el coeficiente Kappa.

4.1.5 Tablas descriptivas por dimensión

A continuación, se presentarán las tablas descriptivas que corresponden a las cuatro dimensiones evaluadas mediante el cuestionario CAPA: Conocimiento (K) en la **¡Error! No s e encuentra el origen de la referencia.**, Actitud (A) en la **¡Error! No se encuentra el**

origen de la referencia., Práctica (P) en la **¡Error! No se encuentra el origen de la referencia.** y Aptitud (AA) en la **¡Error! No se encuentra el origen de la referencia.**. Estas tablas se encargan de recoger valores otorgados por los dos administradores del Departamento de Tecnologías de la Información y Comunicación (DTIC) del laboratorio 404 de la Universidad Nacional de Chimborazo, quienes participaron en la evaluación del prototipo de la administración centralizada. La presente organización de información por dimensión permite identificar los patrones de respuesta, niveles de dominio técnico, percepciones respecto al funcionamiento del sistema y la capacidad operativa atribuida al uso de Microsoft, Entra ID y Microsoft Intune.

Tabla 2. Resultados descriptivos de la dimensión Conocimiento (K) obtenidos a partir del cuestionario CAPA aplicado a los administradores de la DTIC para la evaluación del prototipo de administración centralizada

Fuente: Autor

Código	Ítem	Adm. 1	Adm. 2
K1	Conoce el proceso de registro de dispositivos en Intune	5	4
K2	Comprende la configuración de grupos de seguridad	5	4
K3	Comprende el funcionamiento del inicio de sesión Entra ID	5	5
K4	Entiende la gestión de identidades	5	5
K5	Conoce el modo PC Shared	5	5
K6	Comprende las restricciones de aplicaciones	5	4
K7	Conoce el nivel general de seguridad	4	4

Tabla 3. Resultados descriptivos de la dimensión Actitud (A) obtenidos a partir del cuestionario CAPA aplicado a los administradores de la DTIC para la evaluación del prototipo de administración centralizada

Fuente: Autor

Código	Ítem	Adm. 1	Adm. 2
A1	Considera beneficioso registrar dispositivos	5	5
A2	Considera útiles los grupos de seguridad	5	5
A3	Valora el inicio de sesión institucional	5	5
A4	Valora gestionar identidades desde Entra ID	5	5
A5	Considera adecuado el PC Shared	5	5
A6	Cree que las restricciones mejoran la seguridad	5	5
A7	Considera apropiado el nivel de seguridad	5	5

Tabla 4. Resultados descriptivos de la dimensión Práctica (P) obtenidos a partir del cuestionario CAPA aplicado a los administradores de la DTIC para la evaluación del prototipo de administración centralizada

Fuente: Autor

Código	Ítem	Adm. 1	Adm. 2
P1	Implementaría el registro de dispositivos	5	5
P2	Aplicaría grupos de seguridad	5	5
P3	Configuraría inicio de sesión institucional	4	5
P4	Gestionaría identidades desde Entra ID	5	5

P5	Activaría PC Shared	5	5
P6	Aplicaría restricciones de aplicaciones	5	5
P7	Mantendría el nivel de seguridad definido	5	5

Tabla 5. Resultados descriptivos de la dimensión Aptitud (AA) obtenidos a partir del cuestionario CAPA aplicado a los administradores de la DTIC para la evaluación del prototipo de administración centralizada

Fuente: Autor

Código	Ítem	Adm. 1	Adm. 2
AA1	Capacidad para aplicar configuraciones	5	4
AA2	Capacidad para interpretar información técnica	5	4
AA3	Capacidad para gestionar equipos en la nube	5	4

4.1.6 Promedios por dimensión y gráfico comparativo

Con la finalidad de sintetizar los resultados obtenidos del cuestionario CAPA, se calcularon los promedios de cada una de las cuatro dimensiones evaluadas: Conocimiento (K), Actitud (A). Práctica (P) y Aptitud (AA). Los promedios se obtuvieron a partir de las puntuaciones otorgadas por los administradores participantes, tomando como referencia a la escala Likert de 1 a 5. Estos valores permiten identificar el nivel general de dominio percibido en cada dimensión, así como comparar el grado de coherencia que hay entre ambas evaluaciones.

Tabla 6. Promedios obtenidos por dimensión del cuestionario CAPA aplicados por los administradores de la DTIC para la evaluación del prototipo de administración centralizada de identidades y dispositivos en la nube

Fuente: Autor

DIM	ADM1_mean	ADM2_mean
A	5	5
AA	5	4
K	4,86	4,43
P	4,86	5

La **¡Error! No se encuentra el origen de la referencia.** muestra los promedios o btenidos por ambos administradores en cada una de las dimensiones del cuestionario CAPA. En conclusión, los puntajes son altos, evidenciando un nivel favorable de conocimiento, actitud, prácticas y aptitud frente al uso del prototipo implementado. Las dimensiones A (Actitud) y AA (Aptitud) presentan los valores más diferenciados entre los administradores, mientras que las dimensiones K (Conocimiento) y P (Prácticas) reflejan los resultados similares, con unas ligeras variaciones.

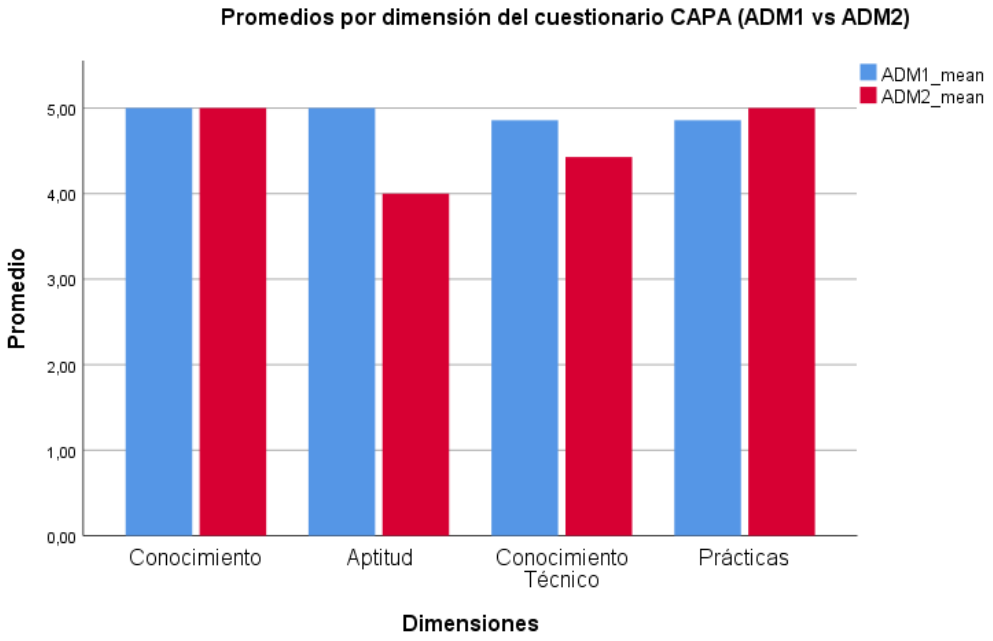


Figura 7. Comparación en SPSS calculados en la escala de Likert de 1 a 5 de los promedios por dimensión del cuestionario CAPA entre los administradores ADM1 y ADM2 en la evaluación del prototipo de administración centralizada de identidades y dispositivos

Fuente: Autor

La **¡Error! No se encuentra el origen de la referencia.** compara visualmente los p romedios por dimensión entre ambos administradores. Se puede observar que ambos presentan un desempeño consistente en las cuatro categorías evaluadas, manteniendo así los puntajes cercanos entre sí. Las mayores diferencias se evidencian en las dimensiones de Aptitud y Conocimiento Técnico, mientras que en lo que respecta a Prácticas y Actitud los valores son prácticamente equivalentes.

4.1.7 Coeficiente Kappa: análisis de concordancia

Tabla 7. Tabla cruzada de frecuencias entre las puntuaciones otorgadas por los administradores ADM1 y ADM2 en el cuestionario CAPA para la evaluación del prototipo de administración centralizada

Fuente: Autor

Tabla cruzada ADM1*ADM2

	ADM2	Total

			4,00	5,00	
ADM 1	4,00	Recuento	1	1	2
		% dentro de ADM1	50,0%	50,0%	100,0%
		% dentro de ADM2	14,3%	5,9%	8,3%
	5,00	Recuento	6	16	22
		% dentro de ADM1	27,3%	72,7%	100,0%
		% dentro de ADM2	85,7%	94,1%	91,7%
Total		Recuento	7	17	24
		% dentro de ADM1	29,2%	70,8%	100,0%
		% dentro de ADM2	100,0%	100,0%	100,0%

La **¡Error! No se encuentra el origen de la referencia.** muestra lo que es la d istribución conjunta de las respuestas del ADM1 Y ADM2 observando así que la mayoría de los ítems fueron valorados con la puntuación 5 por ambos administradores, pero también existen diferencias puntuales donde ADM2 asignó en lo que es la categoría 4, como consecuencia estas variaciones reflejan las discrepancias moderadas en lo que es la percepción de algunos aspectos evaluados del prototipo. Evidenciando una alta coincidencia en las respuestas de ambos administradores y reflejando que los resultados obtenidos son muy buenos.

Tabla 8. Medidas simétricas del coeficiente Kappa de concordancia entre los administradores ADM1 y ADM2 obtenidas mediante el análisis estadístico en SPSS para la evaluación del cuestionario CAPA

Fuente: Autor

Medidas simétricas

		Valor	Error estándar asintótico[a]	T aproximada[b]	Significación aproximada
Medida de acuerdo	Kappa	0,106	0,180	0,677	0,498
N de casos válidos		24			

a. No se presupone la hipótesis nula.

b. Empleo del error estándar asintótico basado en la suposición de la hipótesis nula.

Como se puede evidenciar en la **¡Error! No se encuentra el origen de la referencia.** e l coeficiente Kappa (k=0,106; p=0,498) indica un nivel débil entre los administradores, lo cual es esperable ya que el número reducido de evaluadores (N=2), disminuye la estabilidad del estadístico y genera valores bajos incluso cuando las respuestas son muy similares. Aun así, es importante destacar que ambos administradores calificaron casi todos los valores entre 4 y 5 en escala de Likert, reflejando una muy buena valoración general del prototipo y de las dimensiones evaluadas.

4.2 Prueba Chi-Cuadrado

Tabla 9. Resultados de la prueba de chi-cuadrado aplicada a las evaluaciones realizadas por los administradores ADM1 y ADM2 para analizar la asociación entre sus valoraciones en el cuestionario CAPA

Fuente: Autor

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	,458[a]	1	,498		
Corrección de continuidad[b]	,000	1	1,000		
Razón de verosimilitud	,420	1	,517		
Prueba exacta de Fisher				,507	,507
Asociación lineal por lineal	,439	1	,507		
N de casos válidos	24				

a. 2 casillas (50,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,58

b. Sólo se ha calculado para una tabla 2x2

Los resultados de la prueba Chi-Cuadrado en la **¡Error! No se encuentra el origen de la referencia.** muestran que no existe como tal una asociación estadísticamente significativa entres las respuestas de ADM1 y ADM2 ($\chi^2 = 0{,}458$; $p = 0{,}498$), indica que ambos evaluadores otorgaron valores dentro de un patrón consistentes y estable. Aunque no se identificó dependencia entre las variables, el comportamiento homogéneo de las puntuaciones refleja una adecuada coherencia en la percepción general de los evaluadores, alineado con las altas valoraciones registras en la escala Likert.

4.3 Proceso de realización del prototipo

En la siguiente sección se detalla el proceso a través del cual se llevó a cabo la elaboración del prototipo de administración centralizada en el entorno institucional permitiendo evidenciar su funcionamiento real.

Paso 1: En un inicio se crearon tres máquinas virtuales en Oracle VirtualBox, como se muestra en la **¡Error! No se encuentra el origen de la referencia.**, siguiendo una n omenclatura estandarizada como LABXPC404 para la identificación de los dispositivos las cuales simulan las condiciones del laboratorio 404 de la DTIC en donde cada máquina fue

instalada con Windows 11 Pro **¡Error! No se encuentra el origen de la referencia.**, versión r equerida para habilitar las funciones de administración y permitir su incorporación a Microsoft Entra ID e Intune.

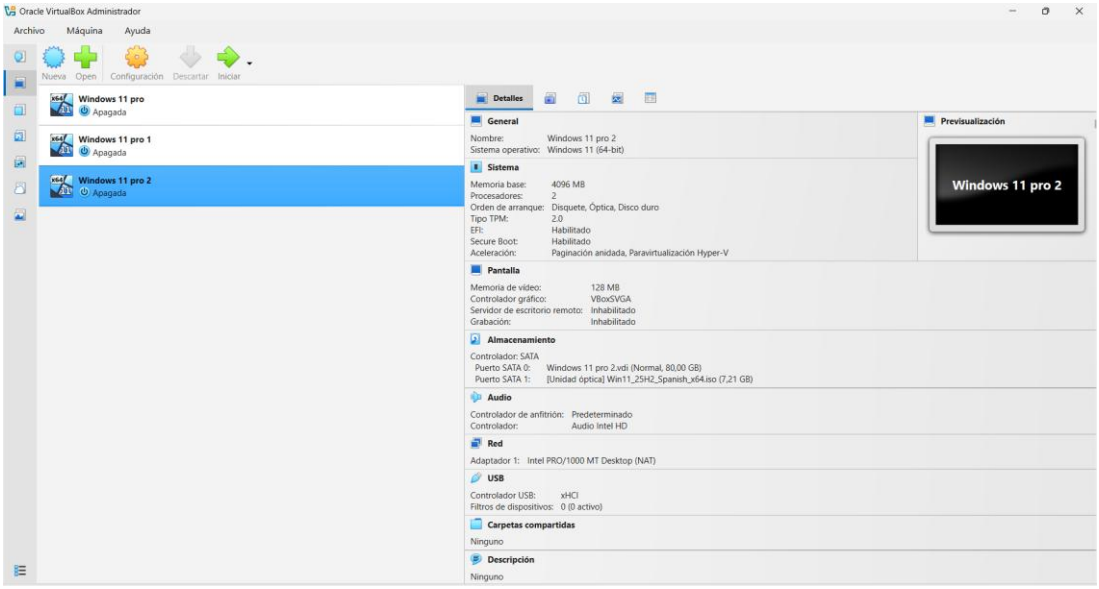


Figura 8. Creación y configuración inicial de las máquinas virtuales en Oracle VirtualBox para la simulación del entorno de laboratorio de la DTIC previo a su integración con Microsoft Entra ID e Intune

Fuente: Autor

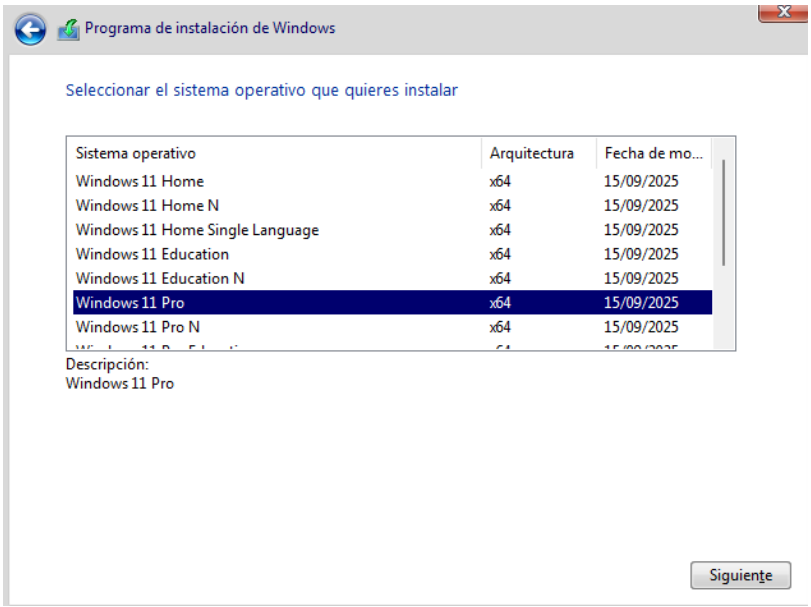


Figura 9. Selección e instalación del sistema operativo Windows 11 Pro como requisito para la administración centralizada de dispositivos mediante Microsoft Entra ID e Intune

Fuente: Autor

Paso 2: Se procedió a la creación de Grupos de Seguridad en Microsoft Entra ID para la organización tanto de los usuarios del laboratorio como los dispositivos, como se observa en la **¡Error! No se encuentra el origen de la referencia.**, ya que estos grupos p ermiten segmentar y seccionar las políticas de configuración, acceso y seguridad. De este modo, se garantiza que cada conjunto de usuarios y equipos solo se le asignen las directivas correspondientes a su rol.

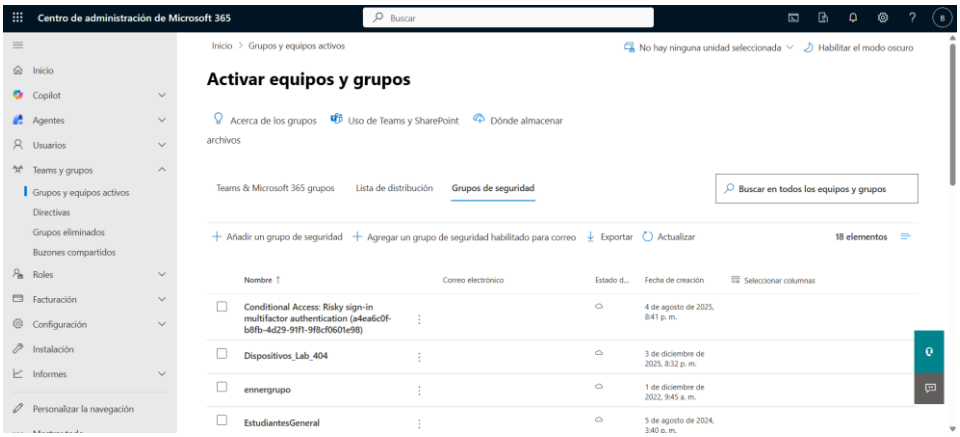


Figura 10. Creación y administración de grupos de seguridad en Microsoft Entra ID para la segmentación de usuarios y dispositivos y la aplicación centralizada de políticas de acceso y configuración

Fuente: Autor

Paso 3: En el grupo llamado Usuarios_LAB 404 se designó un propietario y se añadieron 3 usuarios institucionales creados únicamente para el entorno de prueba, como se muestra en la **¡Error! No se encuentra el origen de la referencia.**.

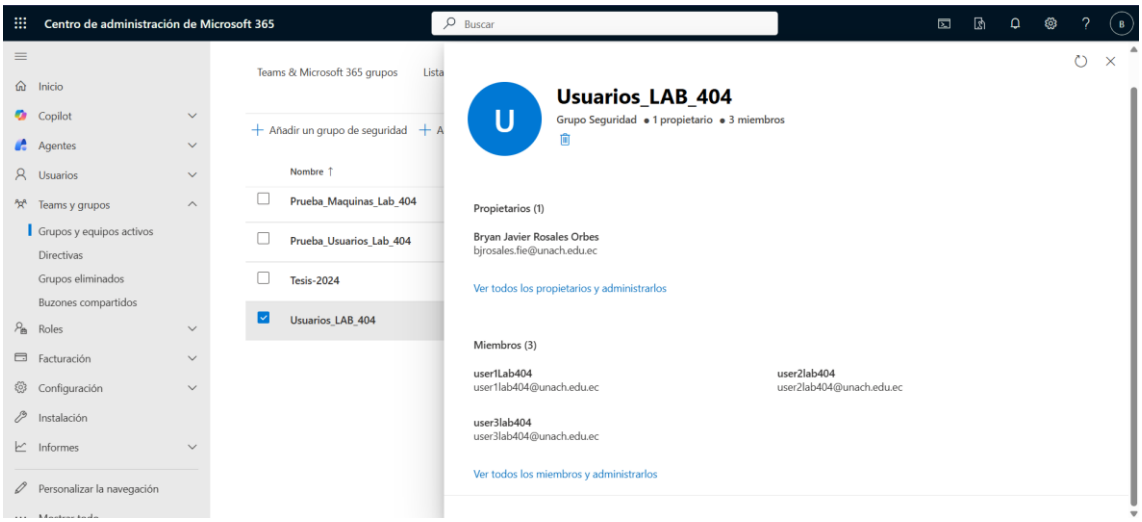


Figura 11. Grupo de seguridad Usuarios_LAB_404

Fuente: Autor

Paso 4: De igual manera dentro del grupo de seguridad Dispositivos_LAB404 se añadieron las máquinas virtualizadas desde el centro de administración de Microsoft Entra, incorporándolas de forma uniforme al esquema de gestión definido para el laboratorio, como se muestra en la **¡Error! No se encuentra el origen de la referencia.**.

Figura 12. Asignación de dispositivos al grupo Dispositivos_LAB_404 en Microsoft Entra

Fuente: Autor

Paso 5: Como se puede observar en la Figura 13, se llevó a cabo el cambio de la autoridad MDM del inquilino, pasando de Microsoft 365 a Microsoft Intune, permitiendo habilitar la administración modernizada de los dispositivos y centralizar por completo la gestión dentro de Intune.

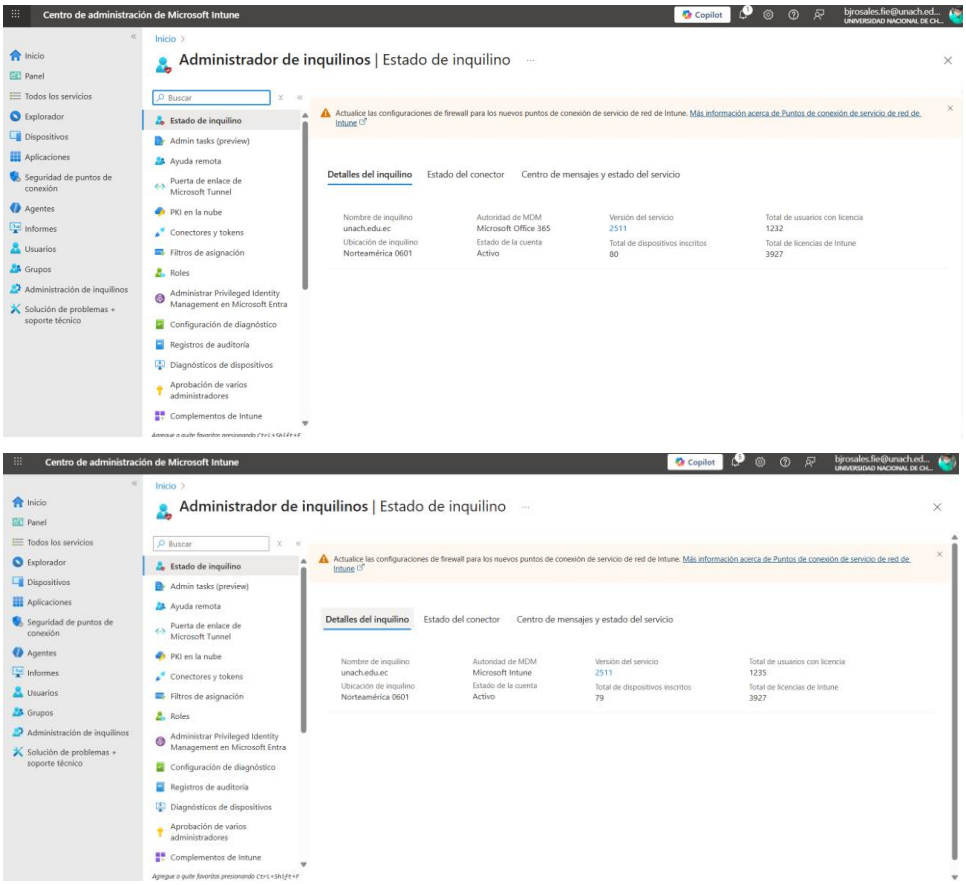


Figura 13. Cambio de la autoridad de administración MDM del inquilino desde Microsoft 365 hacia Microsoft Intune para la gestión centralizada y completa de dispositivos

Fuente: Autor

Es importante resaltar que este cambio se llevó a cabo porque cuando el MDM tiene una autoridad de Microsoft Office 365 el equipo o dispositivo se administra de manera parcial mientras que cuando es manejada con MDM autoridad de Intune se gestiona totalmente.

Paso 6: Al grabar un dispositivo en lo que es el Microsoft Intune, Windows aplica automática configuraciones base mediante CSPs del sistema, lo que habilita la gestión inicial de la máquina sin necesidad de crear políticas adicionales. Para ajustes más avanzados, Intune emplea plantillas por medio de ADMX ingestión permitiendo así aplicar directivas similares a las GPO tradicionales consolidando de esta manera un modelo de administración moderna basado en la nube, como se muestra en la Figura 14.

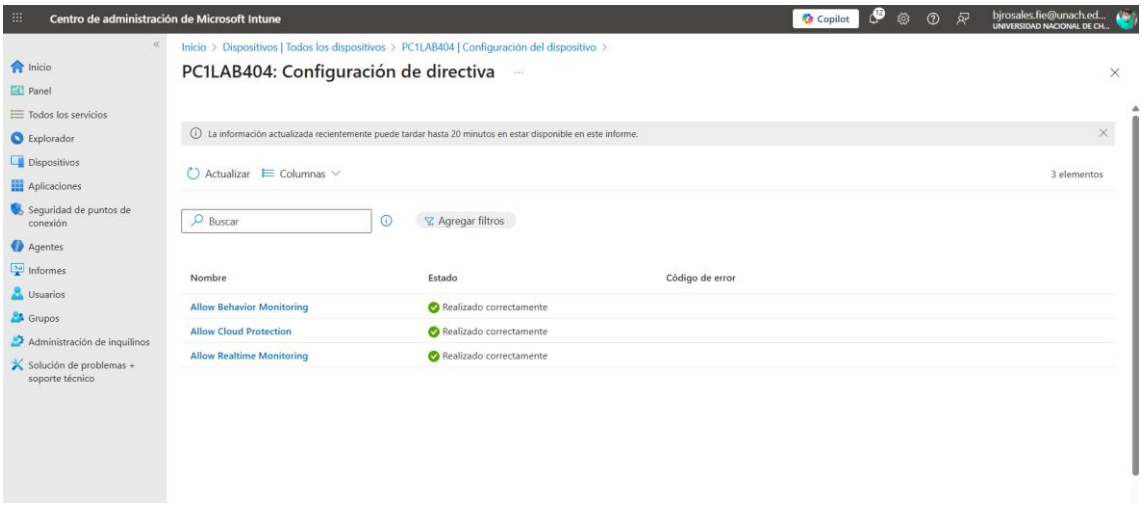


Figura 14. Aplicación automática de configuraciones base y directivas administrativas en un dispositivo inscrito en Microsoft Intune

Fuente: Autor

Paso 7: Se procedió a crear una directiva de Microsoft Defender Antivirus en Intune con el propósito de habilitar la protección basada en la nube y también configurar los parámetros de bloqueo y respuesta avanzada para consolidar la seguridad del dispositivo y velar porque las amenazas sean supervisadas desde los servicios inteligentes de Microsoft, como se muestra en la Figura 15.

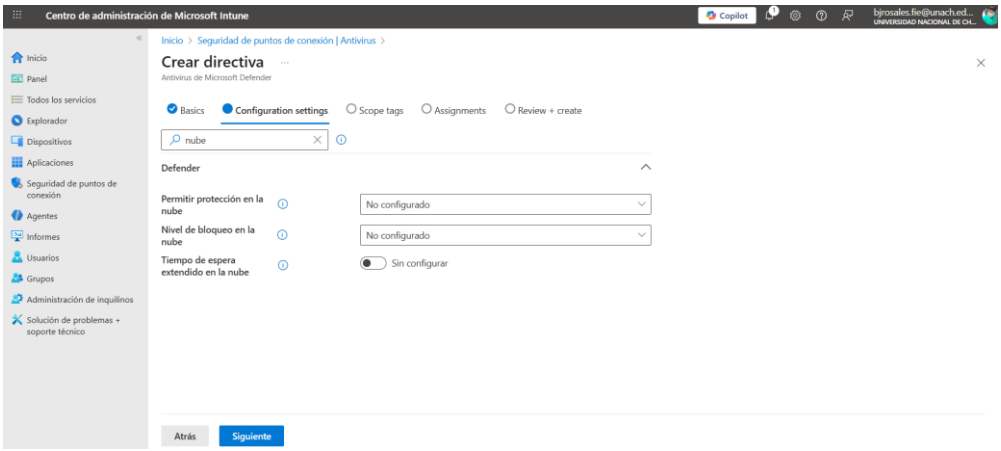


Figura 15. Creación y configuración de una directiva de Microsoft Defender Antivirus en Microsoft Intune

Fuente: Autor

Dentro de la configuración de esta directiva se habilitó la supervisión del comportamiento lo que hace que el antivirus registre actividades extrañas o maliciosas según patrones de comportamiento del sistema mejorando así la protección preventiva del dispositivo, como se puede observar en la Figura 16.

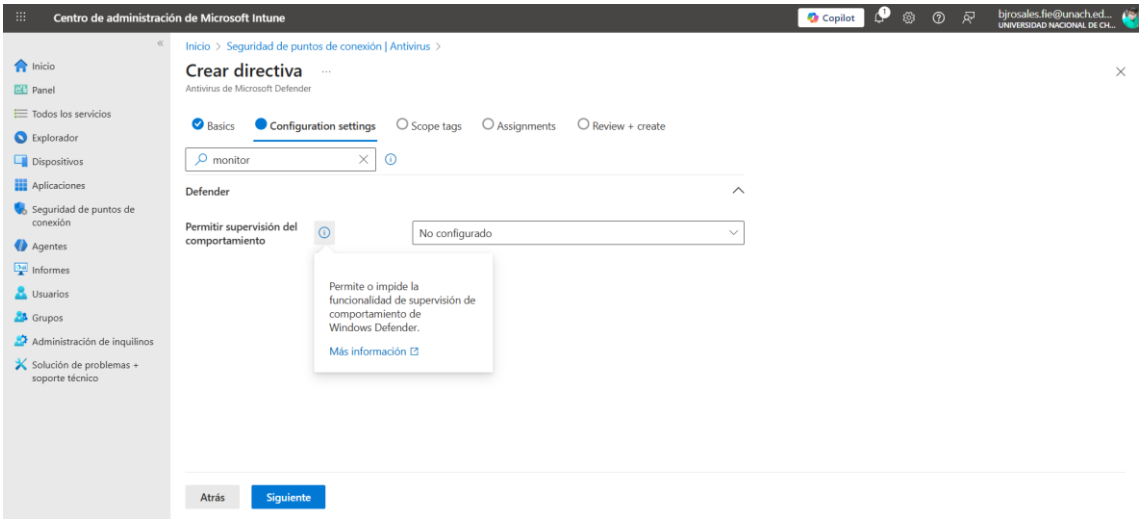


Figura 16. Configuración de la supervisión del comportamiento en Microsoft Defender Antivirus mediante Intune

Fuente: Autor

Finalmente, en la Figura 17 la directiva de antivirus se creó exitosamente y quedó disponible en el módulo de seguridad de puntos de conexión donde se puede supervisar el estado Figura 18 y aplicación en los dispositivos.

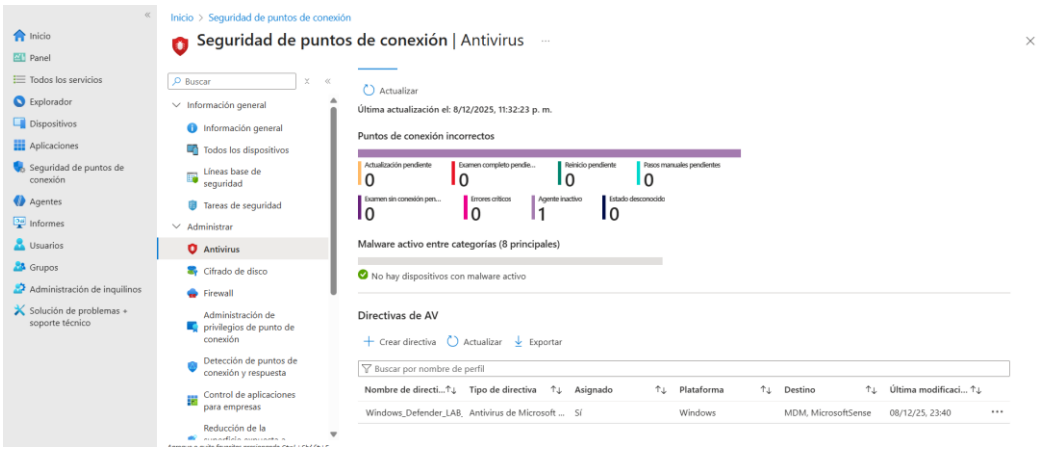


Figura 17. Visualización y monitoreo de la directiva de Microsoft Defender Antivirus en el portal de Microsoft Intune

Fuente: Autor

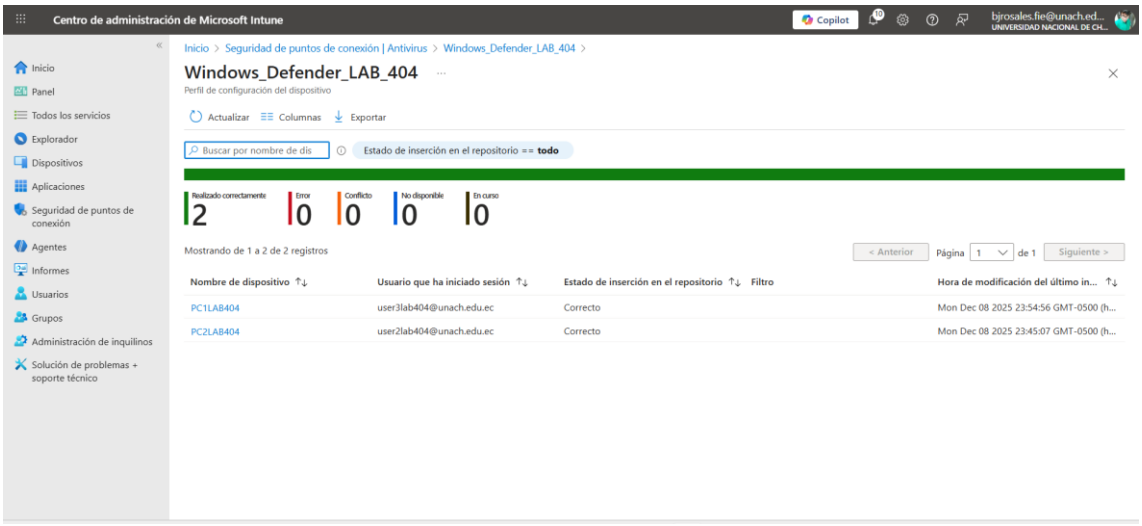


Figura 18. Estado de implementación de la directiva Windows_Defender_LAB_404

Fuente: Autor

Paso 8: En la Figura 19 se creó y aplicó la directiva de PC compartido permitiendo optimizar el uso del equipo cuando es utilizado por varios usuarios en este caso el flujo de estudiantes en un laboratorio.

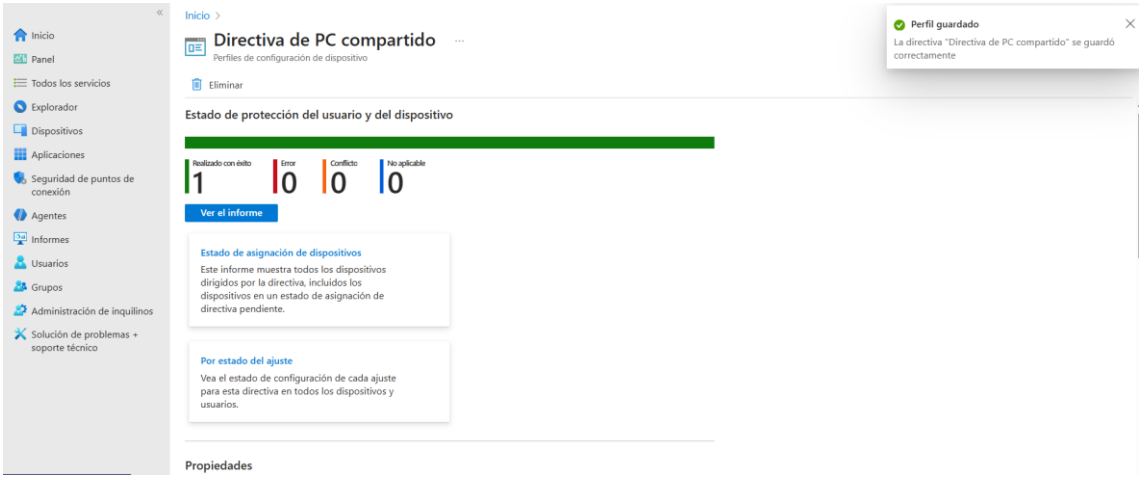


Figura 19. Aplicación y estado de la directiva de PC compartido en un dispositivo administrado mediante Microsoft Intune

Fuente: Autor

Paso 9: De la misma manera en la Figura 20, se evidencia que se realizó la directiva de restricción de aplicaciones en donde se bloquea las instalaciones de aplicaciones ajenas a Microsoft Store en este caso se evidenció con la ejecución del instalador de Steam y mostró

un mensaje de alerta confirmando que las reglas de control de aplicaciones de aplicaron correctamente en el dispositivo y también la instalación centralizada de aplicaciones por Microsoft Intune Extension como se puede evidenciar en la Figura 21.

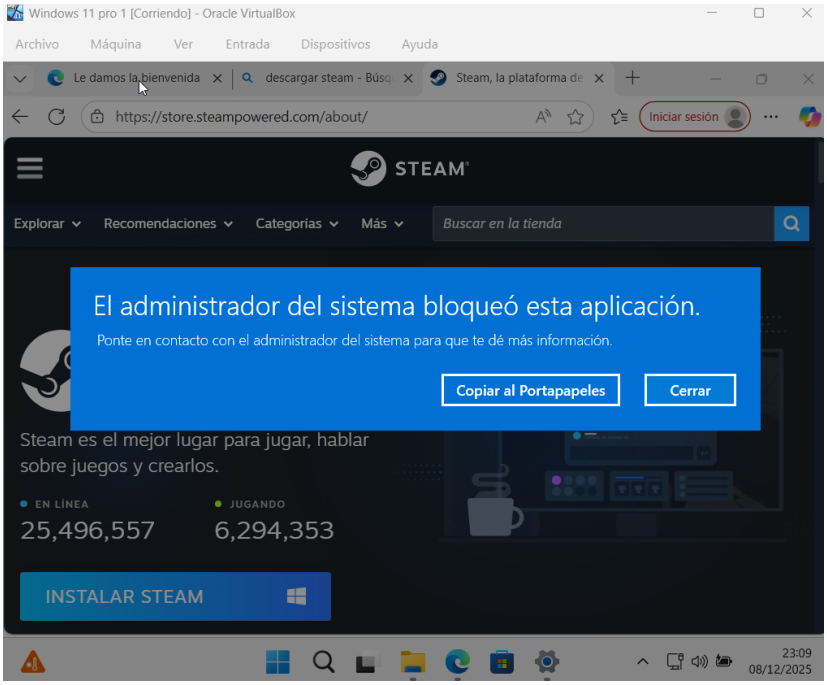


Figura 20. Bloqueo de la instalación de aplicaciones externas a Microsoft Store mediante directivas de Microsoft Intune

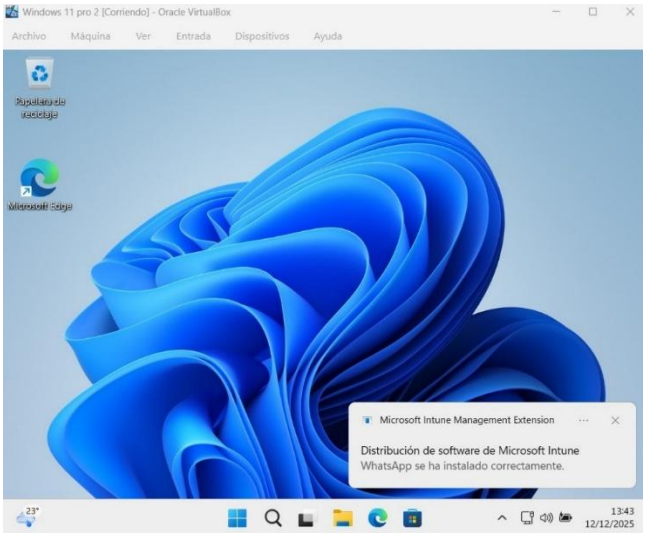


Figura 21. Despliegue e instalación centralizada de aplicaciones mediante Microsoft Intune Management Extension

Fuente: Autor

Paso 10: Se aplicó una política de restricción para bloquear el acceso al Panel de control en los dispositivos administrados evitando que los usuarios hagan cambios no autorizados en la configuración del sistema reforzando de esta manera el control e integridad del laboratorio, como se muestra en la Figura 22.

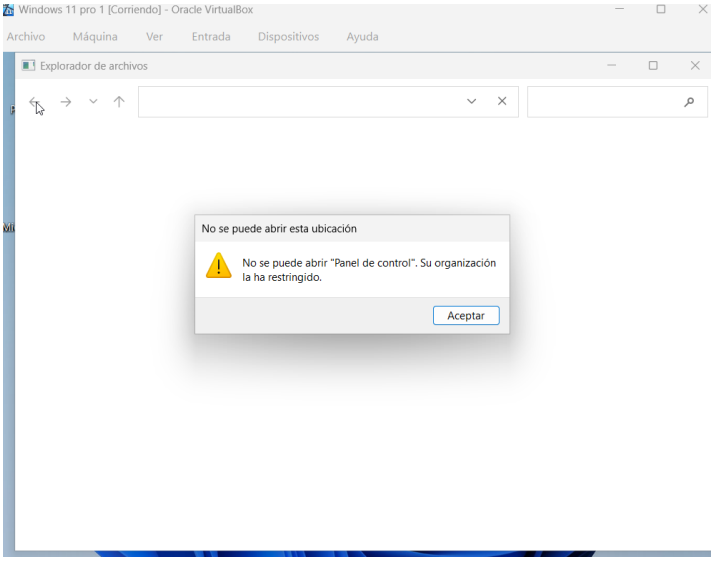


Figura 22. Aplicación de políticas de restricción para el bloqueo del Panel de control en dispositivos administrados mediante Microsoft Intune

Fuente: Autor

Paso 11: De la misma manera para controlar el acceso a las aplicaciones se optó por configurar en Intune una política que bloquea el uso de Microsoft Store en los dispositivos del laboratorio haciendo alusión al escenario en donde permita únicamente la instalación de software autorizado desde la consola de administrador y ningún otro usuario en este caso estudiantes puedan instalar cualquier programa dando como resultado que al intentar abrir la tienda el sistema muestre un mensaje de que el uso está restringido, como se observa en la Figura 23.

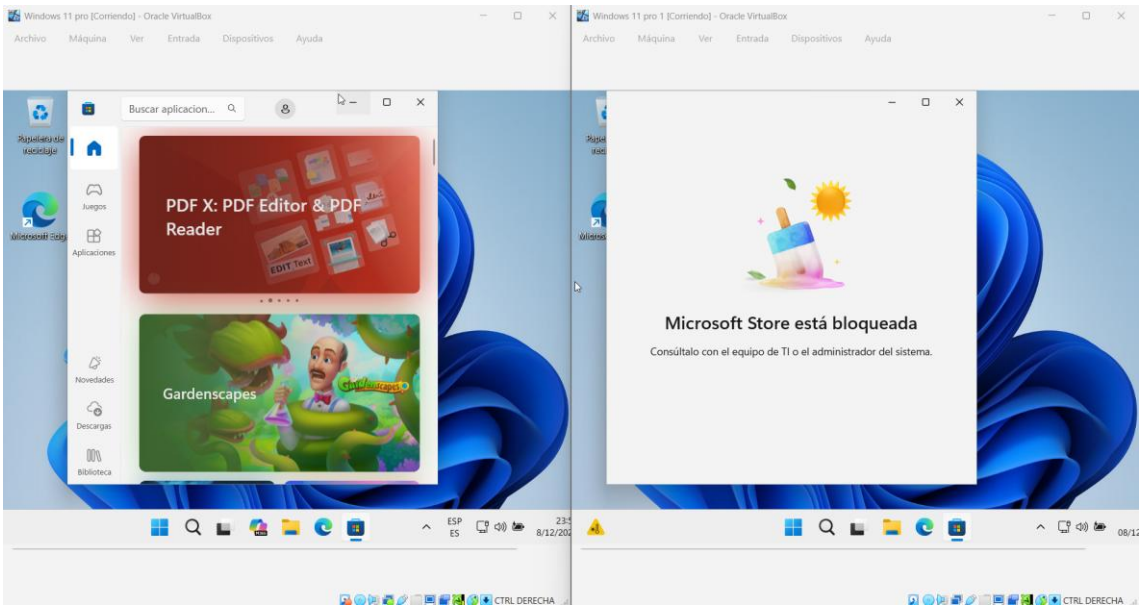


Figura 23. Bloqueo de acceso a Microsoft Store mediante políticas de administración aplicadas desde Microsoft Intune

Fuente: Autor

Paso 12: Complementando el paso anterior asimismo para la instalación centralizada de aplicaciones se utilizó Microsoft Store integrada en Intune, como se evidencia en la Figura 24, permitiendo distribuir programas o software sin necesidad de generar archivos intuwin y simplificando la administración en este caso se añadió la aplicación de Telegram Desktop para su distribución a los usuarios en el entorno de laboratorio.

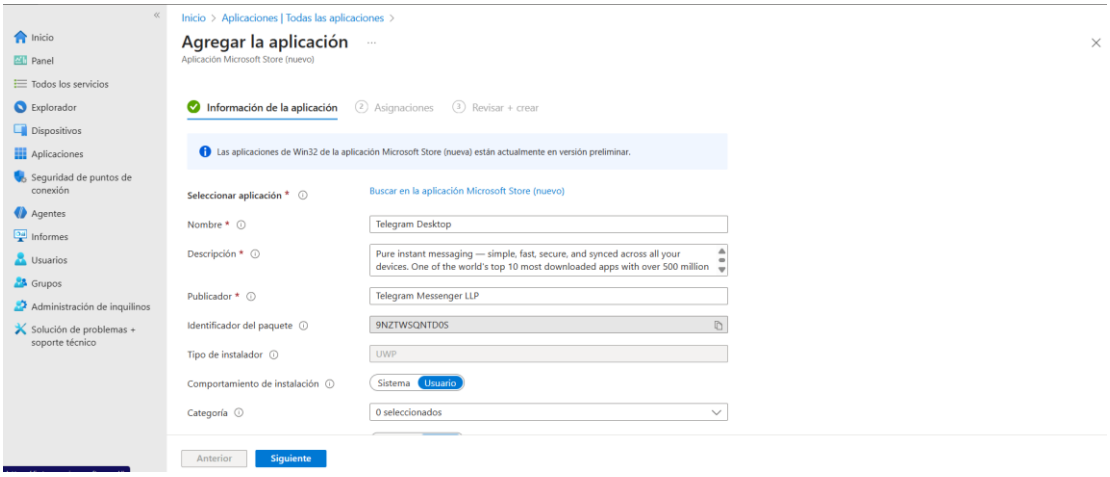


Figura 24. Distribución centralizada de aplicaciones mediante Microsoft Store integrada en Microsoft Intune, sin uso de paquetes .intunewin

Fuente: Autor

Paso 13: Finalmente en la Figura 25, para llevar un control y monitoreo en el portal de Microsoft Entra se puede evidenciar los registros de inicio de sesión de los usuarios del laboratorio mostrando entre accesos exitosos, intentos interrumpidos y la aplicación de las políticas de autenticación confirmando así el funcionamiento adecuado de los usuarios dentro del entorno administrado.

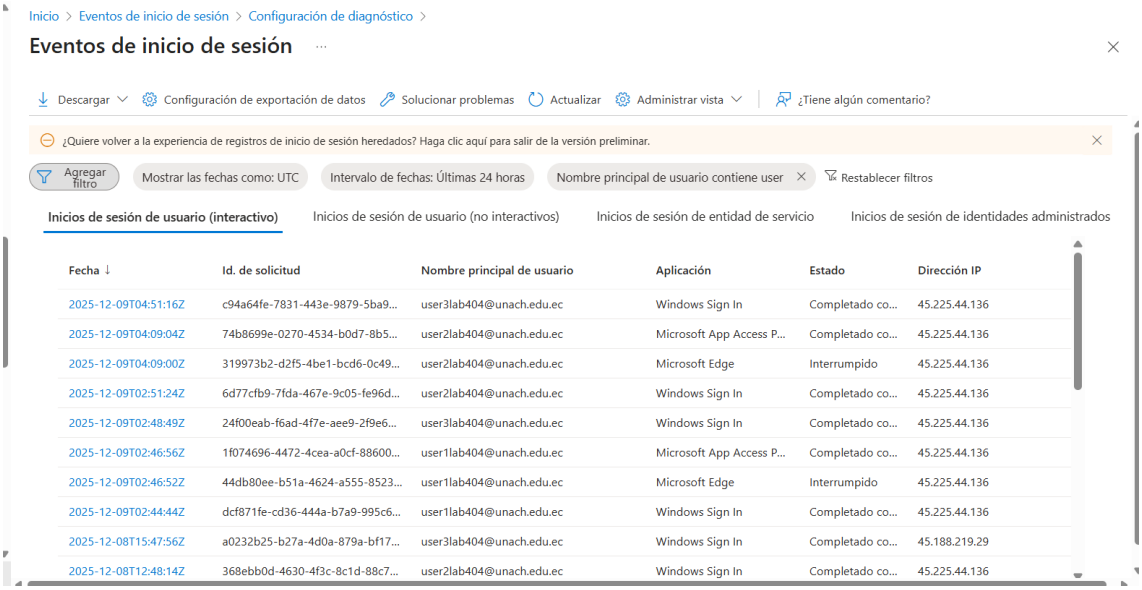


Figura 25. Visualización y monitoreo de registros de inicio de sesión de usuarios en el portal de Microsoft Entra ID

Fuente: Autor

4.4 Resultados comparativos pre-post

En la **¡Error! No se encuentra el origen de la referencia.** se presenta los valores q ue se han registrado antes y después de la implementación del prototipo en las máquinas virtuales configuradas para simular los equipos de laboratorio. Los indicadores permiten visualizar el avance logrado en lo que es la administración centralizada y en la seguridad operativa del entorno evaluado.

Tabla 10. Comparación pre y post implementación de los indicadores técnicos de administración centralizada y seguridad del laboratorio

Fuente: Autor

N°	Indicador	Pre	Post

1	Dispositivos registrados en los laboratorios	0	3
2	Grupos de seguridad configurados en los laboratorios	0	2
3	Método de inicio de sesión en los laboratorios	0	1
4	Gestión centralizada de identidades en los laboratorios	0	3
5	PC Shared (equipos compartidos)	0	3
6	Control de instalación de aplicaciones	0	1
7	Nivel general de seguridad	0	1

4.5 Análisis de los indicadores

4.5.1 Dispositivos registrados

El número de los dispositivos administrados pasó de 0 a 3, puesto que antes de la intervención no existía ningún equipo inscrito en una plataforma de administración centralizada, lo que imposibilitaba ejercer el control, aplicar las políticas o monitoreas el estado operativo. Con la implementación del prototipo, en las máquinas virtuales, los tres dispositivos que se han seleccionado quedaron registrados en Microsoft Intune, habilitando así la administración centralizada del entorno y el seguimiento operativo del entorno evaluado.

4.5.2 Grupo de seguridad configurados

El presente indicador aumentó de 0 a 2. La creación de grupos de seguridad específicos ha permitido organizar las políticas aplicadas a usuarios y dispositivos. Este avance establece una estructura básica de administración, inexistente antes de la intervención.

4.5.3 Método de inicio de sesión

El indicador cambió de 0 a 1, lo que refleja que las cuentas locales sin supervisión fueron sustituidas por un inicio de sesión institucional administrado a través de Microsoft

Entra ID. Este cambio fortalece el control de accesos y facilita el seguimiento de las actividades, asegurando que cada sesión iniciada en los equipos esté asociada a usuarios debidamente autenticados.

4.5.4 Gestión centralizada de identidades

El incremento de 0 a 3 refleja que los tres equipos pasaron a vincularse con identidades institucionales gestionadas desde Entra ID. Debido a este cambio fue posible aplicar un modelo de administración unificado, en el que las cuentas, los permisos y las configuraciones dependen del sistema centralizado y no de cada equipo por separado.

4.5.5 PC Shared (equipos compartidos)

El indicador pasó de 0 a 3, evidenciando que todas las máquinas virtuales fueron configuradas bajo el modo PC Shared. Esta configuración facilita el trabajo con varios usuarios, lo que reduce el riesgo de cambios no autorizados y garantiza una experiencia uniforme.

4.5.6 Control de instalación de aplicaciones

El valor aumentó de 0 a 1, esto señala que anteriormente se permitía instalar software sin restricciones y, tras la intervención, se aplicó una política de control. Esta medida mejora la seguridad al bloquear la ejecución de programas no autorizados y disminuir la posibilidad de malware y prácticas inseguras.

4.5.7 Nivel general de seguridad

El indicador pasó de 0 a 1, reflejando así el cambio de un entorno sin lineamiento ni una supervisión a uno con un nivel elemental de seguridad desde lo que es Intune por lo que aunque represente un progreso importante, este valor pone en evidencia la necesidad de incorporar medidas adicionales como las políticas de cumplimiento, el acceso condicional y la autenticación multifactorial para lograr los niveles altos de protección.

4.5.8 Representación gráfica de los resultados

La Figura 26, representa de forma gráfica las variaciones en los indicadores más relevantes antes y después de la implementación del prototipo. Estos incrementos permiten evidenciar el efecto de la administración centralizada en el entorno evaluado.

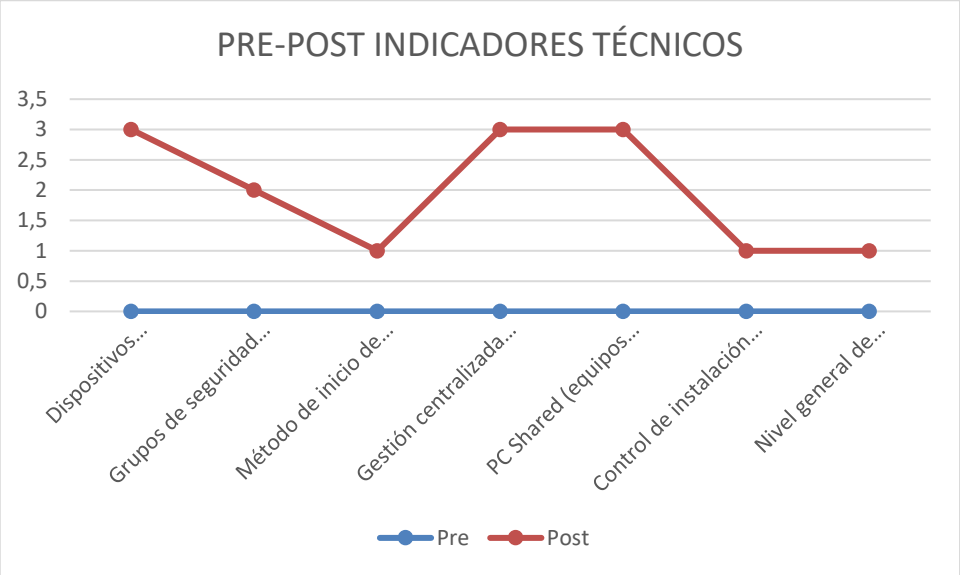


Figura 26. Gráfico comparativo pre y post implementación de los indicadores técnicos de administración centralizada

Fuente: Autor

4.6 Discusión de los resultados

Los resultados muestran que la puesta en marcha del prototipo produjo mejoras relevantes en la administración de los equipos analizados. La incorporación a Microsoft Intune hizo posible aplicar control remoto sobre configuraciones, estados operativos y políticas. Por su parte, la gestión de identidades mediante Microsoft Entra ID reforzó la seguridad al introducir el inicio de sesión institucional y una administración centralizada.

También la activación de PC Shared y restricción en la instalación de las aplicaciones contribuyeron a un mayor orden, estandarización y protección del entorno.

Para finalizar, se pasó de un escenario sin gestión a uno con políticas activas representando un progreso considerable en donde estos hallazgos constituyen un punto de partida para futuras optimizaciones, como la adopción de políticas de cumplimiento, acceso condicional, clasificación de equipos y mecanismos de autenticación más robustos.

CAPÍTULO V.

5. PROPUESTA

5.1 Lineamientos para la implementación institucional

5.1.1 Gestión Centralizada de identidades

Se sugiere centralizar la gestión de identidades de los usuarios de los laboratorios mediante Microsoft Entra ID a fin de que el acceso a los equipos se realice exclusivamente a través de cuentas institucionales y se evite el uso de usuarios locales permitiendo así una administración más eficiente y asimismo contribuir a reforzar el control de accesos y la trazabilidad de las actividades realizadas en los equipos de laboratorio.

5.1.2 Inscripción de dispositivos en una plataforma MDM

Se propone que los equipos destinados a los laboratorios sean inscritos previamente en una plataforma de Mobile Device Management (MDM) como Microsoft Intune con el propósito de garantizar la aplicación automática y consistente de las políticas institucionales, esta práctica facilitaría la administración remota de los dispositivos y reduciría la necesidad de configuraciones manuales, además permitiría mantener un inventario centralizado de los equipos gestionados.

5.1.3 Asignación de políticas mediante grupos de seguridad

Se sugiere la adopción de asignar las políticas de configuración y seguridad mediante grupos de seguridad permitiendo de esta manera que cada usuario o dispositivo reciba únicamente las directivas correspondientes a su rol dentro del entorno de laboratorio, esta segmentación facilitaría una gestión más organizada y escalable de políticas y asimismo permitiría realizar cambios de configuración de forma centralizada sin afectar a otros entornos del tenant.

5.1.4 Uso de perfiles de equipos compartidos

Resulta pertinente implementar perfiles de equipos compartidos en los laboratorios académicos para que no se conserven credenciales ni información de sesiones anteriores en un mismo dispositivo, esto permitiría un uso eficiente de los equipos por múltiples

estudiantes y paralelamente reduciría riesgos asociados al acceso a información residual de sesiones previas.

5.1.5 Restricción de configuraciones críticas del sistema

Se considera viable restringir el acceso a configuraciones críticas del sistema operativo tales como el panel de control y la instalación de aplicaciones no autorizadas con el objetivo de preservar la integridad del entorno de laboratorio. Estas restricciones contribuirían a mantener configuraciones similares en todos los equipos y también permitirían disminuir incidentes por cambios no controlados por los administradores de TI.

5.1.6 Gestión centralizada de aplicaciones

Se plantea administrar la instalación de aplicaciones de manera centralizada priorizando el uso de la Microsoft Store, con el fin de estandarizar el software presente en los laboratorios, esta estrategia facilitaría la actualización y mantenimiento de las aplicaciones y además permitiría reducir riesgos de seguridad relacionados a la instalación de software externo no autorizado.

5.1.7 Protección básica del endpoint

Se indica mantener habilitadas políticas básicas de protección del endpoint que posibiliten el monitoreo de la seguridad de los dispositivos gestionados desde el sistema central, estas normativas ayudarían a la identificación temprana de riesgos, además permitirían observar el estado general de la seguridad de los dispositivos en el laboratorio.

5.1.8 Trazabilidad y auditoría de accesos

Se propone establecer sistemas de trazabilidad y auditoría usando los datos de inicio de sesión y actividad que proporciona Microsoft Entra ID, esta información facilitaría la identificación de que usuario ingresó a un dispositivo y en qué instante permitiendo así el refuerzo de la supervisión administrativa y el análisis de incidentes.

5.1.9 Consideración de las limitaciones del entorno educativo

Se plantea también tener muy en cuenta las restricciones específicas del entorno educativo institucional, como las licencias disponibles, el alcance funcional del tenant y las habilidades técnicas de la infraestructura actual, este método ayudaría a establecer una

implementación que sea viable y sostenible. También facilitaría la identificación de características que aporten mayor valor al ambiente académico.

CAPÍTULO VI.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

En la elaboración del presente trabajo de investigación se logró desarrollar un prototipo de administración centralizada de identidades y dispositivos en la nube empleando herramientas Microsoft, el mismo que permitió optimizar la gestión y control de los equipos y de los usuarios que ingresan a los laboratorios de la Dirección de Tecnologías de la información de la UNACH, la planificación y ejecución de este prototipo demostró que es factible centralizar, implementar políticas y gestionar dispositivos de manera eficiente incluso teniendo en cuenta las restricciones propias del entorno académico.

Con base al análisis realizado de la situación actual en los laboratorios de DTIC se observó no existe un modelo para la gestión de usuarios y dispositivos es así que la utilización de herramientas Microsoft como Entra ID e Intune permitió establecer un entorno adecuado para la administración apoyándose en diversas funcionalidades de estas herramientas demostrando que son capaces de gestionar completamente los equipos y controlar los accesos desde cualquier lugar y permitiendo beneficiarse de las políticas derivadas de un tenant educativo.

Finalmente, en base a los resultados obtenidos fue posible sugerir directrices o lineamientos para una futura implementación y de esta manera actuando directamente como un modelo de administración centralizada de identidades y dispositivos con un enfoque completamente educativo que contempla las restricciones adaptadas al entorno y favoreciendo una gestión escalable a nivel institucional.

6.2 Recomendaciones

Se recomienda establecer una estructura clara de gobernanza del tenant institucional, teniendo en cuenta la distribución y/o asignación de roles administrativos, la distinción de responsabilidades y la regulación controlada de autorizaciones y permisos con el objetivo de asegurar una gestión segura y ordenada a través de la plataforma en la nube.

También se recomienda elaborar documentación técnica y manuales internos que expliquen las normal, configuraciones y prácticas del modelo de administración sugerido lo cual ayudaría en su mantenimiento, replicabilidad y continuidad operativa a largo plazo.

De igual manera se sugiere realizar la capacitación continua del personal de la DTIC en el uso de las herramientas junto con la revisión y actualización recurrente de las políticas y configuraciones implementadas considerando tanto la evolución de las necesidades institucionales como las actualizaciones de las plataformas en la nube con el propósito de garantizar una administración adecuada y una respuesta oportuna ante incidentes.

Finalmente se recomienda ampliar de manera gradual el modelo sugerido a diferentes laboratorios basándose en los resultados del prototipo, esta capacidad de escalar permitiría realizar modificaciones paulatinas conforme a las necesidades de la institución y de igual forma, disminuiría los riegos vinculados a implementaciones a gran escala sin una validación previa.

7. BIBLIOGRAFÍA

[1] S. Devlekar y V. Ramteke, “Identity and Access Management: High-level Conceptual Framework”, *Cardiometry* |, vol. 393, 2022, doi: 10.18137/cardiom.

[2] A. P. Singh, I. Kuzminykh, y B. Ghita, “Industry Perception of Security Challenges with Identity Access Management Solutions”, 2024, *Ithaca*. [En línea]. Disponible en: https://www.proquest.com/working-papers/industry-perception-security-challenges-with/docview/3095285126/se-2?accountid=36757

[3] K. Bálint, “Secure University Decentralized Data Storage Solutions”, *Management, Enterprise and Benchmarking in the 21st Century*, pp. 126–135, 2023, Consultado: el 8 de diciembre de 2025. [En línea]. Disponible en: https://www.proquest.com/scholarly-journals/secure-university-decentralized-data-storage/docview/2906884653/se-2?accountid=36757

[4] R. Rodriguez y N. Syynimaa, “Exploring Applicability of LLM-Powered Autonomous Agents to Solve Real-Life Problems: Microsoft Entra ID Administration Agent (MEAN)”, en *International Conference on Enterprise Information Systems, ICEIS - Proceedings*, Science and Technology Publications, Lda, 2024, pp. 881–887. doi: 10.5220/0012735700003690.

[5] Microsoft Corporation, “Documentación de Microsoft Intune”, 2024.

[6] Microsoft Corporation, “Fundamentos de Microsoft Entra”, 2023. Consultado: el 10 de noviembre de 2024. [En línea]. Disponible en: https://learn.microsoft.com/es-es/entra/fundamentals/

[7] “Bulletproofing your threat surface with the Microsoft security ecosystem”, *CIO*, jul. 2023, [En línea]. Disponible en: https://www.proquest.com/trade-journals/bulletproofing-your-threat-surface-with-microsoft/docview/2839662741/se-2?accountid=36757

[8] D. Badenhorst, G. Barbour, A. McDonald, W. Gertenbach, y E. Buckinjohn, “On the Zero-Trust Intranet Certification Problem”, marzo de 2024, *Academic Conferences International Limited, Reading*. [En línea]. Disponible en: https://www.proquest.com/conference-papers-proceedings/on-zero-trust-intranet-certification-problem/docview/3082337116/se-2?accountid=36757

[9] S. R. Bashir, S. Raza, y V. Misic, “A Narrative Review of Identity, Data and Location Privacy Techniques in Edge Computing and Mobile Crowdsourcing”, *Electronics (Basel)*, vol. 13, 2024, doi: 10.3390/electronics13214228.

[10] M. Haber, “Protecting data in the cloud”, *Risk Management*, vol. 62, núm. 10, p. 8+, 2015. [En línea]. Disponible en: https://link.gale.com/apps/doc/A441690486/AONE?u=unach_cons&sid=bookmark-AONE&xid=64ac0f4e

[11] S. Bradley, “Think security first when switching from traditional Active Directory to Azure AD”, *CSO (Online)*, may 2023, [En línea]. Disponible en: https://www.proquest.com/trade-journals/think-security-first-when-switching-traditional/docview/2817562459/se-2?accountid=36757

[12] P. Chukwuma y S. Rai, “Security in a cloud; Auditors must review risks across three distinct domains when organizations outsource IT security administration”, *Internal Auditor*, vol. 66, núm. 4, p. 21+, 2009. [En línea]. Disponible en: https://link.gale.com/apps/doc/A206051048/AONE?u=unach_cons&sid=bookmark-AONE&xid=41e4d952

[13] N. Hirapra, “Security in Azure Cloud”, *Dataquest*, jun. 2024, [En línea]. Disponible en: https://www.proquest.com/trade-journals/security-azure-cloud/docview/3071610877/se-2?accountid=36757

[14] A. Goel y Y. Rahulamathavan, “A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility”, *Future Internet*, vol. 17, núm. 1, p. 1, 2025, doi: https://doi.org/10.3390/fi17010001.

[15] Pratik Jain, “Identity and Access Management in the Cloud”, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 11, núm. 2, pp. 1528–1535, mar. 2025, doi: 10.32628/cseit25112523.

[16] M. Rifki, Hermanzoni, E. Edmizal, A. Ariston, y F. Muda, “Program Pengembangan Usaha Produk Intelektual Kampus Pusat Sport Entrepreneur”, *JURNAL PENGABDIAN MASYARAKAT OLAHRAGA DAN KESEHATAN (JASO)*, vol. 2, pp. 30–37, jul. 2022, doi: 10.24036/jaso.v2i1.13.

[17] S. des technologies de l'information Auditor General of the Ville de Montréal, "Centralized Identity and Access Management Auditor General of the Ville de Montréal Centralized Identity and Access Management Background", 2022. Consultado: el 11 de diciembre de 2025. [En línea]. Disponible en: https://bvgmtl.ca/wp-content/uploads/2022/05/AR_2021_EN_Section3.3..pdf

[18] J. Glöckler, J. Sedlmeir, M. Frank, y G. Fridgen, "A Systematic Review of Identity and Access Management Requirements in Enterprises and Potential Contributions of Self-Sovereign Identity", *Business & Information Systems Engineering*, vol. 66, núm. 4, pp. 421–440, ago. 2024, doi: https://doi.org/10.1007/s12599-023-00830-x.

[19] Y. Zhang, B. Liu, Y. Gong, J. Huang, J. Xu, y W. Wan, "Application of Machine Learning Optimization in Cloud Computing Resource Scheduling and Management", 2024, *Ithaca*. [En línea]. Disponible en: https://www.proquest.com/working-papers/application-machine-learning-optimization-cloud/docview/2932621571/se-2?accountid=36757

[20] I. B. Haimed, M. Albahar, y A. Alzubaidi, "Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks", *Future Internet*, vol. 15, núm. 7, p. 226, 2023, doi: https://doi.org/10.3390/fi15070226.

[21] J. Kamlofsky, "Vista de Computación en la Nube: Fundamentos, Críticas y Desafíos". Consultado: el 12 de enero de 2025. [En línea]. Disponible en: https://raia.revistasuai.ar/index.php/raia/article/view/2/32

[22] P. Goswami, N. Faujdar, S. Debnath, A. K. Khan, y G. Singh, "Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability", *Journal of Cloud Computing*, vol. 13, núm. 1, p. 45, dic. 2024, doi: https://doi.org/10.1186/s13677-024-00605-z.

[23] V. Dakić, Z. Morić, A. Kapulica, y D. Regvart, "Analysis of Azure Zero Trust Architecture Implementation for Mid-Size Organizations", *Journal of Cybersecurity and Privacy*, vol. 5, núm. 1, p. 2, 2025, doi: https://doi.org/10.3390/jcp5010002.

[24] S. Sharma, "Microsoft Intune Suite consolidates endpoint management and protection", el 2 de marzo de 2023, *Foundry, Framingham*. [En línea]. Disponible en:

https://www.proquest.com/other-sources/microsoft-intune-suite-consolidates-endpoint/docview/2781251104/se-2?accountid=36757

[25] J. Savill, “Savill’s FAQs: Microsoft Intune Licensing and Device Management”, *Windows IT Pro (Online)*, Informa, Chicago, el 20 de enero de 2018. [En línea]. Disponible en: https://www.proquest.com/magazines/savills-faqs-microsoft-intune-licensing-device/docview/1989234668/se-2?accountid=36757

[26] A. Taylor, *Microsoft Intune Cookbook: Over 75 recipes for configuring, managing, and automating your identities, apps, and endpoint devices*. Packt Publishing Ltd, 2024.

8. ANEXOS

CUESTIONARIO KAPA

Evaluación del Prototipo de Administración Centralizada (DTIC UNACH)

Instrucciones:

Marque con una **X** la opción que mejor exprese su nivel de acuerdo con cada afirmación.

Escala Likert (1–5):
1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Neutral
4 = De acuerdo
5 = Totalmente de acuerdo

SECCIÓN K – CONOCIMIENTO (Knowledge)

Código	Ítem	1	2	3	4	5
K1	Conozco el proceso mediante el cual los dispositivos se registran en Microsoft Intune.	☐	☐	☐	☐	☒
K2	Comprendo cómo se configuran los grupos de seguridad en Microsoft Entra ID.	☐	☐	☐	☐	☒
K3	Conozco el funcionamiento del método de inicio de sesión institucional mediante Entra ID.	☐	☐	☐	☐	☒
K4	Entiendo cómo se gestiona la identidad del usuario desde Microsoft Entra ID.	☐	☐	☐	☐	☒
K5	Conozco la utilidad y funcionamiento del modo PC Shared en equipos compartidos.	☐	☐	☐	☐	☒
K6	Comprendo cómo funcionan las restricciones para la instalación de aplicaciones en Intune.	☐	☐	☐	☐	☒
K7	Conozco los elementos que conforman el nivel general de seguridad aplicado al laboratorio.	☐	☐	☐	☒	☐

SECCIÓN A – ACTITUD (Attitudes)

Código	Ítem	1	2	3	4	5
A1	Considero que registrar los dispositivos en Intune mejora la administración del laboratorio.	☐	☐	☐	☐	☒
A2	Los grupos de seguridad facilitan el control y organización de usuarios y equipos.	☐	☐	☐	☐	☒
A3	El método de inicio de sesión institucional aporta mayor seguridad y trazabilidad.	☐	☐	☐	☐	☒
A4	La gestión de identidades desde Entra ID es beneficiosa para la infraestructura del laboratorio.	☐	☐	☐	☐	☒
A5	El modo PC Shared es adecuado para el uso académico en equipos compartidos.	☐	☐	☐	☐	☒
A6	Las restricciones de instalación de aplicaciones contribuyen significativamente a la seguridad.	☐	☐	☐	☐	☒
A7	El nivel de seguridad aplicado mediante el prototipo es apropiado para el laboratorio 404.	☐	☐	☐	☐	☒

Anexo 1. Instrumento de evaluación del prototipo de administración centralizada mediante el coeficiente Kappa (Evaluador 1)

SECCIÓN P – PRÁCTICA (Practice)

Código	Ítem	1	2	3	4	5
P1	Implementaría el registro de dispositivos en todos los equipos del laboratorio.	☐	☐	☐	☐	☒
P2	Aplicaría grupos de seguridad para organizar usuarios y dispositivos.	☐	☐	☐	☐	☒
P3	Configuraría los equipos para utilizar inicio de sesión institucional.	☐	☐	☐	☒	☐
P4	Gestionaría identidades exclusivamente desde Entra ID.	☐	☐	☐	☐	☒
P5	Activaría PC Shared en equipos compartidos del laboratorio.	☐	☐	☐	☐	☒
P6	Aplicaría políticas de restricción de aplicaciones como estándar de seguridad.	☐	☐	☐	☐	☒
P7	Mantendría el nivel general de seguridad definido por el prototipo como práctica institucional.	☐	☐	☐	☐	☒

SECCIÓN AA – APTITUD / CAPACIDAD (Ability)

Código	Ítem	1	2	3	4	5
AA1	Me siento capaz de aplicar las configuraciones del prototipo sin supervisión.	☐	☐	☐	☐	☒
AA2	Puedo interpretar correctamente la información mostrada por Intune y Entra ID.	☐	☐	☐	☐	☒
AA3	Estoy preparado(a) para gestionar equipos mediante administración centralizada en la nube.	☐	☐	☐	☐	☒

Anexo 2. Instrumento de evaluación práctica y de capacidad del prototipo de administración centralizada mediante el coeficiente Kappa (Evaluador 1)

CUESTIONARIO KAPA

Evaluación del Prototipo de Administración Centralizada (DTIC UNACH)

Instrucciones:

Marque con una **X** la opción que mejor exprese su nivel de acuerdo con cada afirmación.

Escala Likert (1–5):
1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Neutral
4 = De acuerdo
5 = Totalmente de acuerdo

SECCIÓN K – CONOCIMIENTO (Knowledge)

Código	Ítem	1	2	3	4	5
K1	Conozco el proceso mediante el cual los dispositivos se registran en Microsoft Intune.	☐	☐	☐	☑	☐
K2	Comprendo cómo se configuran los grupos de seguridad en Microsoft Entra ID.	☐	☐	☐	☑	☐
K3	Conozco el funcionamiento del método de inicio de sesión institucional mediante Entra ID.	☐	☐	☐	☐	☑
K4	Entiendo cómo se gestiona la identidad del usuario desde Microsoft Entra ID.	☐	☐	☐	☐	☑
K5	Conozco la utilidad y funcionamiento del modo PC Shared en equipos compartidos.	☐	☐	☐	☐	☑
K6	Comprendo cómo funcionan las restricciones para la instalación de aplicaciones en Intune.	☐	☐	☐	☑	☐
K7	Conozco los elementos que conforman el nivel general de seguridad aplicado al laboratorio.	☐	☐	☐	☒	☐

SECCIÓN A – ACTITUD (Attitudes)

Código	Ítem	1	2	3	4	5
A1	Considero que registrar los dispositivos en Intune mejora la administración del laboratorio.	☐	☐	☐	☐	☒
A2	Los grupos de seguridad facilitan el control y organización de usuarios y equipos.	☐	☐	☐	☐	☒
A3	El método de inicio de sesión institucional aporta mayor seguridad y trazabilidad.	☐	☐	☐	☐	☒
A4	La gestión de identidades desde Entra ID es beneficiosa para la infraestructura del laboratorio.	☐	☐	☐	☐	☒
A5	El modo PC Shared es adecuado para el uso académico en equipos compartidos.	☐	☐	☐	☐	☒
A6	Las restricciones de instalación de aplicaciones contribuyen significativamente a la seguridad.	☐	☐	☐	☐	☒
A7	El nivel de seguridad aplicado mediante el prototipo es apropiado para el laboratorio 404.	☐	☐	☐	☐	☒

Anexo 3. Instrumento de evaluación del prototipo de administración centralizada mediante el coeficiente Kappa (Evaluador 2)

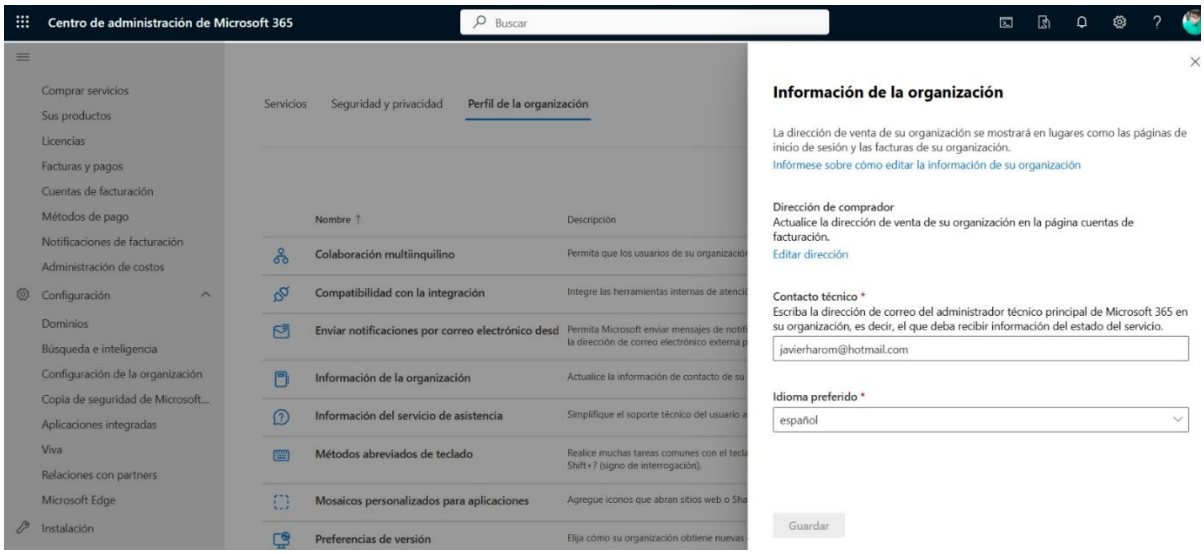
SECCIÓN P – PRÁCTICA (Practice)

Código	Ítem	1	2	3	4	5
P1	Implementaría el registro de dispositivos en todos los equipos del laboratorio.	☐	☐	☐	☐	☑
P2	Aplicaría grupos de seguridad para organizar usuarios y dispositivos.	☐	☐	☐	☐	☑
P3	Configuraría los equipos para utilizar inicio de sesión institucional.	☐	☐	☐	☐	☑
P4	Gestionaría identidades exclusivamente desde Entra ID.	☐	☐	☐	☐	☑
P5	Activaría PC Shared en equipos compartidos del laboratorio.	☐	☐	☐	☐	☑
P6	Aplicaría políticas de restricción de aplicaciones como estándar de seguridad.	☐	☐	☐	☐	☑
P7	Mantendría el nivel general de seguridad definido por el prototipo como práctica institucional.	☐	☐	☐	☐	☑

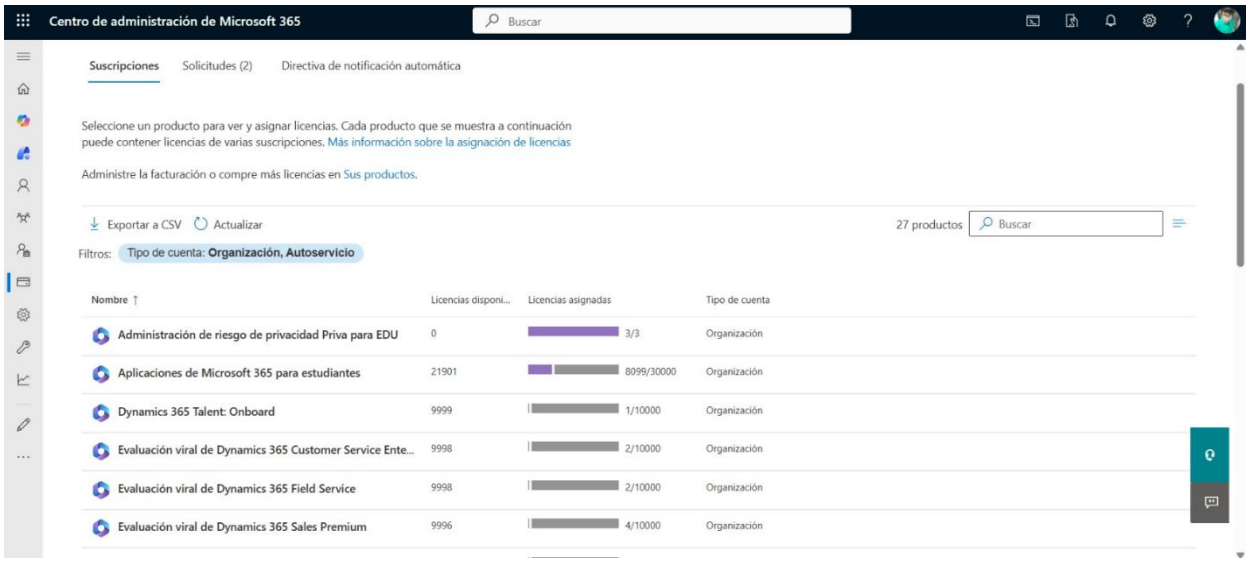
SECCIÓN AA – APTITUD / CAPACIDAD (Ability)

Código	Ítem	1	2	3	4	5
AA1	Me siento capaz de aplicar las configuraciones del prototipo sin supervisión.	☐	☐	☐	☑	☐
AA2	Puedo interpretar correctamente la información mostrada por Intune y Entra ID.	☐	☐	☐	☑	☐
AA3	Estoy preparado(a) para gestionar equipos mediante administración centralizada en la nube.	☐	☐	☐	☑	☐

Anexo 4. Instrumento de evaluación práctica y de capacidad del prototipo de administración centralizada mediante el coeficiente Kappa (Evaluador 2)



Anexo 5. Información general y configuración del tenant institucional de Microsoft 365



Anexo 6. Relación de licencias disponibles para la administración centralizada en Microsoft 365