PROPUESTA DE SERVICIO

Implementación de Línea Base de Seguridad – Microsoft 365 y EMS E3

IDEA

MAYO 2026

CONFIDENCIAL

White Hat Consultores, S.A. de C.V.

Distribución restringida por los derechos reservados. El presente documento es propiedad de White Hat Consultores, S.A. de C.V. quien distribuye una copia a IDEA, únicamente para ser considerada como información guía en una posible implementación a futuro del servicio. El contenido en este documento tiene información confidencial que pertenece a White Hat Consultores, S.A. de C.V. y a IDEA, no podrá ser utilizada, fotocopiada, duplicada o revelada para cualquier propósito diferente a los indicados por la empresa.

Contenido

Introducción 3

Objetivo 5

Alcances Funcionales del Servicio 5

Identidad y Acceso (Microsoft Entra ID) 6

Gestión y Seguridad de Dispositivos (Microsoft Intune) 8

Ciclo de vida y gestión de los dispositivos 8

Seguridad del Correo y Colaboración (Exchange Online Protection & Defender for Office 365) 10

Protección y Gobernanza de la Información (Microsoft Purview Information Protection) 12

Cierre y Entregables 15

Metodología del despliegue 15

Proceso de Ejecución 16

Ventajas del Despliegue Canario 16

Evaluación del cambio 17

Ejemplo del despliegue en oleadas 17

Metodología de Etiquetado de la Información 17

Plan de Trabajo y Cronograma de Implementación 20

Fase 1 (Semana 1): Arranque, Identidad y Accesos 20

Fase 2 (Semana 2): Gestión y Seguridad de Endpoints 21

Fase 3 (Semana 3): Seguridad del Correo y Colaboración 21

Fase 4 (Semana 4): Protección y Gobernanza de la Información 21

Fase 5 (Semana 5): Documentación, Transferencia de Conocimiento y Cierre 22

Fase 6: Active Directory on-premise (Esta fase se iniciará en la semana 2 y tendrá una duración de 4 semanas) 22

Fase 7 – Monitoreo y Alertamiento SOC 24

Propuesta económica 26

Prerrequisitos técnicos 27

Generales 27

Microsoft Intune 28

Microsoft Purview 28

Microsoft Defender for Office 365 28

Entregables del Proyecto 28

Supuestos y Condiciones del Servicio 29
Bolsa de Horas de Acompañamiento 29

Introducción

Evaluar el riesgo debe ir más allá de detectar vulnerabilidades. La gestión de la seguridad debe identificar la probabilidad y el impacto de la explotación, un evento de ese tipo puede implicar un robo de datos, pérdida de clientes, sanciones o daño reputacional. Este enfoque integral se denomina escenario de riesgo y es el eje central de la propuesta.

En el pasado, las organizaciones centraban sus defensas en proteger el perímetro de la red con firewalls y VPN locales, asumiendo que todo el entorno interno era seguro. Sin embargo, en la actualidad, con la distribución de los datos hacia la nube y entornos híbridos, el modelo de seguridad Zero Trust (Confianza Cero) ha evolucionado para hacer frente a un conjunto más amplio y complejo de vectores de ataque.

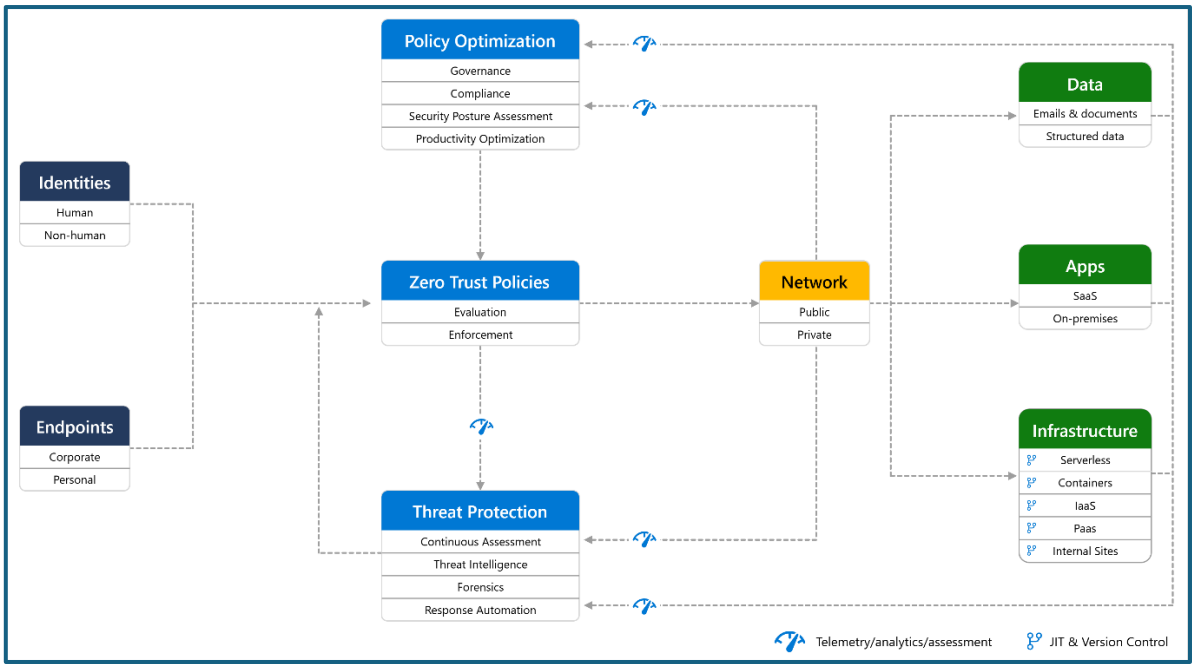


Ilustración 1. Arquitectura unificada de Zero Trust en áreas funcionales.

En este contexto, la estrategia de seguridad propuesta por White Hat Consultores se fundamenta en el modelo Zero Trust, articulada bajo los principios de mínimo privilegio, mitigación y reducción de riesgos.

Este modelo tiene como punto de partida la identidad: verifica y garantiza que únicamente las personas, dispositivos y procesos con la autorización adecuada puedan acceder a los recursos críticos de la organización.

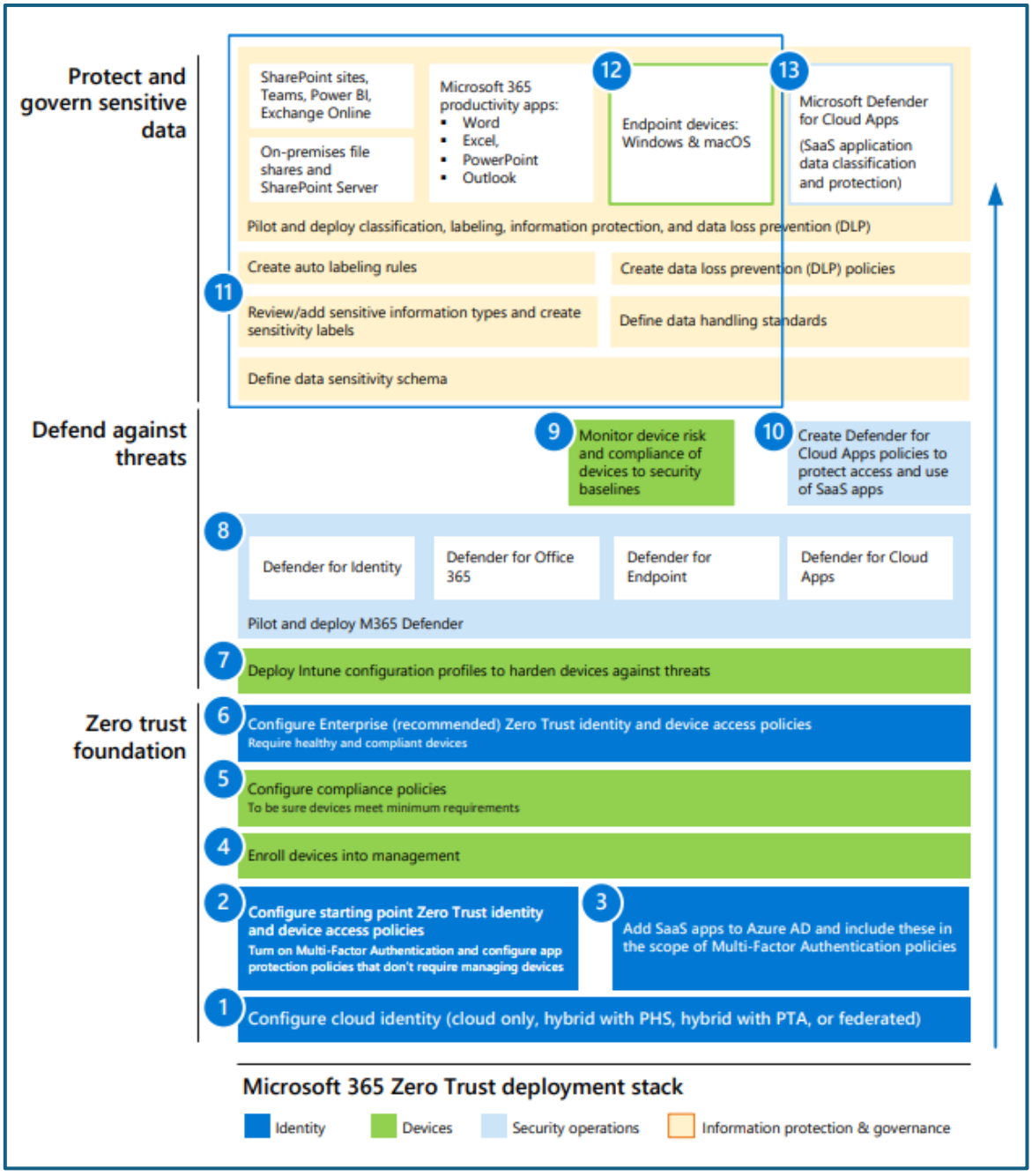


Ilustración 2. Despliegue de Zero Trust en Microsoft 365.

Objetivo

El objetivo del presente servicio es **implementar** una **línea base de seguridad** en el entorno (**Tenant**) de **Microsoft 365 aprovechando** el **licenciamiento de EMS E3** de la organización. Esta implementación está orientada a fortalecer la identidad, el control de acceso, la gestión de dispositivos y la protección de la información.
Todo el **despliegue** se realizará **alineado** a las mejores prácticas de seguridad en la nube y bajo la arquitectura de **Zero Trust (Confianza Cero)**, garantizando un entorno seguro, gobernable y documentado, con la premisa de no afectar la continuidad operativa del negocio.

Alcances Funcionales del Servicio

A continuación, se detalla el alcance funcional del servicio, estructurado en **fases secuenciales** para **implementar una línea base de seguridad** integral bajo el modelo de arquitectura Zero Trust.
El proyecto abarcará, a nivel general: el fortalecimiento de la **identidad y el control de acceso** para asegurar la autenticación al entorno; la **gestión y seguridad de dispositivos** para estandarizar el cumplimiento de los equipos y móviles; el ajuste de **controles de seguridad para el correo y la colaboración** frente a amenazas externas; la **aplicación de políticas iniciales** para la **protección y gobernanza** de la información sensible; y, finalmente, una **fase de cierre** enfocada en la documentación y transferencia de conocimiento al equipo administrador.

	• ~250 usuarios
	• ~250 dispositivos

Identidad y Acceso (Microsoft Entra ID)

Transformar la identidad en el nuevo perímetro de seguridad del IDEA, garantizando que el acceso a la información financiera y de proyectos se otorgue bajo el principio de "mínimo privilegio" y la confianza cero (*Zero Trust*).Actividades para mejorar la gestión de la identidad:

- **Evaluación del Estado Actual**
  No podemos mejorar lo que no medimos. Iniciaremos con un análisis profundo del Microsoft Secure Score, enfocándonos en:
  - Auditoría de roles privilegiados (Administradores Globales) para reducirlos al mínimo necesario.
  - Detección de brechas en configuraciones actuales frente a los estándares de seguridad.
- **Políticas de Acceso Condicional**
  Diseño e implementación de **políticas basadas en el contexto del usuario**. Esto incluye:
  - Filtros por Ubicación y Dispositivo: Restringir el acceso a usuarios que intenten conectar desde fuera de Colombia o desde dispositivos que no estén registrados y evaluados por el Instituto.
  - Control de Aplicaciones: Diferenciar el nivel de seguridad requerido para entrar al correo electrónico versus aplicaciones financieras críticas.
- **Habilitación de Autenticación Multifactor (MFA)**
  Implementación y exigencia de MFA para todos los usuarios, siendo posible la configuración del segundo factor de autenticación para toda la organización, priorizando el uso de la aplicación Microsoft Authenticator mediante notificaciones Push y Number Matching (coincidencia de números) para mitigar ataques de fatiga de MFA.
- **Bloqueo de Autenticación Heredada**
  Cierre de protocolos antiguos (como POP3, IMAP, SMTP heredado) que no soportan MFA y son el principal vector de ataques de fuerza bruta. De esta manera se permitirá únicamente el acceso mediante la capa de MFA.
- **Autoservicio de Restablecimiento de Contraseña (SSPR)**
  Configuración del portal de autoservicio para que los usuarios puedan recuperar sus credenciales de forma segura, reduciendo la carga operativa de la mesa de ayuda.
- **Cuentas de Emergencia**
  Configuración de cuentas "**Break-Glass**" (cuentas de acceso de emergencia) para evitar la pérdida de acceso al Tenant en caso de fallas sistémicas. Se propone la creación de dos cuentas sin MFA pero bajo un proceso estricto de monitoreo y contraseñas de +30 caracteres.

- **Pruebas Controladas**
  Activación de las políticas en **modo "Solo informe" (Report-only)** para evaluar el **impacto**, seguido de la validación con un **grupo de usuarios piloto** antes del despliegue general.
- **Capacidad de control de cumplimiento**
  Se mostrará al equipo de IDEA como acceder a informes de uso y registro de auditoria mediante la consola de Microsoft Entra.
    - **Sign-in Logs (Registros de inicio de sesión):** Podrás ver en tiempo real cada intento de acceso. Sabrás si una política de **Acceso Condicional** bloqueó a alguien, por qué lo hizo y desde qué IP/país ocurrió.
    - **Audit Logs:** Registra cada cambio en la configuración (ej. si alguien desactivó el MFA a un usuario o cambió una política de acceso). Es vital para auditorías internas y de entes de control.
    - **Informes de MFA:** Permite ver cuántos funcionarios ya están registrados en la App Authenticator y cuántos siguen usando métodos menos seguros.

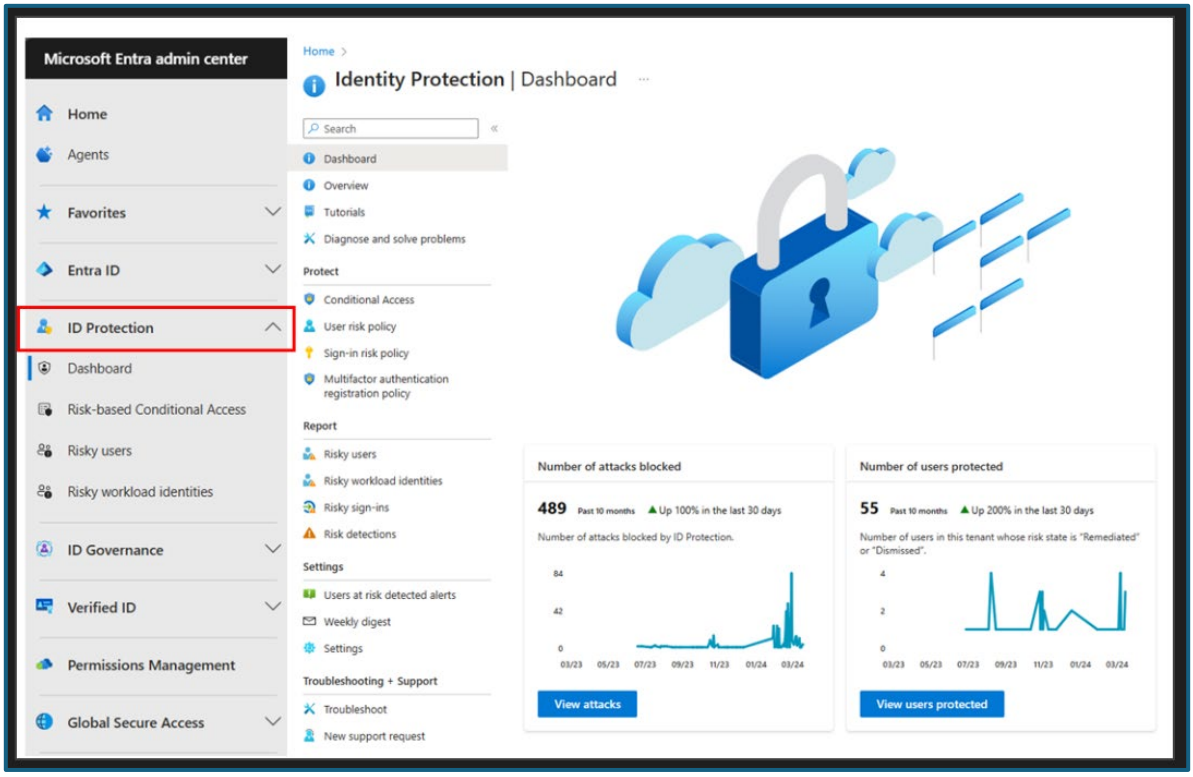


Imagen de ejemplo del panel de Microsoft Entra

Gestión y Seguridad de Dispositivos (Microsoft Intune)

Buscaremos habilitar a IDEA para pasar de una gestión tradicional a una gestión basada en la nube, ideal para el trabajo híbrido y la protección de los datos en un esquema de trabajo en oficinas principales, en campo y desde sucursales.



Ilustración 3. Diagrama de la protección de activos (dispositivos y aplicaciones) en una organización con Microsoft Intune.

Con este componente de la propuesta se busca establecer un control centralizado y automatizado sobre todos los activos tecnológicos del **IDEA**, garantizando que cualquier dispositivo (computador o móvil) que acceda a la información institucional cumpla con estándares rigurosos de seguridad, independientemente de su ubicación.

Ciclo de vida y gestión de los dispositivos

- **Incorporación de dispositivos**
  Registrar y gestionar dispositivos dentro de la organización utilizando la plataforma de gestión de dispositivos de Microsoft.
- **Asignación de directivas de cumplimiento**
  Definir las directivas que los dispositivos deben cumplir para acceder a los recursos corporativos.
- **Asignación de directivas de perfiles de configuración**
  Crear y configurar perfiles para aplicar configuraciones específicas a los dispositivos, como Wi-Fi, VPN, restricciones de seguridad, etc.
- **Inventario y monitoreo de dispositivos**
  Utilizar el panel de Microsoft Intune para monitorear el estado de los dispositivos, la conformidad y la implementación de políticas.

- **Limpieza y retirada de dispositivos**
  Realizar acciones remotas como borrar, bloquear o restablecer dispositivos y eliminar aquellos que no pertenezcan a la organización después de un periodo de inactividad o no cumplimiento.

Esta fase establece el **control sobre los puntos de conexión (endpoints)** desde los cuales se accede a la información corporativa, asegurando que cumplan con los **estándares mínimos de la organización**.

- **Preparación del Entorno (MDM/MAM)**
  Configuración de **Microsoft Intune** como la autoridad de gestión de dispositivos móviles (**MDM**) y gestión de aplicaciones móviles (**MAM**).
    - **MDM (Mobile Device Management):** Para dispositivos propiedad del Instituto, control total del inventario, configuración de Wi-Fi, certificados y capacidad de **borrado remoto total**.
    - **MAM (Mobile Application Management):** Para escenarios donde el funcionario usa su dispositivo personal para consultar el correo o Teams. Se crean contenedores seguros donde la información del IDEA está aislada de las apps personales (evitando, por ejemplo, copiar datos del correo institucional a un WhatsApp personal).
- **Políticas de Cumplimiento (Compliance Policies)**
  Definición de reglas de salud y seguridad que debe cumplir un dispositivo para acceder a los datos. Incluye:
    - **Exigencia** de versiones mínimas de sistema operativo.
    - **Gestión de Actualizaciones (Windows Update for Business):** Automatización de parches de seguridad y actualizaciones de sistema operativo para mitigar vulnerabilidades de día cero.
    - **Configuración de Seguridad de Endpoint:** Restricción de puertos USB (opcional), configuración de Firewall de Windows y Windows Defender Antivirus gestionado desde una consola única.
    - **Requisitos** de complejidad de contraseñas y bloqueos de pantalla.
    - **Detección** de **dispositivos** comprometidos (Jailbreak en iOS / Root en Android).
    - **Bloqueo de acceso** si el dispositivo tiene el antivirus desbloqueado.
- **Perfiles de Configuración Base**
  Despliegue de configuraciones estándar (**Configuration Profiles**) para endurecer la seguridad del sistema, tales como la activación y forzado del cifrado de disco (**BitLocker para Windows 10/11 Enterprise**).
  Con el cifrado de datos (BitLocker) de activación obligatoria y gestión de claves de recuperación en la nube para asegurar que, en caso de pérdida o robo del equipo, la información sea inaccesible.

- **Protección de Aplicaciones (App Protection Policies)**
  Configuración de **políticas MAM** para dispositivos personales (**BYOD - Bring Your Own Device**). Esto permite **proteger** los **datos corporativos** dentro de las aplicaciones de Microsoft (Outlook, Teams, OneDrive) sin necesidad de administrar el dispositivo personal del usuario por completo (evitando copiar/pegar información a aplicaciones personales y requiriendo PIN de acceso a la app).

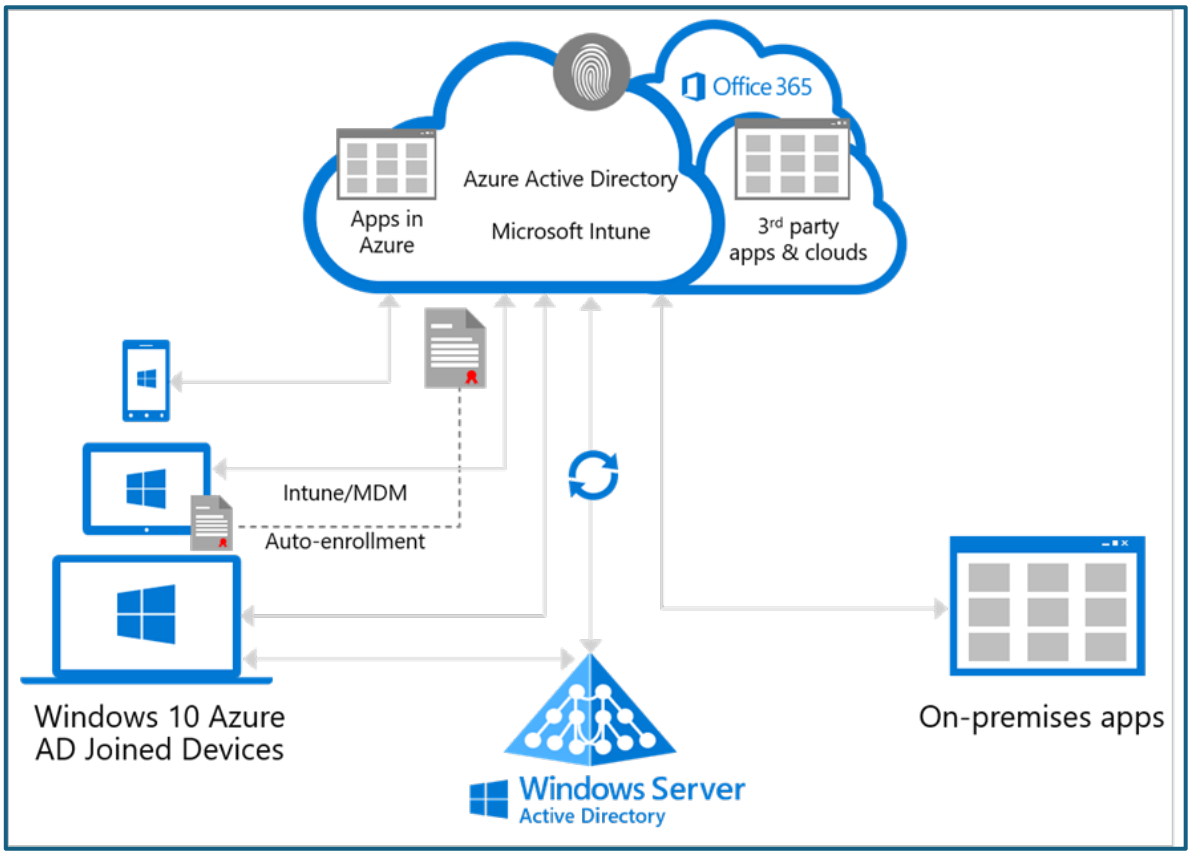


Ilustración 4. Arquitectura del despliegue de Microsoft Intune.

Seguridad del Correo y Colaboración (Exchange Online Protection & Defender for Office 365)

Exchange Online Protection y Defender for Office 365 (MDO) protegen contra amenazas en el **correo electrónico y herramientas de colaboración** de los canales de comunicación más críticos contra las amenazas externas más comunes.

- **Auditoría de Higiene de Correo**

Revisión y recomendaciones sobre los registros DNS de seguridad del dominio (SPF, DKIM y DMARC) para prevenir la suplantación de identidad (Spoofing). Esto asegura que los correos enviados por el Instituto no sean marcados como fraudulentos por otras entidades.

Cifrado de Mensajes

Uso de *Office 365 Message Encryption* (incluido en E3) para permitir que los funcionarios envíen correos con información sensible (como datos financieros) de forma cifrada a destinatarios externos.

- **Protección Avanzada de Colaboración**

  Habilitación de la detonación en sandbox de archivos adjuntos (Safe Attachments) y la reescritura de enlaces en tiempo de clic (Safe Links) para proteger contra phishing de día cero y ransomware en **Exchange Online** y **Microsoft Teams**.
- **Configuración de Políticas de Seguridad en MDO**
  - **Protección contra Phishing:** Configurar políticas para detectar y bloquear correos electrónicos de phishing. Esto incluye la configuración de directivas específicas para proteger a los usuarios de ataques de suplantación de identidad.
  - **Protección contra Spam:** Establecer políticas para identificar y filtrar correos electrónicos no deseados, asegurando que los usuarios reciban solo correos electrónicos legítimos
  - **Protección Antimalware:** Configuración de filtros de archivos adjuntos para bloquear extensiones ejecutables y scripts peligrosos, además de la purga automática de malware detectado en fase de entrega.
  - **Datos Adjuntos Seguros:** Implementar políticas que escanean y verifican la seguridad de los archivos adjuntos antes de que los usuarios puedan acceder a ellos
  - **Vínculos Seguros:** Configurar políticas para proteger a los usuarios de enlaces maliciosos en correos electrónicos y documentos. Los enlaces se reescriben y se verifican en tiempo real cuando los usuarios hacen clic en ellos
- **Validación Funcional**

  Para garantizar que la seguridad no afecte la operatividad del Instituto, se seguirá un protocolo de validación:
  - **Simulación y Monitoreo:** Uso de herramientas de reporte para observar cuántos correos legítimos podrían ser afectados antes de poner las políticas en modo estricto.
  - **Ajuste de Falsos Positivos:** Creación de listas de remitentes seguros (Allow Lists) para entidades aliadas y gubernamentales con las que el IDEA interactúa frecuentemente.

- **Auditoría de Cuarentena:** Capacitación y configuración para que los administradores de TI puedan gestionar correos retenidos de forma ágil, garantizando que ninguna comunicación crítica de negocio se pierda.

- **Monitoreo**
  Accediendo a los reportes de seguridad en el *Microsoft Defender Portal* el Instituto ver exactamente cuántos ataques de phishing han sido bloqueados mensualmente, facilitando la rendición de cuentas ante la alta gerencia.

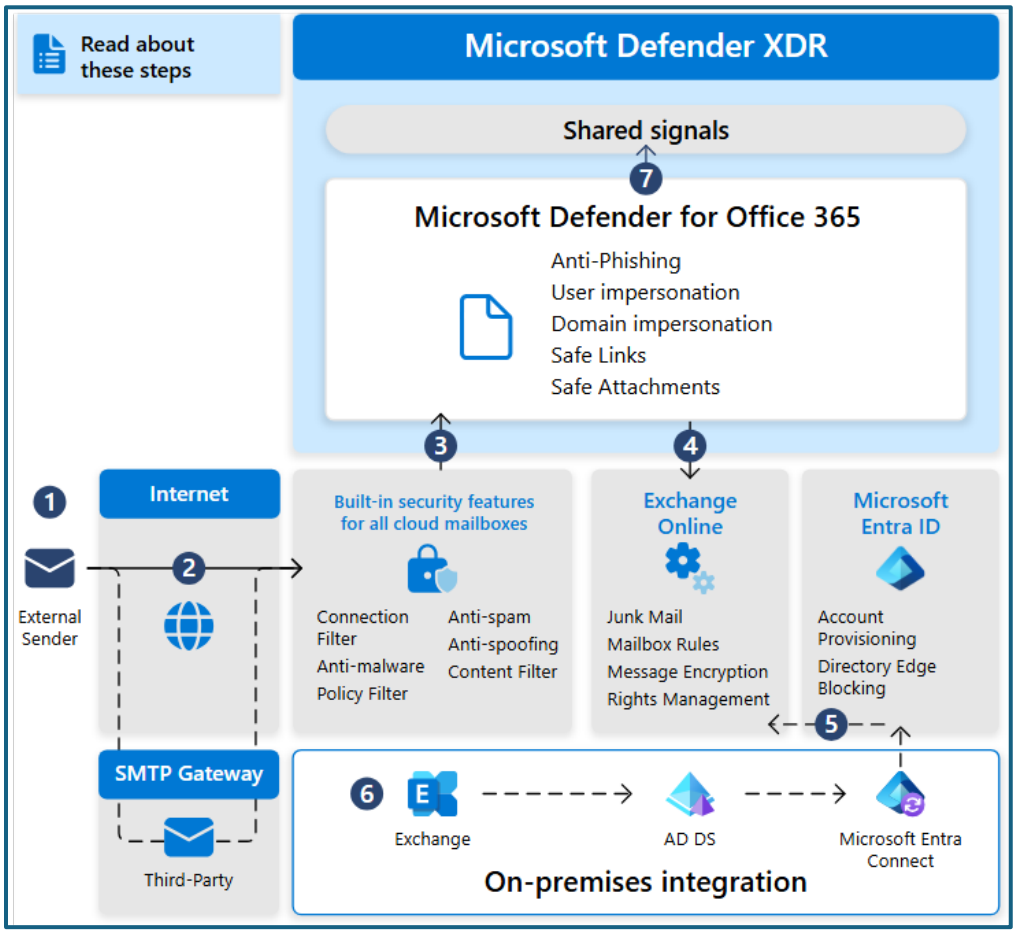


Ilustración 5. Diagrama de la arquitectura de línea base para Microsoft Defender para Office 365, que puede incluir una pasarela SMTP de terceros o integración local.

Protección y Gobernanza de la Información (Microsoft Purview Information Protection)

El objetivo de este componente del proyecto es garantizar la integridad, disponibilidad y confidencialidad de los activos digitales del **IDEA**, asegurando que la información

sensible esté protegida en todo su ciclo de vida y cumpla con las leyes de transparencia y protección de datos personales.



Ejemplo referencial

Las actividades contempladas buscan **descubrir, clasificar y proteger los datos sensibles** de la organización, independientemente de dónde residan o adónde se muevan.

- **Taxonomía y Clasificación**
  Acompañamiento en la definición de una **estructura básica de clasificación de datos** (ej. Pública, Uso Interno, Confidencial).
- **Etiquetas de Sensibilidad (Sensitivity Labels)**
  Creación y publicación de **etiquetas en Microsoft Purview** para que los usuarios puedan marcar visualmente **correos y documentos** (Word, Excel, PowerPoint), aplicando marcas de agua, encabezados o pies de página según el **nivel de confidencialidad**. Si un archivo etiquetado como "Confidencial" sale del IDEA, solo podrá ser abierto por usuarios autorizados.
- **Etiquetas de Retención:**
  Configuración de políticas para asegurar que documentos legales o financieros se conserven por el tiempo mínimo exigido por la ley y se eliminen de forma segura una vez cumplido su ciclo de vida, optimizando el almacenamiento.
- **Prevención de Pérdida de Datos (DLP)**
  Implementación de **políticas DLP base en Exchange Online, SharePoint y OneDrive**. Si un usuario intenta enviar un archivo clasificado a un dominio

externo no autorizado, la acción será bloqueada y se mostrará un Policy Tip (consejo de política) para educar al usuario.

- **Auditoría y Retención**
  Activación de la **búsqueda de registros** de auditoría unificada (**Unified Audit Log**) para trazabilidad de eventos, y configuración de una política general de retención de datos si la organización lo requiere por temas de cumplimiento.
  Alertas de Actividad Anómala: Notificaciones automáticas ante comportamientos sospechosos, como la descarga masiva de documentos en un corto periodo de tiempo.

  Content Search: Herramientas de búsqueda rápida para procesos de auditoría interna o respuesta a requerimientos legales, permitiendo localizar información en todo el Tenant de forma centralizada.

Monitoreo y Medición del Cumplimiento de Datos

Para garantizar que estas políticas no sean solo configuraciones estáticas, se entrenará al equipo de IDEA en el **Explorador de Actividades (Activity Explorer)** y el **Panel de Información de Protección de Datos** en Microsoft Purview. Estas herramientas permitirán visualizar en tiempo real cómo se está clasificando la información y detectar anomalías, tales como el etiquetado incorrecto de documentos sensibles o intentos inusuales de compartir información confidencial fuera de la red institucional. Este monitoreo constante facilita la identificación de brechas de seguridad y permite ajustar las políticas de DLP basándose en el comportamiento real de los funcionarios.

Asimismo, se implementará el **Administrador de Cumplimiento (Compliance Manager)**, que proporcionará al Instituto una "puntuación de cumplimiento" específica para la gobernanza de datos. A través de informes detallados, el IDEA podrá demostrar ante entes de control y auditorías internas el estado de protección de sus activos, evidenciando el cumplimiento de controles técnicos vinculados a la **Ley 1581 de Protección de Datos** y el Modelo de Seguridad y Privacidad de la Información (**MSPI)**. Esta visibilidad integral asegura que la gobernanza de la información sea medible, auditable y esté alineada con los objetivos estratégicos de transparencia del Instituto.

Cierre y Entregables

Aseguramiento de que el equipo del cliente tiene el conocimiento y la documentación necesaria para operar y mantener el entorno seguro.

- **Documentación de Arquitectura**
  Entrega de un documento técnico detallando todas las políticas, perfiles, reglas y configuraciones aplicadas en el Tenant durante el proyecto.
- **Informe de Recomendaciones (Roadmap)**
  Presentación de los hallazgos obtenidos y una hoja de ruta sugerida para futuras maduraciones de seguridad (fases 2 y 3).
- **Sesiones de Transferencia de Conocimiento (Knowledge Transfer)**
  Sesiones técnicas remotas, se estiman unas 20 sesiones de una hora llevadas a cabo de manera diaria en veinte días útiles. Estas sesiones serán, de preferencia, con el equipo administrador del cliente; se podrá tener hasta cuatro (4) asistentes adicionales a estas sesiones. Se revisará la consola de administración, el monitoreo básico de alertas, la gestión de cuarentenas y el procedimiento para añadir o excluir usuarios de las políticas implementadas.

Metodología del despliegue

La metodología de despliegue se basa en un ciclo de mejora de procesos que permite evaluar riesgos y corregir a fin de prevenir errores en esta etapa.

Fase	Descripción
Plan	• Selección de grupo piloto • Selección de casos de uso
Do	• Despliegue de soluciones
Check	• Evaluación de los cambios
Act	• Corrección y consideraciones de mejora

Tabla 1. Fases generales de la metodología del despliegue Canario.

Para garantizar la **continuidad operativa** de los **250 colaboradores y los 250 dispositivos** durante la transición tecnológica, **White Hat Consultores** ejecuta este tipo de proyectos utilizando la estrategia de **Despliegue Canario**.
A diferencia de un despliegue abrupto o tipo masivo, el Despliegue Canario es una **estrategia de liberación controlada** que consiste en aplicar las nuevas **políticas de seguridad**, **configuraciones de dispositivos (MDM/MAM)** y **agentes de protección** a un pequeño subconjunto de usuarios estratégicos antes de masificar el cambio a toda

la organización. Este enfoque nos permite **monitorear** el **comportamiento** de las herramientas en un entorno de producción real, garantizando la estabilidad y **detectando cualquier impacto en la productividad** antes de afectar a toda la base de usuarios.

Proceso de Ejecución

- **Selección del Grupo Canario (Piloto Técnico)**
  Se elige un grupo inicial reducido (típicamente personal de TI y usuarios avanzados o Champions) para recibir las configuraciones base. Este grupo valida que las aplicaciones corporativas críticas operen sin fricción bajo los nuevos controles de seguridad (ej. Acceso Condicional, DLP, etc.).
- **Monitoreo y Evaluación Activa**
  Se evalúa de manera continua la telemetría en las consolas de Microsoft y se monitorea los incidentes para identificar posibles falsos positivos o bloqueos inesperados.
- **Despliegue Escalonado en Oleadas**
  Tras validar la estabilidad en el grupo canario, **White Hat Consultores** procede con la liberación estructurada en "Oleadas". Se aplican las configuraciones a lotes controlados de 25 en 25 usuarios. Conforme se afianza la estabilidad y disminuyen las incidencias, el volumen de las oleadas se incrementa progresivamente hasta alcanzar el despliegue masivo por departamentos o localidades.
- **Decisión y Reversión Rápida**
  Si se detecta un comportamiento anómalo durante una oleada, la política o configuración específica se revierte de manera quirúrgica solo para ese grupo afectado. Se realizan los ajustes y exclusiones necesarias en la arquitectura antes de reanudar el avance.

Ventajas del Despliegue Canario

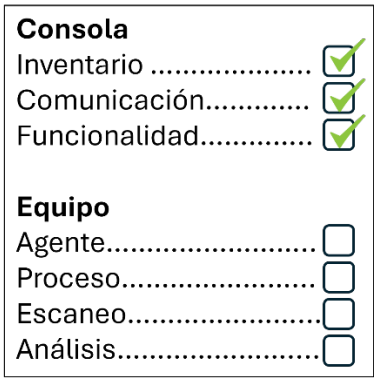
- **Mitigación de Riesgos Operativos**
  Al limitar la exposición inicial, aseguramos que un bloqueo preventivo de Defender o una regla estricta de Intune no paralice la operación de un departamento completo.
- **Detección Temprana de Fricciones**
  Permite identificar problemas de compatibilidad en una etapa temprana.

- **Mejora y Calibración Continua**
  Facilita el ajuste fino (tuning) de las políticas a partir del feedback real de la operación, logrando el equilibrio perfecto entre seguridad y experiencia de usuario.
- **Agilidad de Respuesta**
  Ofrece la capacidad de revertir un cambio en minutos, minimizando el impacto para el usuario final y manteniendo la confianza en el proyecto.

En **White Hat Consultores**, hemos adoptado el **Despliegue Canario en Oleadas** como nuestra práctica estándar para asegurar transiciones tecnológicas transparentes, evaluando constantemente la funcionalidad y garantizando una adopción exitosa.

Evaluación del cambio

- **Pruebas:** Se prueban los componentes individuales del servicio para asegurar que funcionen correctamente.
- **Pruebas de Sistema:** Se prueba el sistema completo para asegurar que cumple con los requisitos especificados.
- **Pruebas de Aceptación:** Se realizan pruebas casos de uso y requerimientos.



Ejemplo del despliegue en oleadas

Usuarios	25 Grupo piloto	25 Oleada 2	50 Oleada 3	n.. Oleada n
Pruebas	✓	✓	✓	...
Semana	S1	S2	S4	...

Tabla 2. Ejemplo del despliegue Canario por oleadas.

Metodología de Etiquetado de la Información

White Hat Consultores proporcionará consultoría para la clasificación de la información de acuerdo con su nivel de sensibilidad, importancia y confidencialidad,

a través de métodos que permiten a las Organizaciones establecer los criterios necesarios para definir de manera efectiva la clasificación y evitar la fuga de información, a fin de implementar medidas de protección según su relevancia.

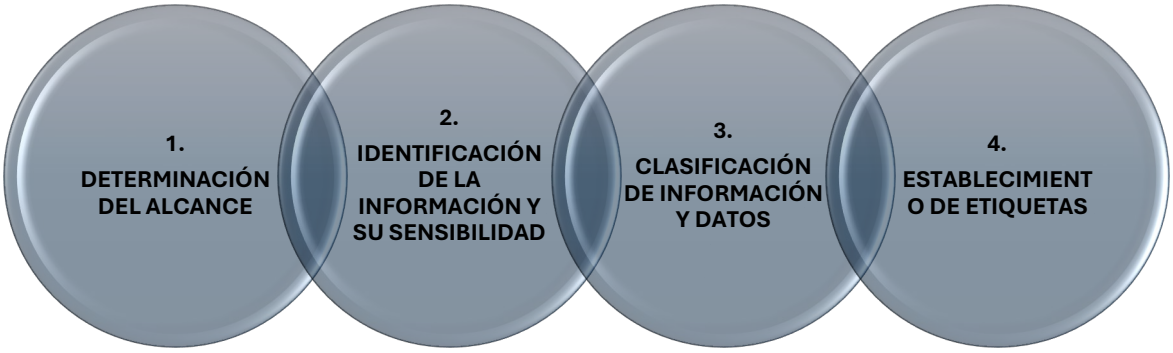


Ilustración 6. Fases de la metodología de etiquetado de la información.



Ilustración 7.Detalles de la Fase 1 - Determinación del Alcance.



Ilustración 8. Detalles de la Fase 2 – Identificación de la información y su sensibilidad.



Ilustración 9. Detalles de la Fase 3 - Clasificación de información y datos.

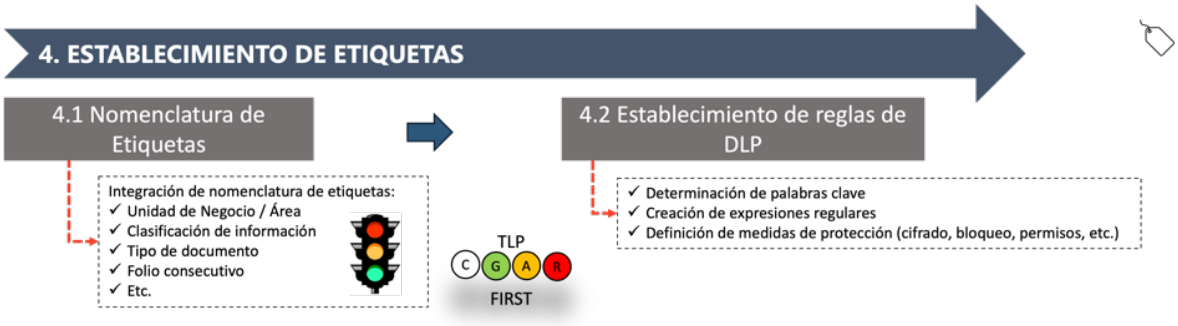


Ilustración 10. Detalles de la Fase 4 - Establecimiento de etiquetas.

El despliegue del etiquetado se deberá realizar de la siguiente manera.

Usuarios	25 Grupo piloto	25 Oleada 2	50 Oleada 3	n Oleada n
Pruebas	✓	✓	✓	...
Semana	S1	S2	S4	...
Etiqueta	✓	✓	✓	...

Tabla 3. Ejemplo del despliegue de Microsoft Purview por oleadas.

Plan de Trabajo y Cronograma de Implementación

Para asegurar el **éxito del proyecto** y **minimizar** cualquier **impacto** en la operación diaria de la organización, la **implementación** se ejecutará **bajo un enfoque por fases**. Cada fase incluirá etapas de diseño, configuración, pruebas controladas (piloto) y despliegue general. Se estima una **duración total del proyecto de 5 semanas**, siempre y cuando se cumplan los tiempos de respuesta y aprobaciones por parte del equipo del cliente.
A continuación, se detalla el cronograma y las actividades por fase.

Fase 1 (Semana 1): Arranque, Identidad y Accesos

Alinear las expectativas operativas del proyecto, evaluar el estado actual del Tenant y establecer una frontera de seguridad robusta basada en la identidad del usuario.

Actividades Clave

- Reunión de inicio (Kick-off) para presentación del equipo, definición de canales de comunicación y validación de accesos administrativos.
- Revisión diagnóstica del estado de seguridad actual del Tenant.
- Diseño y configuración de políticas de Acceso Condicional (bloqueo de autenticación heredada, ubicaciones de confianza).
- Habilitación de la Autenticación Multifactor (MFA) e inicio de pruebas con un grupo de usuarios piloto.

Entregables

- Minuta de reunión de Kick-off

- Informe de estado de seguridad inicial y políticas de identidad configuradas en entorno piloto.

Fase 2 (Semana 2): Gestión y Seguridad de Endpoints

Estandarizar la seguridad de los puntos de conexión (equipos y móviles) para garantizar que solo los dispositivos que cumplan con las normativas corporativas accedan a los datos.

Actividades Clave

- Monitoreo de la configuración MFA de la semana previa.
- Configuración del entorno de Microsoft Intune (MDM y MAM).
- Creación de políticas de cumplimiento (contraseñas, cifrado, versión de SO, etc) y perfiles de configuración para Windows, iOS y Android.
- Ejecución de pruebas de enrolamiento y aplicación de políticas con dispositivos piloto.

Entregables

- Políticas de cumplimiento y protección de aplicaciones (MAM/MDM) creadas en la consola, y validación de dispositivos piloto enrolados.

Fase 3 (Semana 3): Seguridad del Correo y Colaboración

Blindar el flujo de correo electrónico y las herramientas de colaboración contra amenazas externas avanzadas y prevenir la suplantación de identidad.

Actividades Clave

- Auditoría y recomendaciones sobre los registros DNS de seguridad (SPF, DKIM, DMARC).
- Ajuste de políticas de protección: Anti-phishing, Anti-spam y Anti-malware en Exchange Online.
- Configuración de Safe Links y Safe Attachments para detonación de amenazas en entornos seguros.
- Pruebas funcionales simulando el envío y recepción de correos con adjuntos o enlaces controlados.

Entregables

- Controles de seguridad de correo habilitados y reporte de validación de flujo de correo seguro.

Fase 4 (Semana 4): Protección y Gobernanza de la Información

Proveer a la organización de las herramientas necesarias para clasificar su información confidencial y evitar la fuga de datos sensibles (DLP).

Actividades Clave

- Sesión de trabajo para definir la taxonomía y clasificación básica de la información.
- Configuración y publicación de etiquetas de sensibilidad a través de Microsoft Purview.
- Despliegue de políticas base de Prevención de Pérdida de Datos (DLP) orientadas a monitorizar o bloquear el uso compartido no autorizado.
- Activación del registro de auditoría unificada.

Entregables

- Etiquetas de sensibilidad publicadas para los usuarios, políticas DLP base configuradas y auditoría activada.

Fase 5 (Semana 5): Documentación, Transferencia de Conocimiento y Cierre

Entregar formalmente el entorno asegurado, documentar las configuraciones realizadas y capacitar al equipo del cliente para la administración continua.

Actividades Clave

- Revisión final de todas las configuraciones y estabilización del entorno.
- Elaboración de la documentación técnica "As-Built" y el Roadmap de maduración.
- Impartición de la sesión remota de transferencia de conocimiento (capacitación técnica) al equipo administrador.
- Presentación de resultados y formalización del cierre del proyecto.

Entregables

- Documento de arquitectura y políticas aplicadas, Informe de recomendaciones, sesión de transferencia impartida y Acta de cierre del servicio firmada.

Fase 6: Active Directory on-premise (Esta fase se iniciará en la semana 2 y tendrá una duración de 4 semanas)

Objetivo: Revisión y fortalecimiento de Active Directory

Fortalecer la postura de seguridad del **Active Directory On-Premise** de IDEA, reduciendo riesgos asociados a configuraciones heredadas, cuentas privilegiadas, políticas débiles y controles de auditoría insuficientes, estado de salud general garantizando además una **integración híbrida segura con Microsoft Entra ID**.
Esta fase se alinea al modelo **Zero Trust**, extendiendo los controles de identidad desde la nube hacia la infraestructura local.

Actividades Clave

- **Estructura y delegación**
  - Revisión de la **estructura de Unidades Organizativas (OU)**.
  - Validación de segregación administrativa y alineación a buenas prácticas.
  - Revisión de **delegaciones administrativas** y eliminación de permisos innecesarios o excesivos.

- **Políticas y configuración**
  - Revisión de **GPO críticas** relacionadas con:
    - Seguridad de cuentas
    - Endurecimiento de estaciones y servidores
    - Registro y auditoría
  - Evaluación y ajuste de la **Password Policy** (longitud, complejidad, expiración).
  - Revisión de **políticas de auditoría** del dominio.

- **Cuentas y privilegios**
  - Identificación y revisión de **cuentas privilegiadas** (Domain Admins, Enterprise Admins, operadores).
  - Detección de **cuentas con privilegios excesivos**.
  - Revisión de **cuentas inactivas** on-prem y cloud sin actividad de inicio de sesión en los últimos 30 dias.
  - Recomendaciones de reducción de privilegios y separación de identidades administrativas.

- **Sincronización híbrida**
  - Revisión del estado de la **sincronización híbrida (AD Connect / Cloud Sync)**.
  - Validación de cuentas sincronizadas y atributos críticos.

- Identificación de riesgos de identidad híbrida, permisos de cuenta de sincronización y configuración legacy Dirsync.

- **Endurecimiento de controladores de dominio**
  - Revisión de configuración de **Domain Controllers**.
  - Recomendaciones de **hardening** (servicios, protocolos heredados, superficie de ataque).
  - Validación de buenas prácticas de seguridad y resiliencia.

Entregables

- Informe específico de Active Directory On Premise, que incluirá:
  - Hallazgos técnicos
  - Riesgos identificados
  - Brechas frente a buenas prácticas
  - Recomendaciones priorizadas de remediación

Fase 7 – Monitoreo y Alertamiento SOC

Objetivo

Habilitar capacidades de monitoreo y alertamiento operativo sobre el ecosistema Microsoft 365 y el entorno híbrido, proporcionando visibilidad temprana de eventos de seguridad relevantes para la operación institucional y/o su integración con un SOC existente.

Actividades Clave

- **Configuración de casos mínimos de alertamiento**
  Configuración de alertas útiles y accionables para los siguientes casos de uso mínimos:
  - Intentos de acceso sospechosos.
  - Impossible travel.
  - Elevación de privilegios.
  - Desactivación de MFA.
  - Malware detectado.
  - Phishing confirmado.
  - Exfiltración de datos.
  - Eventos DLP críticos.
  - Creación de cuentas privilegiadas.

Las alertas serán configuradas utilizando las capacidades nativas de Microsoft (Entra ID, Defender, Purview), priorizando eventos de alto impacto y bajo ruido operacional.

Entregables

- Matriz de alertas configuradas, indicando:
  - Caso de uso
  - Fuente de datos
  - Severidad
  - Descripción del evento
  - Recomendaciones de respuesta

Propuesta económica

Descripción del bien y/o servicio	Precio (Pesos colombianos)+IVA
Implementación de línea base de seguridad	77,600,000.00 (setenta y siete millones con seiscientos mil pesos colombianos)

Consideraciones:

- El precio está en pesos colombianos
- No incluye impuestos ni retenciones
- La vigencia de la propuesta es de 30 días naturales.

Prerrequisitos técnicos

Para garantizar el éxito del proyecto, la correcta **ejecución del Despliegue Canario** y evitar retrasos en el cronograma establecido, la organización deberá **asegurar el cumplimiento** de las siguientes **condiciones técnicas**, **operativas y de infraestructura** antes del inicio de la fase de configuración. Los requisitos se han segmentado por solución tecnológica para facilitar su validación por parte de los distintos equipos de TI (Redes, Seguridad, Infraestructura, etc).

Generales

- **Licenciamiento Activo:** Contar con las suscripciones activas y aprovisionadas en el Tenant de las licencias requeridas para este alcance: **Microsoft 365 y Enterprise Mobility + Security (EMS) E3.**
- **Accesos y Privilegios:** Provisión de al menos una cuenta con el rol de **Global Administrator (Administrador Global)** para los ingenieros involucrados durante el tiempo que dure el proyecto.
- **Gestión de DNS Público:** Contar con acceso a la consola de administración del proveedor de dominio (DNS) de la organización, o en su defecto, asignar a un recurso técnico interno con la capacidad de crear y modificar registros TXT y CNAME ágilmente (necesario para las configuraciones de seguridad de correo: SPF, DKIM y DMARC).
- **Definición de Grupo Piloto:** Tener identificado y comunicado un grupo de usuarios piloto (recomendado entre 5 y 15 personas) de diferentes áreas de la organización. Estos usuarios deberán contar con dispositivos representativos (Windows, Android, iOS) para validar las políticas de MFA, MDM/MAM y protección de información antes del despliegue general.
- **Líder de Proyecto / Responsable Técnico:** Asignar a un responsable técnico o líder de proyecto por parte de la organización, quien actuará como punto de contacto principal. Este rol deberá tener la autoridad para aprobar las políticas de seguridad diseñadas, coordinar la comunicación con los usuarios piloto y participar activamente en las sesiones de validación y transferencia de conocimiento.
- **Estado del Entorno:** El entorno de Microsoft 365 debe encontrarse en un estado operativo normal (sin incidentes críticos de ciberseguridad activos al momento de iniciar el servicio).

Microsoft Intune

Los prerrequisitos varían dependiendo de si el **enfoque es MDM** (equipos corporativos) **o MAM** (dispositivos personales/BYOD).

- **Ecosistema Apple (iOS):** Creación y aprovisionamiento de un certificado de Apple Push Notification service (APNs) utilizando un ID de Apple corporativo (no personal) para permitir la gestión de dispositivos de esta marca.
- **Ecosistema Google (Android):** Vinculación de una cuenta de Managed Google Play corporativa para habilitar los perfiles de trabajo (Work Profiles) en Android.
- **Sistemas Operativos Soportados:** Los dispositivos para enrolar deben contar con versiones de sistema operativo que se encuentren dentro del ciclo de soporte oficial del fabricante (ej. Windows 10/11 actualizados, iOS 15+, Android 10+).

Microsoft Purview

El éxito de DLP depende tanto de la tecnología como de las definiciones de negocio.

- **Paquetería de Office:** Los equipos deben contar con Microsoft 365 Apps for enterprise (Word, Excel, PowerPoint) instaladas y actualizadas para soportar el monitoreo nativo de DLP sin plugins adicionales.

Microsoft Defender for Office 365

- **Arquitectura de Mensajería:** Los buzones de los usuarios objetivo deben estar alojados y operando nativamente en Exchange Online.
- **Registros MX:** Los registros MX del dominio deben apuntar directamente a Exchange Online Protection (EOP).
- **Filtros de Terceros:** Si el cliente utiliza actualmente un Secure Email Gateway (SEG) de terceros frente a Microsoft 365 (ej. Proofpoint, Mimecast, etc), se requerirá configurar Enhanced Filtering for Connectors (Skip Listing) para asegurar que MDO reciba las direcciones IP de origen correctas y no genere falsos positivos en las políticas de Safe Links y Safe Attachments.

Entregables del Proyecto

Al finalizar el servicio, el cliente recibirá formalmente los siguientes elementos:

- **Entorno Configurado:** Línea base de seguridad completamente operativa en el Tenant de Microsoft 365.
- **Informe de Diagnóstico:** Documento con el estado de seguridad inicial y recomendaciones estratégicas.
- **Documento de Arquitectura:** Detalle técnico de la arquitectura implementada y las políticas aplicadas.
- **Informe específico de Active Directory On Premise**
- **Matriz de alertas configuradas de Monitoreo y Alertamiento SOC**
- **Acta de Cierre:** Documento formal de aceptación y finalización del servicio.

Supuestos y Condiciones del Servicio

Para garantizar el éxito y los tiempos del proyecto, se establecen las siguientes condiciones:

- **Volumetría:** La línea base está estimada para cubrir hasta 250 usuarios y 250 dispositivos (con un margen de variación aceptable del ±15%).
- **Modalidad:** El servicio se ejecutará en formato 100% remoto.
- **Licenciamiento:** La entidad contratante será responsable de proveer el licenciamiento necesario (Microsoft 365 y EMS E3) activo y asignado previo al inicio del proyecto.
- **Horarios:** Las actividades se realizarán en horario laboral estándar. Se definirá un esquema de atención particular y acordado previamente para la atención de eventos críticos.
- **Idioma:** Toda la comunicación, soporte y documentación se entregará en idioma español.

Bolsa de Horas de Acompañamiento

El presente contrato incluye una bolsa de 50 horas de acompañamiento técnico con una vigencia de 12 meses. Esta bolsa está diseñada para brindar flexibilidad y soporte adicional en:

- **Actividades complementarias de implementación.**
- **Ajustes menores a las políticas tras la salida a producción.**
- **Soporte especializado durante la fase de puesta en marcha.**
- **Aclaración técnica de hallazgos derivados de la línea base de seguridad.**

Nota: El consumo y uso de estas horas se realizará bajo demanda y deberá ser acordado y registrado previamente entre los líderes de proyecto de ambas partes.