\newpage

Prefacio

Este manual completo de Microsoft 365 recopila todos los contenidos del curso de administración de Office 365, proporcionando una guía integral para administradores, técnicos de TI y profesionales que necesiten gestionar entornos de Microsoft 365.

El contenido está organizado en seis partes principales que cubren desde los fundamentos básicos hasta configuraciones avanzadas de seguridad y cumplimiento.

Estructura del Manual

- **Parte I**: Fundamentos y configuración inicial
- **Parte II**: Gestión de identidades y usuarios
- **Parte III**: Administración de Exchange Online
- **Parte IV**: SharePoint Online y colaboración
- **Parte V**: Microsoft Teams
- **Parte VI**: Seguridad y cumplimiento

Cada capítulo incluye explicaciones detalladas, ejemplos prácticos y mejores prácticas para la implementación en entornos empresariales.

\newpage

\newpage

Capítulo 1: Documento Informativo: Análisis del Curso de Administración de Office 365

Resumen Ejecutivo

Este documento sintetiza los temas, argumentos y datos clave presentados durante un curso de formación sobre la administración de Microsoft Office 365. El análisis subraya la naturaleza dinámica y en constante evolución de la plataforma, enfatizando la necesidad de una adaptación y aprendizaje continuos por parte de los administradores. El licenciamiento emerge como un pilar fundamental, determinando el acceso a funcionalidades críticas, especialmente en el ámbito de la seguridad. Se destaca la licencia Business Premium como la de mejor relación coste-beneficio debido a la inclusión de herramientas avanzadas como Defender for Business, Intune y Azure AD P1, que habilitan capacidades de seguridad robustas como el Acceso Condicional y la gestión de dispositivos.

La formación distingue claramente entre los métodos de administración: la interfaz web, adecuada para tareas cotidianas, y PowerShell, indispensable para la gestión avanzada, masiva y para configurar opciones no disponibles en la GUI. Se detalla la arquitectura de identidades, con Azure Active Directory (Azure AD) como el servicio central que cohesiona todas las aplicaciones. En cuanto a la colaboración, se expone la transformación de SharePoint desde un modelo jerárquico a una arquitectura plana de sitios independientes y

se establece la interconexión fundamental entre Teams, Sitios de SharePoint y Grupos de Microsoft 365 como la unidad colaborativa moderna. Finalmente, se exploran en profundidad los centros de administración de Exchange, SharePoint, Teams, Seguridad y Cumplimiento (Purview), proporcionando un marco integral para la gestión, seguridad y gobernanza de la plataforma.

---

1. Fundamentos y Naturaleza de la Plataforma Office 365

La plataforma Office 365 se presenta como un ecosistema en permanente evolución, utilizado por más de 200 millones de personas. Esta dinámica obliga a los administradores a adoptar un rol proactivo, no solo de mantenimiento, sino de adaptación y evolución continua.

1.1. Recursos Oficiales de Administración

Para una gestión informada, es crucial consultar las fuentes oficiales de Microsoft, que actúan como la "letra pequeña" y la referencia definitiva del servicio.

Recurso Propósito y Relevancia Descripciones del Servicio Detalla los límites, capacidades y características exactas de cada plan y servicio (p. ej., tamaño de buzón, límites de envío, funcionalidades por licencia). Es la referencia oficial para resolver dudas sobre la inclusión de una característica. Microsoft 365 Roadmap Anuncia las funcionalidades futuras, las que están en desarrollo y las que se están desplegando. Permite anticipar cambios y planificar la adopción de nuevas herramientas. Actualmente, muestra 526 funcionalidades en desarrollo y 110 en despliegue. M365 Maps (m365maps.com) Herramienta externa recomendada que proporciona una matriz visual e interactiva de las características incluidas en cada tipo de licencia, facilitando la comparación y toma de decisiones.

1.2. Gestión de Cambios y Versiones del Tenant

La implementación de cambios en Office 365 no es simultánea para todos los clientes (tenants). Los administradores pueden configurar las preferencias de publicación para controlar la velocidad con la que reciben las actualizaciones.

- Tenant: Se refiere al entorno o inquilino específico de una organización en Office 365.
- Centro de Mensajes (Message Center): Es el canal oficial dentro del panel de administración donde Microsoft notifica los cambios que llegarán específicamente a un tenant, con fechas y detalles. Se destaca que se producen cambios casi a diario.
- Preferencias de Publicación:
    - Versión Estándar (Standard Release): Los cambios llegan más tarde, una vez que han sido probados y estabilizados.
    - Versión Dirigida (Targeted Release): Recibe las actualizaciones con mayor rapidez. Se puede configurar para toda la organización o solo para usuarios específicos (p. ej., administradores), permitiéndoles evaluar los cambios antes de su despliegue general.

2. Licenciamiento: El Habilitador de Funcionalidades

El licenciamiento es el factor más crítico para determinar las capacidades disponibles. Existe una gran disparidad entre planes, especialmente en seguridad.

2.1. Recomendación: Licencia Business Premium

Se identifica la licencia Microsoft 365 Business Premium como la más valiosa actualmente, superando a la Business Standard. Esta recomendación se basa en la reciente inclusión de funcionalidades de alto valor que, si se contrataran por separado, superarían el coste adicional de la licencia.

- Defender for Business: Es una solución de antivirus con capacidades EDR (Endpoint Detection and Response), que permite la caza de amenazas (threat hunting) y la correlación de eventos de seguridad entre equipos. Un producto similar podría costar alrededor de 50 € por equipo al año.
- Intune: Sistema de gestión de plataformas (MDM/MAM) para controlar dispositivos (inventario, distribución de software/actualizaciones, políticas de seguridad, Autopilot).
- Azure AD P1: Habilita funcionalidades de seguridad cruciales. Contratarlo por separado tiene un coste de 5,10 € por usuario al mes.
    - Acceso Condicional: Permite crear reglas de acceso granulares basadas en el contexto del usuario (ubicación, dispositivo, nivel de riesgo) para, por ejemplo, exigir MFA solo fuera de la red corporativa o bloquear inicios de sesión desde ubicaciones sospechosas.
    - Protección de Identidad y Grupos Dinámicos: Herramientas avanzadas para gestionar riesgos y automatizar la membresía de grupos.

2.2. Gestión y Mezcla de Licencias

Es posible y común mezclar distintos tipos de licencias dentro de un mismo tenant para optimizar costes.

- Usuarios con diferentes necesidades: Se pueden asignar licencias básicas (p. ej., Frontline/Kiosco para personal temporal o con acceso limitado) y licencias más potentes para otros usuarios.
- Asignación de Funcionalidades: Dentro de una misma licencia, es posible activar o desactivar aplicaciones específicas para cada usuario, permitiendo un despliegue progresivo de herramientas y evitando abrumar a los usuarios con opciones que aún no han recibido formación.
- Gestión de Licencias: Se puede realizar manualmente por usuario, o de forma automatizada mediante grupos de licencias en Azure AD, donde la pertenencia a un grupo asigna automáticamente un paquete de licencias predefinido.

3. Administración de Identidades y Acceso

La identidad es el "pegamento" que unifica todos los servicios de Office 365. La gestión de usuarios y grupos se realiza principalmente a través del panel de administración, pero su repositorio fundamental es Azure Active Directory (Azure AD).

3.1. Tipos de Objetos de Identidad

Tipo Descripción y Función Usuarios Activos Cuentas que pueden iniciar sesión en Office 365. No consumen coste hasta que se les asigna una licencia. Su identidad reside en Azure AD. Usuarios Invitados Se crean automáticamente cuando se comparte contenido con usuarios externos. Permiten el acceso a recursos específicos compartidos. No se deben eliminar manualmente, ya que se rompería el acceso a dichos recursos. Contactos Son objetos que no pueden iniciar sesión. Su única función es aparecer en la Lista Global de Direcciones (GAL) para que todos los usuarios de la organización puedan enviarles correos fácilmente o incluirlos en listas de distribución. Buzones Compartidos No consumen licencia y actúan como un buzón de correo colaborativo al que múltiples usuarios pueden acceder. Ideal para direcciones genéricas como soporte@empresa.com. Se pueden convertir buzones de usuarios que dejan la empresa en buzones compartidos para conservar el historial y liberar la licencia.

3.2. Grupos

Tipo de Grupo Descripción y Propósito Listas de Distribución El tipo más simple. Es una dirección de correo que expande el mensaje a todos sus miembros. No tiene repositorio propio. Grupos de Seguridad Utilizados para asignar permisos a recursos. Su uso en el modelo moderno de SharePoint es limitado. Grupos de Microsoft 365 Es un objeto central para la colaboración. Al crearse, provisiona un conjunto de recursos compartidos: un buzón y calendario de grupo (Exchange), un sitio de colaboración (SharePoint) y un bloc de notas. Es la base sobre la que se construyen los equipos de Microsoft Teams.

3.3. Autenticación Multifactor (MFA)

Microsoft ha anunciado la obligatoriedad de los Security Defaults, que incluyen la activación de MFA para todos los usuarios a partir de septiembre/octubre. Para usuarios sin teléfono de empresa, se proponen alternativas al SMS o la app de autenticación:

- Windows Hello: El uso de biometría (huella, reconocimiento facial) en un equipo compatible cuenta como un segundo factor.
- Llaves de Seguridad FIDO2 (p. ej., Yubico): Dispositivos físicos USB/NFC que actúan como "algo que tienes". Un usuario puede conectarla a su PC y pulsar un botón para verificar su identidad. Tienen un coste asequible (desde 25 €).

4. Métodos de Administración

La plataforma se puede gestionar a través de dos interfaces principales con propósitos distintos.

4.1. Panel de Administración Web

- Función: Adecuado para tareas del día a día y configuraciones básicas.
- Estructura: Se organiza en un panel principal para acciones comunes (gestión de usuarios, grupos) y múltiples Centros de Administración especializados (Exchange, SharePoint, Teams, Seguridad, etc.). Es común tener que saltar entre diferentes centros para completar una configuración.

4.2. PowerShell

- Función: Esencial para la administración avanzada, automatización, tareas masivas y para acceder a configuraciones que no están disponibles en la interfaz web. Su conocimiento no es opcional para un administrador completo.
- Módulos Necesarios: Para interactuar con los diferentes servicios, se deben instalar módulos específicos.
    - Identidad: MSOnline (antiguo) y AzureAD (nuevo). Se recomienda instalar ambos por compatibilidad con scripts.
    - Exchange: ExchangeOnlineManagement (V2).
    - SharePoint: Microsoft.Online.SharePoint.PowerShell (módulo oficial, limitado a la gestión de sitios) y PnP.PowerShell (módulo de la comunidad, esencial para manipular el contenido dentro de los sitios).
    - Teams: MicrosoftTeams.
- Comandos y Técnicas Clave:
    - La conexión se establece con cmdlets como Connect-ExchangeOnline o Connect-AzureAD.
    - Out-GridView -PassThru: Un comando muy útil que muestra la salida de un cmdlet (p. ej., Get-Mailbox) en una ventana gráfica con filtros, permitiendo seleccionar objetos visualmente y pasar la selección al siguiente comando en la tubería (|).

- Import-Csv | ForEach-Object: Técnica estándar para realizar operaciones masivas, leyendo los datos desde un archivo CSV y procesando cada fila en un bucle.

4.3. Power Automate vs. PowerShell

Power Automate está diseñado para la automatización de procesos de usuario final, no para la administración de la plataforma. No puede ejecutar scripts de PowerShell directamente. Para una automatización de nivel administrativo similar, se debe recurrir a Azure Logic Apps, que puede interactuar con las APIs de la plataforma y ejecutar scripts.

5. Administración del Correo Electrónico (Exchange Online)

La gestión del correo se centraliza en el Centro de Administración de Exchange, que está migrando de una versión "clásica" a una moderna.

5.1. Registros DNS Críticos

La correcta configuración de los registros DNS es vital para el flujo de correo y la conectividad de los clientes.

Registro Propósito MX Dirige el correo entrante a los servidores de Office 365. SPF (Sender Policy Framework) Declara qué servidores están autorizados para enviar correo en nombre de un dominio, ayudando a combatir el spam y el spoofing. DKIM (DomainKeys Identified Mail) Añade una firma digital a los correos salientes para verificar su autenticidad e integridad. Es un complemento a SPF. DMARC Indica a los servidores receptores qué hacer si un correo falla las comprobaciones de SPF o DKIM (no hacer nada, cuarentena o rechazar). Autodiscover Permite a los clientes de Outlook configurar automáticamente la cuenta y localizar el buzón del usuario. Es un servicio web obligatorio para clientes modernos.

5.2. Herramientas de Diagnóstico

- Microsoft Remote Connectivity Analyzer: Herramienta web para realizar pruebas de conectividad desde fuera de la red (p. ej., verificar Autodiscover, conectividad de Outlook, flujo de correo).
- Analizador de Mensajes: Permite pegar las cabeceras de un correo para analizar su ruta y propiedades de forma legible.
- Herramienta de diagnóstico de Outlook: Accesible manteniendo Ctrl y haciendo clic derecho en el icono de Outlook en la bandeja del sistema. Permite probar la configuración de Autodiscover y ver el XML de configuración.

5.3. Flujo de Correo y Reglas de Transporte

- Seguimiento de Mensajes: La herramienta principal para investigar qué ha ocurrido con un correo específico (si se entregó, falló, fue marcado como spam, etc.). Permite búsquedas de hasta 90 días.
- Reglas de Transporte: Permiten aplicar acciones automáticas a los correos en tránsito (entrantes, salientes o internos) basadas en condiciones. Ejemplos: adjuntar un descargo de responsabilidad (disclaimer), reenviar una copia a un buzón de archivo, bloquear adjuntos específicos o notificar a un moderador.
- Conectores: Se utilizan para configurar rutas de correo especiales, principalmente para integrar dispositivos locales (impresoras multifunción) o aplicaciones que necesitan enviar correo (hacer "relay") a través de Office 365, tratándolos como una fuente de confianza basada en su IP pública.

5.4. Políticas de Seguridad del Correo

Configurables en el Centro de Seguridad y Cumplimiento, son cruciales para la protección.

- Anti-Phishing: Protege contra la suplantación de identidad (spoofing) de usuarios y dominios. Las licencias avanzadas permiten una protección más granular.
- Anti-Spam: Define umbrales y acciones para el correo no deseado. Es importante tener cuidado al configurar filtros demasiado estrictos (p. ej., rechazar correos sin SPF válido), ya que muchos remitentes legítimos tienen configuraciones incorrectas.
- Anti-Malware: Bloquea el malware. La política por defecto es robusta, pero se puede personalizar para bloquear tipos de archivos adicionales que puedan ser vectores de ataque (p. ej., .iso, .lnk).

6. Administración de SharePoint Online

SharePoint ha experimentado una transformación fundamental, abandonando su antiguo modelo jerárquico por una arquitectura moderna y plana.

6.1. El Cambio de Arquitectura: De Jerarquía a Modelo Plano

- Modelo Clásico (Antiguo): Se basaba en una "Colección de Sitios" que contenía un sitio principal y una jerarquía de subsitios. Esta estructura implicaba herencia de permisos y navegación, lo que la hacía rígida y compleja de gestionar.
- Modelo Moderno (Actual): Elimina el concepto de subsitios jerárquicos. Cada sitio de SharePoint moderno es una colección de sitios independiente. No hay herencia de permisos entre ellos. La estructura se crea de forma "artificial" mediante la navegación y los Sitios Centrales (Hub Sites).
    - Hub Sites: Un sitio puede ser designado como "central", y otros sitios pueden asociarse a él. Los sitios asociados heredan la barra de navegación superior y el tema visual del hub, creando una experiencia de usuario consistente, pero sin crear una dependencia estructural ni heredar permisos.

6.2. Tipos de Sitios Modernos

Tipo de Sitio Propósito Principal Creado por defecto con... Sitio de Colaboración Espacio para que un equipo trabaje activamente con documentos y contenido (modelo "many-to-many"). Grupos de Microsoft 365 y Equipos de Teams. Sitio de Comunicación Diseñado para difundir información a una audiencia amplia, con pocos creadores de contenido (modelo "one-to-many"). Ideal para intranets y portales de noticias. No se asocia a un Grupo de Microsoft 365.

6.3. Sincronización con OneDrive: Una Advertencia

Se desaconseja firmemente el uso de la función "Sincronizar" para bibliotecas de documentos de SharePoint (colaborativas).

- Riesgos: A medida que más usuarios sincronizan la misma biblioteca, aumenta exponencialmente la probabilidad de conflictos de sincronización, creación de archivos duplicados y pérdida de la integridad de los datos, especialmente si los usuarios trabajan sin conexión o la sincronización se interrumpe.
- Alternativa Recomendada: Trabajar directamente desde la interfaz de Teams o SharePoint Online. Esto garantiza que todos los usuarios operen sobre la única versión verdadera del documento, aprovechando la coautoría en tiempo real y evitando problemas de sincronización. OneDrive es para archivos individuales; SharePoint (a través de Teams) es para archivos colaborativos.

7. Administración de Microsoft Teams

Teams es la interfaz principal para la colaboración, pero funcionalmente es una capa de visualización y servicios construida sobre la infraestructura de Grupos de Microsoft 365 y SharePoint.

- Creación de un Equipo: Al crear un equipo en Teams, automáticamente se provisiona un Grupo de Microsoft 365 y un Sitio de Colaboración de SharePoint por debajo.
- Canales y Carpetas: Cada canal creado en un equipo corresponde a una carpeta dentro de la biblioteca de documentos del sitio de SharePoint asociado.
- Canales Privados: Al crear un canal privado, se crea un sitio de SharePoint completamente nuevo e independiente para almacenar sus archivos, con permisos restringidos solo a los miembros de ese canal.
- Administración: Se realiza desde su propio centro de administración. La gestión se basa en directivas (policies) que permiten aplicar configuraciones granulares a diferentes conjuntos de usuarios (p. ej., directivas de reuniones, de mensajería, de aplicaciones, de llamadas). La aplicación de cambios en las directivas de Teams puede tardar hasta 24 horas en propagarse.

8. Seguridad y Cumplimiento (Purview)

La gestión de la seguridad y el cumplimiento normativo se divide en dos centros de administración principales, reflejando la separación de roles entre administradores de TI y personal legal/de auditoría. La suite de cumplimiento ha sido renombrada como Microsoft Purview.

8.1. Centro de Seguridad

- Puntuación de Seguridad (Security Score): Herramienta que evalúa la postura de seguridad del tenant y ofrece recomendaciones de mejora con instrucciones paso a paso para implementarlas.
- Análisis de Amenazas: Proporciona inteligencia sobre campañas de ataque globales, detallando sus técnicas y el posible impacto en la organización.
- Gestión de Dispositivos (con Intune): Permite ver el inventario de dispositivos, su estado de cumplimiento, vulnerabilidades y aplicar políticas de seguridad desde un único punto.
- Auditoría: Es fundamental activar el registro de auditoría, ya que en tenants más antiguos no viene habilitado por defecto. Este registro captura todas las acciones de usuarios y administradores, siendo indispensable para investigaciones de seguridad.

8.2. Centro de Cumplimiento (Purview)

- Clasificación de Datos: Permite definir etiquetas de confidencialidad (para cifrar y controlar el acceso a la información, p. ej., impedir la impresión) y etiquetas de retención (para evitar que los datos se eliminen antes de que expire un período legal). Estas funcionalidades requieren licencias avanzadas.
- eDiscovery: Herramienta para realizar búsquedas e investigaciones legales sobre el contenido de la plataforma (correo, SharePoint, Teams) en respuesta a requerimientos judiciales, exportando los resultados en un formato admisible.
- Information Protection: Conjunto de herramientas para proteger la información sensible dondequiera que se encuentre, mediante el uso de etiquetas y políticas de prevención de pérdida de datos (DLP).

\newpage

Capítulo 2: ### **Propósito de Agregar un Dominio**

Cuando se da de alta un *tenant* (inquilino) en Office 365 por primera vez, este viene con un dominio interno gestionado por Microsoft, que suele tener un formato como `cpsl.onmicrosoft.com`. Aunque funcional, no es lo ideal para el uso diario, ya que los usuarios prefieren iniciar sesión y usar direcciones de correo electrónico que les resulten más familiares y profesionales, como las de su propia empresa.

Agregar tu propio dominio (por ejemplo, `cpsl.com` o el `.cat` que mencionas) te permite:

- Asignar a los usuarios un **nombre de inicio de sesión** (conocido como User Principal Name o UPN) que coincida con su dirección de correo electrónico corporativa.
- Tener **múltiples dominios** dentro de la misma organización. Por ejemplo, podrías tener `cpsl.com` y `cpsl.cat` y asignar a unos usuarios un dominio y a otros, otro. Incluso se pueden usar subdominios como `external.cpsl.com`.
- Permitir que un usuario tenga una **dirección de correo principal** en un dominio, pero también reciba correos enviados a alias en otros dominios que tengas registrados.

Proceso Detallado para Agregar y Configurar un Dominio

El proceso consta de dos fases principales: la verificación de la propiedad del dominio y la configuración de los servicios (principalmente el correo electrónico).

1. Verificación de la Propiedad del Dominio

Para agregar un dominio, debes demostrarle a Microsoft que eres el propietario. Esto se hace desde el panel de administración, en la sección de **Configuración > Dominios**. El proceso es el siguiente:

1. Haces clic en **"Agregar un dominio"** e introduces el nombre del dominio que quieres registrar (por ejemplo, `pepito.com`).

2. Microsoft te pedirá una **prueba de que el dominio es tuyo**. Para ello, ofrece tres métodos principales:

    - **Agregar un registro TXT en tu DNS (método más común)**: Esta es la opción más sencilla. Microsoft te proporcionará un valor específico (por ejemplo, `MS=ms6539...`) que debes crear como un registro de tipo TXT en la configuración de DNS externa de tu dominio. Una vez creado, esperas un poco y le das al botón de "Verificar". Cuando se confirma, el dominio ya puede ser usado y este registro TXT se puede eliminar si lo deseas.
    - **Agregar un registro MX**: Este método es un poco más "peligroso" porque los registros MX gestionan el flujo de correo. Sin embargo, se puede crear un registro MX con una prioridad muy baja para que no afecte al flujo de correo existente durante la verificación.
    - **Agregar un archivo de texto en el sitio web del dominio**: Si tienes una página web asociada a tu dominio (ej. `cpsl.com`), puedes subir un archivo de texto específico a una URL que Microsoft te indicará. El sistema comprobará que el archivo está ahí y con eso verificará que controlas el dominio.

2. Configuración de los Servicios (Registros DNS)

Una vez verificado el dominio, necesitas crear una serie de registros DNS adicionales para que servicios como el correo electrónico funcionen correctamente. Los registros más importantes son:

- **Registro MX (Mail Exchanger)**: Este registro es crucial y su función es **dirigir todo el flujo de correo electrónico entrante hacia los servidores de Office 365**.

- **Registro SPF (Sender Protection Framework)**: Es un sistema diseñado para reducir el spam. Se trata de un registro TXT en tu DNS público donde declaras qué servidores de correo están autorizados para enviar correos en nombre de tu dominio. Microsoft te pedirá que incluyas `spf.protection.outlook.com` para autorizar a sus servidores. Este registro puede tener modificadores como:
  - `-all` (hard fail): Indica que si un correo no proviene de los servidores autorizados, es falso.
  - `~all` (soft fail): Es menos estricto; sugiere que el correo podría ser falso, pero no lo califica como tal de forma automática.
- **Registro CNAME para Autodiscover**: Este es un alias (por ejemplo, `autodiscover.cpsl.com`) que apunta a los servidores de Microsoft. Su función es permitir que las aplicaciones de Outlook (a partir de la versión 2010) **encuentren y configuren automáticamente el buzón de un usuario sin necesidad de saber en qué servidor físico se encuentra**. El cliente de Outlook busca este servicio para obtener la configuración en un archivo XML. Es importante saber que si tu dominio interno de Active Directory se llama igual que el externo, este registro debe crearse también en el DNS interno. \newpage

Capítulo 3: El proceso de asignación de licencias es fundamental en Microsoft 365, ya que una licencia es lo que otorga a los usuarios el derecho a utilizar las distintas funcionalidades y aplicaciones de la plataforma.

Conceptos Clave del Licenciamiento

Una cuenta de usuario por sí sola no tiene coste hasta que se le asigna una licencia. Sin una licencia, un usuario puede iniciar sesión en Office 365, pero no tendrá acceso a funcionalidades como SharePoint, Teams o un buzón de correo. Las funcionalidades disponibles, especialmente en el ámbito de la seguridad, dependen directamente del tipo de licencia asignada. A mayor coste de la licencia, se obtienen más posibilidades de auditoría, alertas y otras herramientas avanzadas.

Proceso de Asignación de Licencias

Existen métodos manuales y automáticos para asignar licencias a los usuarios.

1. Verificación de Licencias Disponibles

Antes de asignar licencias, es importante saber de cuáles dispone la organización. Esta información se encuentra en la sección de **Facturación > Licencias** en el centro de administración. Allí se puede ver el total de licencias compradas, cuántas están asignadas y cuántas quedan libres.

2. Asignación Manual (a través del Centro de Administración)

Este es el método más directo y se realiza siguiendo estos pasos:

1. Ir a **Usuarios > Usuarios activos** en el centro de administración.
2. Seleccionar el usuario al que se le quiere asignar una licencia.

3. En el panel del usuario, ir a la pestaña **Licencias y aplicaciones**.

En este panel, se pueden activar o desactivar aplicaciones individuales que forman parte del paquete de la licencia. Esta granularidad es útil, por ejemplo, para introducir funcionalidades de manera progresiva a los usuarios a medida que reciben formación. Es importante saber que algunas aplicaciones están vinculadas, como OneDrive, que forma parte de SharePoint y no puede desactivarse de forma independiente.

3. Mezcla de Licencias

Es posible tener una mezcla de distintos tipos de licencias dentro de la misma organización. Por ejemplo, se pueden asignar licencias más básicas y económicas (como las de *Frontline*) a personal externo o temporal que no requiere todas las funcionalidades de un usuario de oficina.

Incluso un mismo usuario puede tener asignados varios paquetes de licencias diferentes simultáneamente. La interfaz de administración muestra claramente qué aplicaciones provienen de cada paquete de licencia asignado. Por ejemplo, un usuario podría tener una licencia *Business Standard* y, además, una licencia de prueba como *Teams Exploratory Trial*.

4. Asignación Automática

Para organizaciones más grandes o para simplificar la gestión, Office 365 ofrece métodos para automatizar la asignación de licencias:

- **Asignación al primer inicio de sesión**: Se puede configurar que las licencias se asignen automáticamente la primera vez que un usuario inicia sesión.
- **Asignación basada en grupos**: Un método más avanzado y recomendable para la gestión a gran escala es asignar licencias según la pertenencia a grupos de usuarios en Azure AD. De esta forma, al añadir un usuario a un grupo determinado (por ejemplo, "Comerciales"), se le asigna automáticamente el paquete de licencias predefinido para ese grupo.

5. Gestión mediante PowerShell

La gestión de licencias también se puede realizar mediante **PowerShell**, lo cual es especialmente útil para operaciones masivas. Se pueden utilizar comandos, como `Set-MSOLUser`, para asignar licencias, cambiar contraseñas o modificar el nombre principal de usuario. También es posible incluir la asignación de licencias como parte de scripts para la creación masiva de usuarios.

Gestión de Costes y Casos Especiales

- **Liberación de licencias**: Cuando un empleado deja la empresa, una práctica común es convertir su buzón en un **buzón compartido**. Esto permite conservar el correo sin consumir una licencia, ya que los buzones compartidos no requieren una.
- **Recursos sin licencia**: Algunos tipos de buzones, como los de **sala** (para salas de reuniones) o los de **equipamiento** (para recursos como proyectores o vehículos), no consumen licencias.
- **Licencias de prueba**: Es importante revisar si los usuarios tienen licencias de prueba, como la "Microsoft Teams Exploratory Trial", que fue una licencia gratuita durante la pandemia. Estas licencias caducan y deben ser reemplazadas por licencias de pago para no perder la funcionalidad. \newpage

Capítulo 4: | Característica | Usuario Activo (con Licencia) | Usuario Invitado (Guest) | Contacto (Contact) |

| :--- | :--- | :--- | :--- | | **Definición** | Usuario con una licencia asignada que incluye Exchange Online (como mínimo Exchange P1). | Usuario cuyo correo se gestiona externamente (ej. Hotmail.com), pero que accede a tu entorno. | Objeto de identidad que es un destinatario básico (recipient) de Exchange. | | **Capacidad de Inicio de Sesión** | **Puede** iniciar sesión en Office 365. | **Puede** iniciar sesión en el *tenant* (entorno) de la organización. | **No puede** iniciar sesión en el directorio activo ni en Office 365. | | **Buzón de Correo** | Tiene un buzón de correo gestionado **dentro** de Exchange Online. | Su correo es gestionado **externamente** (ej. Gmail, Hotmail). | Su correo se gestiona **fuera** de la organización. | | **Acceso a Recursos** | Accede a funcionalidades según la licencia (SharePoint, Teams, etc.). | Solo accede a los recursos que se le hayan **compartido**. | **No tiene** acceso a archivos ni nada. | | **Propósito Principal** | Utilizar los servicios completos de Office 365. | Colaboración externa sobre recursos compartidos (como documentos o Teams). | Aparecer en la **Lista Global de Direcciones (GAL)** de Exchange para recibir correos. | | **Permisos Típicos en Teams** | Lector y escritor (según el rol en el equipo). | Generalmente, es de **lectura y escritura**, pudiendo hacer la mayoría de las cosas de un usuario normal en el equipo. | N/A (No puede iniciar sesión ni acceder a Teams). | | **Creación** | Creado y gestionado dentro del entorno de nube/AD. | Objeto creado automáticamente cuando se comparte algo con un usuario externo. | Creado manualmente o importado a nivel global (por ejemplo, con Power Shell). |

\newpage

Capítulo 5: ### **¿Qué es un Usuario Invitado?**

Un **usuario invitado** es un tipo de objeto de identidad dentro de Microsoft 365, distinto de los usuarios activos y los contactos. Está diseñado para personas externas a tu organización (como colaboradores, personal externo o de otras empresas) con las que necesitas compartir recursos específicos.

A diferencia de un usuario activo, un invitado **solo puede acceder a aquellos recursos que se le hayan compartido explícitamente**. No puede iniciar sesión en el entorno de Office 365 de forma general ni tendrá acceso a un buzón de correo propio o a otras funcionalidades a menos que se le comparta algo directamente.

Proceso de Creación de Usuarios Invitados

La creación de usuarios invitados es mayormente un proceso automático que ocurre en segundo plano:

1. **Creación Automática (el método más común)**: Cuando un usuario de tu organización comparte un recurso (como un documento, un sitio de SharePoint o un Team) con una persona externa, el sistema **crea automáticamente un "objeto de invitado"**. Este objeto sirve como un "enganche" para la identidad de esa persona externa, permitiendo al sistema saber que tiene permiso para acceder a ese recurso concreto.
2. **Creación Manual**: También es posible crear un usuario invitado de forma manual, aunque es menos frecuente en el día a día. Este proceso se realiza desde el portal de **Azure AD**, donde se puede invitar a un usuario, definir su identidad, enviarle un mensaje de bienvenida, añadirlo a grupos específicos y aplicarle ciertas restricciones de acceso.

Los usuarios invitados se distinguen en la lista de usuarios activos porque su nombre de usuario suele incluir el sufijo `_guest` y su dirección de correo electrónico original externa (por ejemplo, de Hotmail o Gmail).

Acceso y Permisos de los Usuarios Invitados

El nivel de acceso de un usuario invitado depende del recurso que se le comparte:

- **Acceso General**: Su acceso está limitado únicamente a lo que se ha compartido con ellos. Si se deja de compartir un recurso con un invitado, este **no pierde su cuenta de invitado, pero sí pierde el acceso** a dicho recurso.
- **Acceso en Microsoft Teams**: Por defecto, un invitado en un Team tiene permisos bastante amplios, similares a los de un miembro normal de la organización. Las directivas de la organización permiten configurar lo que pueden hacer, como por ejemplo:
    - Realizar llamadas privadas uno a uno.
    - Participar en reuniones con vídeo.
    - Compartir su pantalla.
    - Editar los mensajes que han enviado.
    - Utilizar la función de "Reunirse ahora".
- **Nuevas Funcionalidades**: Microsoft está implementando opciones más granulares, como la posibilidad de **compartir un único canal de un Team con personal externo**, en lugar de tener que compartir el equipo completo, lo cual mejora la seguridad y la gestión de la colaboración.

Gestión y Administración

La gestión de los usuarios invitados se realiza de la siguiente manera:

- **Gestión del día a día**: Normalmente es un proceso automático. Cuando alguien comparte algo, el invitado se crea; si se necesita una gestión más detallada, se debe acudir a Azure AD.
- **¡Advertencia sobre la eliminación!**: Es muy importante **no eliminar manualmente los usuarios invitados** desde la lista de usuarios activos. Si se borra un invitado, se rompe la compartición de todos los elementos con esa persona y restaurar esos accesos es un proceso muy complicado.
- **Políticas de compartición**: Desde el centro de administración de SharePoint, se pueden establecer directivas a nivel de sitio para definir con quién se puede compartir, por ejemplo, permitiendo compartir con "invitados nuevos y existentes".

Diferencia entre Usuario Invitado y Contacto

Es fundamental no confundir a un usuario invitado con un "contacto", ya que cumplen funciones totalmente diferentes:

- **Usuario Invitado**: Su propósito es **dar acceso a recursos compartidos** (ficheros, Teams, etc.).
- **Contacto**: Un contacto **no puede iniciar sesión ni acceder a ningún recurso**. Su única función es aparecer en la "libreta de direcciones global" de la organización para que los usuarios internos puedan encontrar fácilmente su dirección de correo y enviarles emails. También pueden ser añadidos a listas de distribución. \newpage

Capítulo 6: ### 1. Lista de Distribución (Distribution List - DL)

- **¿Qué es?** Es un **destinatario de Exchange** (*recipient*).
- **Función principal:** Es un mecanismo sencillo para **enviar correo a múltiples miembros individuales** utilizando una sola dirección de correo electrónico (alias).
- **Funcionamiento clave:** Cuando recibe un correo, lo multiplica (proceso llamado *fanning out*) y lo entrega a la bandeja de entrada de cada miembro.
- **Almacenamiento: No son un buzón**; no tienen un repositorio de información propio para almacenar correos.
- **Administración:** Por defecto, **no son accesibles desde fuera** de la organización. Se pueden configurar para requerir **aprobación** de un delegado antes de enviar el correo.
- **Contexto:** Son anteriores a los Grupos de Microsoft 365.

2. Grupo de Seguridad (Security Group)

- **¿Qué es?** Es un tipo de grupo diseñado para **otorgar permisos**.
- **Función principal:** Se utiliza para gestionar el **acceso** a distintos tipos de contenido o recursos.
- **Uso en SharePoint:** Aunque existen, se usan **muy poco** en el modelo moderno de SharePoint.
- **Relación con correo:** Por defecto, un Grupo de Seguridad no tiene cuenta de correo.

3. Grupo de Seguridad Habilitado para Correo (Mail-Enabled Security Group)

- **¿Qué es?** Es una variante de un Grupo de Seguridad.
- **Función principal:** Además de **otorgar permisos**, tiene asignada una **cuenta de correo electrónico**.
- **Funcionamiento:** Funciona simultáneamente como un Grupo de Seguridad (para permisos) y como un Grupo de Distribución (para correo).

4. Grupo de Microsoft 365 (Grupo Moderno o Unified Group)

- **¿Qué es?** Es un **objeto especial** creado para fomentar la **colaboración**.
- **Almacenamiento clave:** A diferencia de una Lista de Distribución, un Grupo de Microsoft 365 **sí tiene un buzón propio** (un buzón compartido de Exchange).
- **Componentes de colaboración:** Incluye varios elementos para la colaboración además del buzón:
  - Un **calendario compartido**.
  - Un **repositorio de ficheros** (que proviene de SharePoint).
  - Un **blog de notas compartido**.
- **Relación con Teams y SharePoint:**
  - Un Grupo de Microsoft 365 es esencialmente un **sitio moderno de SharePoint**.
  - Sirve como la capa subyacente para un **equipo de Teams** (Team). Teams es una capa adicional de visualización e interacción sobre este grupo de Office 365.

\newpage

Capítulo 7: El buzón compartido es un tipo de **destinatario especial de Exchange**.

1. ¿Qué es un Buzón Compartido y Para Qué Sirve?

Un buzón compartido se utiliza principalmente para direcciones genéricas o de equipo, como `soporte@` o `pedidos@`.

- **Diferencia clave:** A diferencia de una Lista de Distribución, el Buzón Compartido **sí tiene un buzón separado** (un repositorio de información propio) del de los miembros que acceden a él.
- **Acceso:** Los miembros tienen que **acceder activamente** a este buzón compartido para ver los correos, ya que el correo no se les envía a su buzón individual.
- **Licenciamiento:** La gran ventaja del buzón compartido es que **no consume licencia**.
- **Uso común:** Si un usuario se va de la empresa, una técnica común es **convertir su buzón individual a buzón compartido**. De esta forma, se mantiene su historial de correo (todo el contenido del buzón) sin consumir una licencia.

2. Administración y Permisos

Para que un usuario pueda trabajar con un buzón compartido, un administrador debe otorgarle permisos específicos:

Permiso	Propósito	Explicación
Acceso Completo (*Full Access*)	Permite **leer y administrar** el buzón, incluyendo la capacidad de abrirlo.	Cuando un administrador otorga este permiso a un usuario (ej. a Alex y a Megan), ese buzón aparecerá como un buzón adicional en su cliente de correo (a través de *automapping*).
Enviar Como (*Send As*)	Permite **enviar correos electrónicos** en nombre de ese buzón.	Al enviar un correo, en el campo "De" aparecerá la dirección del buzón compartido (`soporte@`) y el destinatario lo recibirá como si lo hubiera enviado el propio buzón, sin que aparezca el nombre del miembro real.

Nota sobre Envío en Nombre de: Existe un permiso relacionado, **"Enviar en Nombre de"** (*Send on Behalf*), donde el destinatario ve que el correo fue enviado por el miembro (ej., Benito) *en nombre* del buzón compartido (ej., Manu). Este es un nivel de suplantación inferior y menos común.

3. Configuraciones Especiales

- **Respuestas Automáticas:** Se le pueden activar respuestas automáticas. Sin embargo, funcionan igual que las de un buzón normal, con un límite de **una respuesta al día** al mismo remitente. Esto es importante para informar que se está procesando su solicitud.
- **Almacenamiento de Copias:** Se puede configurar si la copia del correo enviado desde el buzón compartido se guarda solo en el buzón compartido o si también se guarda una copia en la bandeja de elementos enviados del miembro individual. Esto se gestiona desde la interfaz de administración.

Un buzón compartido es una opción más que se suma a la Lista de Distribución y al Grupo de Office 365 para gestionar comunicaciones colectivas.

\newpage

Capítulo 8: # Roles de Administración y Granularidad de Permisos

Los roles de administración sirven para **separar las tareas de administración**. En lugar de que todos los administradores tengan el mismo acceso a todas las configuraciones (*administradores globales*), los roles permiten aplicar permisos de forma más granular para tareas específicas.

Aquí tienes una explicación detallada de los roles que hemos cubierto y el concepto de granularidad de permisos:

1. El Concepto de Granularidad

- **Administradores Globales:** Son aquellos que tienen **todos** los permisos sobre la plataforma. Curiosamente, incluso ellos pueden no tener ciertos permisos de forma predeterminada (como permisos para abrir casos legales), aunque tienen la capacidad de otorgárselos a sí mismos.
- **Roles Especializados:** Permiten asignar funcionalidades específicas. Cuantos más roles se tengan, más se puede separar la administración. Por ejemplo, existe el rol de **Administrador de Facturación** para gestionar facturas.

2. Roles en el Panel de Administración General

En el panel de administración, se puede ver una lista de **muchos roles** de administración, que pueden ser muy granulares.

- **Asignación:** Se gestionan directamente en la configuración de la cuenta de cada usuario, en la sección de Roles de Administración.

3. Roles en el Contexto del Correo Electrónico (Exchange Online)

El sistema de correo Exchange (la base de Exchange Online) fue el primer producto que utilizó un sistema de control de acceso muy granular llamado **RPAC** (Role-Based Access Control).

- **Granularidad Extrema:** En Exchange, se puede definir un rol de administración diciéndole **qué comandos de Power Shell** van a poder utilizar, **con qué parámetros** y **para qué conjunto de usuarios**. Por ejemplo, podrías crear un rol de "administrador de direcciones de correo electrónico para los usuarios de marketing de Bulgaria".
- **Roles Legales/Compliance:** Dentro de la gestión de roles, existe una división entre el **rol de administración** y el **rol legal**. Los profesionales legales (abogados) necesitan roles que les permitan acceder al centro de cumplimiento (*compliance*) para tareas como realizar un descubrimiento legal (*eDiscovery*), sin tener acceso al panel de seguridad general. Esto requiere ser miembro de ciertos grupos de roles especializados.

4. Directivas de Paquetes de Roles (Teams)

En entornos complejos, asignar roles (o, en el caso de Teams, **Directivas**) uno por uno puede ser tedioso.

- **Paquetes de Directivas:** En Teams, puedes crear un **pack de directiva** (o paquete de roles). Este paquete es una configuración estandarizada que agrupa múltiples directivas (de chat, de llamadas, de reuniones, de aplicaciones, etc.) para un perfil específico (ej. un comercial o un profesor). Esto permite asignar todas las configuraciones necesarias de golpe, en lugar de una a una.

En resumen, el sistema de roles está diseñado para ofrecer una **separación de funciones** (separar al administrador del abogado, por ejemplo) y una **granularidad máxima**, especialmente en Exchange y Teams, donde se pueden crear configuraciones muy específicas para subconjuntos de usuarios.

\newpage

Capítulo 9: Un **buzón de sala** (*Room Mailbox*) y un **buzón de equipamiento** (*Equipment Mailbox*) son tipos de **destinatarios especiales de Exchange**.

El concepto fundamental es que son objetos que tienen asociado un **calendario**, permitiendo a los usuarios ver si están **libres o están ocupados**.

1. Buzón de Sala (*Room Mailbox*)

- **Propósito:** Representa una ubicación física, como una sala de reuniones.
- **Licenciamiento: No ocupa licencia**.
- **Uso:** Un usuario puede convocar una reunión y agregar el buzón de sala como si fuera un asistente más. El buzón de sala usa su calendario para ver si está disponible para esa hora y acepta o rechaza automáticamente la solicitud.
- **Atributos Especiales:** Tiene atributos específicos que no son normales en usuarios:
    - **Capacidad** (*Capacity*): Para indicar cuántas personas caben. Esto se usa como un **filtro**; si metes a 20 personas y la capacidad es de 13, la sala no aparecerá en la lista de salas disponibles.
    - **Delegados:** Personas que pueden ser responsables de **autorizar o no las reservas**. Por defecto, cualquiera puede reservar la sala.
    - **Opciones de Reserva:** Se puede configurar si se permiten reuniones periódicas, la duración máxima de la reserva (ej. 2 horas), si acepta automáticamente las solicitudes o si tiene que preguntar al delegado.

2. Buzón de Equipamiento (*Equipment Mailbox*)

- **Propósito:** Se utiliza para reservar recursos físicos móviles o equipos. Ejemplos incluyen un proyector, un portátil auxiliar, un módem 4G. (Incluso se ha usado para recursos más atípicos como una excavadora).
- **Uso:** Al igual que con las salas, el objetivo es **verificar la disponibilidad** a través del calendario y reservarlo.
- **Administración:** Se configura de manera similar a una sala.

3. Administración Común y Avanzada

La administración de las configuraciones de reserva para ambos (como quién puede reservar, si se acepta automáticamente o no, o si hay restricciones de duración) se suele realizar mediante comandos avanzados de **PowerShell**.

Tanto las salas como el equipamiento se muestran en el **asistente para programación** al convocar una reunión.

\newpage

Capítulo 10: El Soporte Técnico en Microsoft 365 se gestiona principalmente a través del **panel de administración vía web**.

1. Ubicación y Función

- **Acceso:** El soporte técnico se encuentra dentro del centro de administración en una sección llamada **Soporte Técnico**.
- **Propósito:** Este es el lugar donde los administradores dan de alta nuevas **solicitudes de servicio** o **incidencias** a Microsoft. También permite ver el **estado** de esas solicitudes.

2. Proceso de Apertura de una Incidencia

Cuando un administrador inicia una nueva solicitud de servicio, sigue varios pasos:

- **Identificación del Problema:** Se describe el problema (ej. "Falta el calendario de equipo").
- **Autoayuda:** El sistema ofrece una serie de **soluciones de autoayuda**. Si estas soluciones no funcionan, el administrador puede proceder a abrir una incidencia.
- **Método de Contacto:** El administrador elige el método de contacto y la zona horaria. Aunque históricamente el soporte era problemático (llamadas inoportunas desde Sudamérica), ha mejorado con el tiempo, y ahora se puede especificar el momento en que se desea recibir la llamada.
- **Niveles de Soporte:** Microsoft tiene varios niveles de soporte (Nivel 2, Nivel 3), e incluso es posible llegar a hablar con personal en Redmond.

3. Roles y Permisos

- **Control de Acceso:** La apertura de incidencias es un rol; no tienes por qué permitir a todo el mundo abrir incidencias. Es decir, no todos los usuarios tienen permitido dar de alta solicitudes de servicio.

4. Relación con el Centro de Mensajes

El Soporte Técnico también está relacionado con el **Centro de Mensajes**. El Centro de Mensajes informa al administrador sobre cuándo llegarán los cambios y sobre el **estado del servicio**.

- **Estado del Servicio:** En caso de degradación o problemas en Office 365, el administrador puede consultar el **estado del servicio**. Si una incidencia que no ha sido resuelta (**incidencia viva**) está afectando al entorno, el administrador puede marcar "Estoy afectado por esto" para ayudar a Microsoft a resolverlo más rápidamente.

\newpage

Capítulo 11: Los **Usuarios Activos** (Active Users) en la consola de administración de Office 365 representan a las identidades que pueden iniciar sesión en el

entorno. Esta lista es equivalente a los objetos de usuario en Azure AD (Azure Active Directory), que funciona como el gestor de identidades y autenticación para todos los servicios de Microsoft 365.

Aquí tienes un desglose de las principales acciones que se pueden realizar con los usuarios activos:

1. Gestión de Identidad y Licenciamiento

Las acciones sobre usuarios activos están intrínsecamente ligadas a las licencias, ya que una cuenta de usuario sin licencia no tiene ninguna funcionalidad asociada.

- **Asignación de Licencias:** Un usuario solo comienza a generar costos una vez que se le asigna una licencia. La asignación de una licencia es lo que activa funcionalidades como el buzón de Exchange, el acceso a Teams y el acceso a SharePoint.
- **Gestión de Sublicencias:** Es posible activar o desactivar funcionalidades específicas (sublicencias) dentro de un paquete de licencias asignado. Esto permite, por ejemplo, introducir herramientas progresivamente (como Teams o SharePoint) para evitar la sobrecarga del usuario, aunque OneDrive, por ejemplo, forma parte de SharePoint y no se puede desactivar por separado.
- **Configuración del UPN (User Principal Name):** Se puede modificar el nombre principal de usuario (UPN), que es el nombre de inicio de sesión del usuario. Este suele coincidir con la dirección de correo electrónico principal. Si se han agregado múltiples dominios a la organización, se puede seleccionar cuál usar como UPN.
- **Alias de Correo Electrónico:** Se pueden configurar y modificar alias de correo (direcciones SMTP). Es importante notar que, tradicionalmente, solo se puede enviar correo desde la dirección principal, aunque se ha anunciado un cambio inminente para permitir el envío desde cualquiera de los alias. (Nota: Obtener un listado de todos los alias sin el uso de PowerShell no es posible a través de la interfaz web).

2. Acciones de Correo Electrónico (Vía Panel General o Exchange)

Aunque la gestión avanzada del correo se realiza en el Centro de Administración de Exchange, el panel de Usuarios Activos ofrece atajos a las tareas más comunes.

- **Tríada de Permisos:** Se gestionan tres permisos clave sobre el buzón:
  - **Acceso Completo (Full Access):** Permite a otro usuario abrir y administrar el buzón, incluyendo la lectura y modificación de correos.
  - **Enviar Como (Send As):** Permite a otro usuario enviar correos haciéndose pasar por el buzón, lo que es útil, por ejemplo, para asistentes que gestionan el correo de un directivo.
  - **Enviar en Nombre de (Send on Behalf of):** Permite enviar correos, pero dejando claro que el correo ha sido enviado por un delegado en nombre del buzón original.
- **Reenvío de Correo:** Se puede configurar el reenvío automático a otra dirección de correo electrónico. Esta acción es considerada peligrosa y es un método común en ataques de compromiso de correo, por lo que existen alertas para detectarla.

- **Respuestas Automáticas:** Se pueden configurar mensajes de "Fuera de la oficina", con la opción de establecer respuestas distintas para usuarios internos y externos.
- **Ocultar de la GAL (Global Address List):** Se puede ocultar al usuario de la Lista Global de Direcciones (GAL).
- **Conversión de Buzones:** Un buzón de usuario (con licencia) puede convertirse en un buzón compartido (Shared Mailbox), lo que permite que varios usuarios lo administren y, crucialmente, deja de consumir una licencia.

3. Seguridad y Control

- **Suspensión por Litigio (Litigation Hold):** Si el licenciamiento lo permite (generalmente se requiere una licencia avanzada), se puede activar la suspensión por litigio. Esto garantiza que todos los cambios realizados en el buzón (incluidas las eliminaciones) queden registrados y que la información nunca se elimine, sirviendo como una forma de retención legal y evitando la eliminación permanente de correos después del periodo de retención normal.
- **Cerrar Sesiones:** Se puede forzar el cierre de todas las sesiones de Office 365 abiertas por el usuario. Esto es una medida importante en caso de que se detecte una brecha de seguridad para bloquear el acceso incluso después de que se haya cambiado la contraseña.

4. Gestión Avanzada y Masiva

- **PowerShell:** Para tareas masivas o complejas, se utiliza PowerShell (a través de módulos como Exchange Online o Azure AD). Por ejemplo, se puede crear, modificar y asignar licencias a múltiples usuarios a la vez mediante la importación de archivos CSV e iteración con bucles (`for each`).
- **Roles de Administración:** Se puede asignar roles de administración específicos y granulares al usuario, como el rol de Administrador de Facturación o roles con permisos muy acotados.

\newpage

Capítulo 12: El contenido relacionado con la administración detallada de Exchange se encuentra principalmente dentro del **Centro de Administración de Exchange (CAE)**. Sin embargo, muchas de las tareas más comunes o básicas pueden realizarse también a través del panel principal de **Usuarios Activos**.

A continuación, se describen las principales áreas de administración de Exchange Online:

1. Destinatarios (Recipients)

Los destinatarios son los elementos que Exchange Online utiliza para enviar o recibir correo. La gestión en el CAE es más detallada que en el panel de administración general de Office 365.

Tipo de Destinatario	Descripción y Acciones
Cuentas de Usuario (Buzones)	Son usuarios con licencia de Exchange Online, lo que les asigna un buzón. El tamaño predeterminado del buzón es de 50 GB, pero esto debe consultarse en las Descripciones del Servicio.
Buzones Compartidos (Shared Mailboxes)	Funcionan como listas de distribución, pero tienen un buzón separado. **No consumen licencia**. Al crearlos, se otorgan automáticamente permisos de **Acceso Completo** y **Enviar en Nombre de (Send on Behalf of)** a los miembros asignados. Un buzón de usuario (con licencia) puede convertirse en compartido cuando alguien se va de la empresa, manteniendo el historial de correo y liberando la licencia.
Listas de Distribución	El tipo de grupo más sencillo, sin repositorio de información (no es un buzón). El correo enviado se multiplica a todos los miembros de la lista. Se puede configurar si son accesibles desde fuera de la organización (por defecto no lo son) y si requieren aprobación (moderación) para recibir correos.
Grupos de Office 365	Grupos especiales que crean un buzón compartido y un calendario compartido de Exchange, además de un repositorio de SharePoint.
Contactos	Son entradas que aparecen en la Lista Global de Direcciones (GAL) para personas o entidades externas, permitiendo enviarles correo fácilmente. No pueden iniciar sesión en el entorno. Se pueden agregar de forma manual o masiva mediante PowerShell.
Buzones de Recursos	Son buzones que **no ocupan licencia** y se utilizan para salas de reuniones (salas) o equipamiento (excavadoras, coches, etc.). Tienen atributos especiales como capacidad (en el caso de salas) o un delegado responsable de autorizar o rechazar reservas.

1.1 Gestión de Buzones (Detalle)

Dentro del CAE se pueden configurar varios aspectos de los buzones:

- **Direcciones de Correo Electrónico (Alias):** Se pueden añadir alias SMTP (los más comunes) y otros tipos (como X500, ZIP). La dirección de respuesta (primaria) es la que aparece en negrita y mayúsculas. Los alias permiten recibir correo, pero el envío solo se realiza desde la dirección primaria, aunque se ha anunciado que esta limitación cambiará.
- **Permisos (Tríada):** Se gestionan permisos clave que tardan un tiempo en aplicarse (alrededor de una hora o más):
    - **Acceso Completo (Full Access):** Permite a otro usuario abrir y leer el buzón, incluyendo la eliminación de correos.
    - **Enviar Como (Send As):** Permite al usuario delegado enviar correos como si fuera el buzón principal.
    - **Enviar en Nombre de (Send on Behalf of):** Deja claro que el correo fue enviado por un delegado.
- **Reenvío de Correo (Mail Forwarding):** Permite reenviar automáticamente el correo a una dirección interna o externa. Se considera una acción **peligrosa** y es un método común en ataques de compromiso de correo, por lo que existen alertas para detectarla.

- **Cuotas y Límites:** Se pueden configurar límites de tamaño para el buzón (por defecto 50 GB) y establecer un tamaño máximo de mensajes enviados y recibidos (globalmente o individualmente).

2. Flujo de Correo (Mail Flow)

El Flujo de Correo gestiona el camino que sigue el correo al entrar y salir de la organización.

2.1 Reglas de Transporte (Rules)

Las reglas de transporte transforman o actúan sobre el correo mientras está en tránsito, y pueden aplicarse tanto al correo entrante y saliente como al interno.

- **Condiciones:** Se puede aplicar una regla si el remitente es interno o externo, si pertenece a un grupo, o si cumple patrones de texto específicos.
- **Acciones (Efectos):** Las acciones pueden ser redirigir, bloquear, reenviar el mensaje, o adjuntar un texto de renuncia de responsabilidad (disclaimer).
- **Orden de Reglas:** Las reglas se aplican en orden (de arriba abajo), por lo que el orden es crucial. Se puede detener el procesamiento de más reglas con una opción específica.
- **Prueba:** Se pueden probar las reglas en modo de sugerencia de directiva (Policy Tip) para ver qué correos se verían afectados antes de forzar su cumplimiento.

2.2 Seguimiento de Mensajes (Message Trace)

Es la herramienta principal para saber qué pasó con un correo. Permite buscar mensajes por remitente, destinatario, estado de entrega, y más.

- **Limitación de Búsqueda:** Los registros se guardan hasta un máximo de **90 días**. Si se busca más allá, solo está disponible un archivo CSV.
- **Alcance:** Permite ver el camino que sigue el correo dentro de la infraestructura de Office 365, pero no da visibilidad de lo que ocurre una vez que el mensaje se entrega a un sistema de correo de terceros.

2.3 Conectores (Connectors)

Los conectores definen cómo se recibe o se envía el correo en casos particulares, generalmente con servidores internos.

- **Conectores de Recepción (Inbound):** Se usan para aceptar el tráfico de correo de sistemas internos (como servidores de aplicaciones o impresoras multifunción) sin que sean tratados como spam. Esto se suele configurar especificando la IP de origen.
- **Conectores de Envío (Outbound):** Se usan para alterar el flujo de salida, por ejemplo, enviando el correo a través de un dispositivo de seguridad perimetral (appliance/Barracuda) en lugar de la vía pública.

2.4 Dominios Aceptados (Accepted Domains)

Define qué dominios son responsabilidad de este Exchange.

- **Autoritativo:** El dominio es únicamente responsabilidad de este Exchange. Si un destinatario no existe, el correo se rechaza.

- **Retransmisión Interna (Non-Authoritative/Relay):** El Exchange intentará buscar al destinatario internamente; si no lo encuentra, lo enviará al registro MX del dominio (buscando al destinatario en otro sistema de correo externo). Esto se usa durante la coexistencia o migración de entornos.

3. Seguridad del Correo (Vía Centro de Seguridad)

Aunque muchas configuraciones de seguridad estaban históricamente en el CAE, las políticas modernas se gestionan en el Centro de Administración de Seguridad y Cumplimiento.

- **Políticas de Antispam y Antimalware:** Permiten configurar filtros para correo no deseado (spam), correo masivo (bulk) y archivos maliciosos. Es posible bloquear adjuntos por extensión (ej. .ISO, .LNK, .CMD), aunque puede ser un riesgo si la organización necesita esos archivos.
- **Cuarentena (Quarantine):** Permite a los administradores revisar correos marcados como spam o phishing. Las **Políticas de Cuarentena** (introducidas recientemente) permiten configurar si los usuarios pueden acceder a su cuarentena y si pueden **liberar** correos o solo **solicitar** la liberación (lo cual es útil para usuarios menos técnicos).
- **Protección de la Identidad del Emisor (SPF, DKIM, DMARC):** Estas tecnologías se configuran en el DNS para evitar la suplantación de identidad. **DMARC** le indica al servidor receptor cómo debe tratar el correo que falle los chequeos de SPF/DKIM (ej. eliminarlo o ponerlo en cuarentena) y puede solicitar un informe de la actividad de correo que se recibe en nombre de nuestro dominio.

4. Retención de Correo (Legal Hold / Archivo)

- **Retención por Litigio (Litigation Hold):** Requiere una licencia avanzada (generalmente E3 o superior). Garantiza que el contenido del buzón, incluyendo los correos eliminados por el usuario, se mantenga permanentemente o por un periodo definido.
- **Buzón de Archivado (Archive Mailbox):** Proporciona un buzón adicional de 100 GB para el almacenamiento histórico. El buzón de archivado no utiliza el archivo de caché local (OST), lo cual es una ventaja. Si la persona se va, su buzón de archivado se mantiene, y se puede exportar a un PST o convertir a buzón compartido.

\newpage

Capítulo 13: # Flujo de Correo en Exchange Online

El flujo de correo gestiona el camino que sigue un mensaje al entrar, salir o moverse dentro de la organización. La administración avanzada del correo electrónico, incluyendo la configuración del flujo de correo, se realiza en el **Centro de Administración de Exchange (CAE)**.

Aquí te detallo la información clave sobre la administración del flujo de correo basada en las fuentes:

1. Seguimiento de Mensajes (Message Trace)

El seguimiento de mensajes es la herramienta principal para diagnosticar qué ocurrió con un correo.

- **Propósito:** Permite buscar mensajes por remitente, destinatario, estado de entrega, y más. Es útil cuando un usuario indica que un correo no le ha llegado o que hubo un fallo en el envío.
- **Alcance del Reporte:** Los registros se guardan por un máximo de **90 días**. Si se busca más allá de 90 días, solo se dispone de un archivo CSV.

- **Visibilidad:** Esta herramienta muestra el camino que siguió el correo dentro de la infraestructura de Office 365, pero no ofrece visibilidad sobre lo que ocurre una vez que el mensaje es entregado al sistema de correo de terceros.
- **Ejecución:** Se pueden usar consultas predefinidas o crear búsquedas concretas, especificando el remitente (sender) o el destinatario (recipient). Para informes detallados o búsquedas amplias (como un `extended report`), la preparación del informe puede tardar una hora o más, y se notifica al usuario que lo solicitó.

2. Reglas de Transporte (Transport Rules)

Las reglas de transporte son mecanismos que transforman o actúan sobre un correo mientras está en tránsito, aplicándose a mensajes entrantes, salientes e internos.

- **Propósito:** Se utilizan para automatizar acciones, como reenviar mensajes, redirigirlos, bloquearlos, agregar textos de renuncia de responsabilidad (*disclaimers*) o gestionar barreras internas (como prevenir la comunicación entre ciertos departamentos).
- **Configuración:** Al crear una regla, se especifican:
  - **Condiciones:** Qué debe cumplirse para que la regla se aplique (ej. si el remitente es externo, si el destinatario pertenece a un grupo, si contiene un patrón de texto específico, o si el tamaño es excedido).
  - **Acciones (Efectos):** Qué hará la regla si se cumplen las condiciones (ej. redirigir, bloquear, adjuntar un *disclaimer* en HTML, o notificar al destinatario).
- **Orden y Flujo:** Las reglas se aplican en orden (de arriba abajo), y el orden es crucial. Es posible detener el procesamiento de más reglas mediante una opción específica al final de la regla, lo que evita que se apliquen reglas subsiguientes (ej. si una excepción debe aplicarse antes de un *disclaimer* general).
- **Pruebas:** Antes de aplicar una regla de forma activa (exigirla), se recomienda ponerla en modo de **prueba** (*test mode*). El modo "Probar con sugerencia de directiva" (*Policy Tip*) muestra un mensaje al usuario antes de enviar un correo indicando que la regla se aplicaría.
- **Activación Programada:** Las reglas se pueden programar para que comiencen o finalicen automáticamente en una fecha determinada (ej. para un periodo navideño o un cambio de dominio).
- **Riesgos:** Un uso incorrecto o una regla mal configurada puede generar problemas, y debido a que la activación o desactivación de estas reglas no es inmediata, puede haber un periodo de tiempo con errores.

3. Dominios Aceptados (Accepted Domains)

Define qué dominios de correo son responsabilidad de este Exchange Online.

- **Tipos de Dominio Aceptado:**
  - **Autoritativo (Authoritative):** Es la opción por defecto. Exchange Online es el único responsable de gestionar el correo para ese dominio. Si un destinatario en ese dominio no existe, el correo se rechaza.
  - **Retransmisión Interna (Non-Authoritative/Relay):** Se utiliza en escenarios de coexistencia o migración. Exchange intentará buscar el destinatario internamente. Si no lo encuentra, lo enviará al registro MX del dominio, buscando al destinatario en otro sistema de correo (ej. un servidor de correo local o un hosting externo).

4. Conectores (Connectors)

Los conectores permiten gestionar el flujo de correo en casos particulares, definiendo cómo se recibe o se envía el correo a sistemas internos o externos específicos.

- **Conectores de Recepción (Inbound):** Definen cómo se acepta el tráfico de correo proveniente de sistemas internos (servidores de aplicaciones, impresoras multifunción) para que no sean tratados como spam o como tráfico externo. Se configuran generalmente especificando la **IP de origen** de la red local, lo que permite que el sistema envíe correo a través de Office 365 sin necesidad de autenticación.
- **Conectores de Envío (Outbound):** Se usan para dirigir el tráfico de salida a través de una ruta específica, alterando el flujo normal de salida (ej. enviando el correo a través de un dispositivo de seguridad perimetral externo como Barracuda, o a una IP específica en lugar de la ruta pública).
- **Relay de Correo:** La opción de usar un conector de entrada (Opción 3) permite que sistemas internos realicen *relay* (envío de correo a terceros) a través de Office 365 sin necesidad de que la dirección de origen tenga un buzón asignado (ej. `notificaciones@dominio.com`), aunque sí debe ser un dominio aceptado.

5. Configuración General de Flujo

Se pueden configurar opciones globales en el CAE que afectan a todo el tráfico de correo de la organización:

- **Tamaño Máximo de Mensajes:** Se puede configurar el tamaño máximo de los mensajes enviados y recibidos, aunque el límite máximo soportado por la plataforma (alrededor de 128 MB) se encuentra en las descripciones del servicio. Por higiene y para evitar un mal uso, se suele establecer un límite inferior (ej. 32 MB).
- **SMTP Autenticado:** A nivel global, se puede desactivar el protocolo SMTP AUTH para todos los usuarios. Los *tenants* nuevos suelen tenerlo desactivado por defecto, ya que es un método de autenticación considerado vulnerable.
- **Envío desde Alias:** Hay una opción para activar el envío de correo desde cualquiera de los alias de una cuenta, no solo desde la dirección principal, aunque esta es una funcionalidad inminente o muy reciente.

\newpage

Capítulo 14: # Flujo de Correo en Exchange Online##

1. Propósito y Funcionalidad

Las reglas de transporte permiten automatizar acciones y aplicar políticas a los mensajes de correo electrónico en función de condiciones específicas.

- **Alcance:** Originalmente, solo se podían utilizar para el correo que entraba o salía de la organización, pero desde Exchange 2007 (o Exchange 2010), también sirven para el correo interno.
- **Usos Comunes:**
    - **Automación y Transformación:** Se usan para automatizar acciones como reenviar mensajes, redirigirlos, bloquearlos, o agregar textos de renuncia de responsabilidad (*disclaimers*) en la parte inferior.
    - **Seguridad:** Pueden utilizarse para crear "barreras" o compartimentos internos, por ejemplo, impidiendo la comunicación entre ciertos departamentos (Asuntos Internos y empleados) o

alertando sobre información confidencial.
    - **Moderación:** Se puede configurar que los mensajes pasen a un moderador para su aprobación antes de ser enviados.

2. Configuración y Condiciones

Al crear una regla, se especifican condiciones y acciones:

- **Condiciones:** Determinan qué debe cumplirse para que la regla se aplique. Esto incluye:
    - Si el remitente es interno o externo.
    - Si pertenece a un grupo.
    - Si contiene un patrón de texto específico.
    - Si está en una lista de supervisión.
    - El tamaño del adjunto.
    - El remitente o destinatario de la persona.
    - Patrones de texto en el destinatario.
- **Acciones (Efectos):** Lo que ocurrirá si se cumplen las condiciones:
    - Reenviar, redirigir, o bloquear el mensaje.
    - Poner a alguien en copia.
    - Adjuntar un texto de renuncia de responsabilidad (*disclaimer*), el cual puede ser en formato HTML.
    - Cambiar la seguridad del mensaje.
    - Notificar al destinatario (ej. "Gracias por su correo, se le responderá en breve").
- **Excepciones:** Se pueden añadir excepciones para que la regla sea lo más acotada posible y no se aplique a ciertos mensajes, incluso si cumplen las condiciones.
- **Dirección del Remitente:** Es importante notar que, según la arquitectura SMTP, la dirección del remitente puede venir en dos sitios: el **encabezado** y el **sobre**. Las reglas permiten hacer referencia a la dirección del encabezado, del sobre, o de ambas.

3. Orden y Riesgos de Aplicación

El orden en el que se aplican las reglas es fundamental.

- **Procesamiento Secuencial:** Las reglas se aplican en orden (de arriba abajo), y el orden puede subirse y bajarse.
- **Detener Procesamiento:** Es posible detener el procesamiento de más reglas mediante una opción específica al final de la regla. Si no se usa esta opción, se ejecutarán la Regla 1, la Regla 2, la Regla 3, y así sucesivamente.
- **Riesgo por Retraso:** Las reglas de transporte no se activan de forma inmediata. Si se comete un error al configurarlas, tardan un rato en activarse y, si hay que desactivarlas, también tardan un rato, lo que puede causar problemas.

4. Pruebas y Auditoría

Antes de forzar el cumplimiento de una regla, existen modos de prueba para mitigar los riesgos:

- **Modo Activo (Exigir):** La regla está funcionando y se aplica.
- **Probar con Sugerencia de Directiva (*Policy Tip*):** La regla no se aplica, pero si el usuario va a enviar un correo que cumpla la condición, le sale un mensaje antes de enviarlo, avisando que la regla se aplicaría.
- **Probar sin Sugerencia de Directiva:** La regla no se aplica, pero luego se puede sacar un informe para ver qué correos habrían sido afectados.

Auditoría: Se puede auditar la regla con un nivel de gravedad (Alto, Medio, Bajo). Esto permite sacar un informe posterior para ver qué reglas de seguridad se han activado.

5. Configuración Adicional

- **Activación Programada:** Las reglas se pueden configurar para que comiencen o finalicen automáticamente en una fecha determinada.
- **Comentarios:** Es posible agregar un comentario a la regla, por ejemplo, especificando quién ordenó su creación y cuándo (ej. "regla creada el 7 del 6 por orden de Alfredo").

\newpage

Capítulo 15: # Dominios Remotos y Dominios Aceptados en Exchange Online

Dominios Aceptados (Accepted Domains)

Un Dominio Aceptado define qué dominios de correo electrónico son responsabilidad del entorno de Exchange Online.

1. Propósito Principal

El propósito es declarar a Exchange como un responsable potencial de gestionar los buzones o las direcciones de correo para ese dominio. La configuración de estos dominios se realiza en el panel de administración general de Office 365, donde se deben añadir y verificar (por ejemplo, mediante un registro TXT en el DNS público). Una vez verificado, aparece en la configuración de Dominios Aceptados.

2. Tipos de Dominios Aceptados

Un dominio aceptado puede configurarse de dos maneras, lo que determina cómo Exchange maneja el correo dirigido a ese dominio:

- **Autoritativo (Authoritative)**:
    - **Función:** Esta es la opción por defecto.
    - **Comportamiento:** Exchange Online es el **único responsable** de gestionar el correo para ese dominio. Si un mensaje llega a Exchange y el destinatario de ese dominio no existe dentro de la organización de Office 365, el correo **se rechaza**.
- **Retransmisión Interna (Non-Authoritative/Relay)**:
    - **Función:** Se utiliza comúnmente en escenarios de **coexistencia o migración**.

- **Comportamiento:** Exchange intenta encontrar el destinatario internamente (en el buzón de Office 365). Si el destinatario no se encuentra, Exchange **no rechaza** el mensaje, sino que lo envía al registro MX del dominio. De esta manera, el correo es redirigido a **otro sistema de correo externo o local** donde el buzón del destinatario pueda existir.

3. Dominios Remotos (Remote Domains)

Los Dominios Remotos no definen qué dominios acepta Exchange, sino que definen la configuración que Exchange aplicará a los **mensajes salientes** (o, en ciertas configuraciones, a los mensajes entrantes) cuando interactúa con sistemas de correo externos.

1. Propósito Principal

Se utilizan para configurar el flujo de correo entre Exchange Online y un dominio externo, definiendo cómo deben tratarse los mensajes, especialmente en cuanto a la compartición de información y el formato.

2. Funcionalidades y Configuración Comunes

Aunque se encuentran en el Centro de Administración de Exchange (CAE), las configuraciones más importantes de Dominios Remotos están relacionadas con la funcionalidad de calendario y el formato del mensaje:

- **Uso Compartido Federado (Calendario):** En la configuración de uso compartido y organización, se puede **federar** dominios externos para que los usuarios puedan ver la información de disponibilidad de calendario de usuarios en otras organizaciones. Esto es útil si se trabaja frecuentemente con socios o empresas del mismo grupo.
- **Restricciones de Correo:** Históricamente, se usaba para configurar el formato del correo (por ejemplo, forzar el uso de texto enriquecido o formato de texto sin formato) para destinatarios en ese dominio. Sin embargo, en la actualidad, estas opciones predeterminadas suelen ser funcionales y no necesitan cambiarse.

\newpage

Capítulo 16: ### Conectores (*Connectors*) en el Flujo de Correo

Los conectores definen las rutas específicas para cómo el correo se recibe o se envía, especialmente cuando involucra servidores internos o dispositivos perimetrales.

Propósito: La idea de un conector es indicarle a Exchange Online cómo debe realizar el envío o la recepción del correo en **casos particulares**.

1. Conectores de Recepción (Inbound Connectors)

Estos conectores definen cómo Exchange Online debe aceptar el tráfico de correo proveniente de **sistemas internos** (servidores de aplicaciones, impresoras multifunción, etc.) para que no sea tratado como *spam* o como tráfico externo.

- **Uso Principal:** Se utilizan cuando se tienen sistemas en la red interna que también envían correo, como un servidor con una aplicación que envía albaranes.
- **Aceptación de Tráfico:** Se pueden configurar para aceptar el tráfico de correo de sistemas internos.
- **Configuración por IP:** Para que Exchange confíe en el sistema interno, se puede configurar el conector especificando la **dirección IP** de salida de la red local (la IP de origen).
- **Ventajas (Opción 3 del artículo mítico):** Esta es la mejor opción para que las aplicaciones internas envíen correo a través de Office 365.
    - Utiliza el **puerto 25** estándar, lo que facilita la configuración.
    - **No requiere autenticación** (ya que se confía implícitamente en la IP de origen especificada), lo que es más fácil de configurar en dispositivos como impresoras o cacharros.
    - Permite hacer **relay** (reenvío): El sistema aceptará cualquier correo, aunque la dirección de origen (ej. `notificaciones@dominio.com`) no tenga un buzón asignado, siempre que sea de un dominio aceptado por la organización.
    - El correo que ingresa por este conector es tratado como una **conexión interna** y está sujeto a menos restricciones de antispam que si pasara por la puerta pública.

2. Conectores de Envío (Outbound Connectors)

Estos conectores definen cómo se debe enviar el correo desde Exchange Online hacia el exterior en casos específicos, **alterando el flujo normal de salida**.

- **Uso Principal:** Se usan para dirigir el tráfico saliente a través de una ruta específica o un dispositivo perimetral.
- **Alteración del Flujo:** En lugar de enviarlo por el camino público, se le puede indicar que lo envíe a través de una **IP específica** de un servidor de correo (ejemplo de una empresa de automoción que enviaba a un servidor específico de Volkswagen para encargos de piezas).
- **Seguridad:** También se usan cuando se tienen dispositivos de seguridad perimetral externos (como un Barracuda), para que el correo saliente pase primero por ese dispositivo antes de ser entregado al mundo.

3. Diferencia con Reglas de Transporte

Un conector de recepción abre una **segunda puerta** que acepta conexiones desde una IP local y está sujeta a **menos restricciones de antispam**, tratándose como una conexión interna. Esto permite hacer *relay*, cosa que no se puede lograr solo con una regla de transporte.

En resumen: Los conectores permiten configurar escenarios complejos, como que una aplicación interna sin buzón pueda enviar correos de manera segura (*relay* usando la Opción 3) o que todo el correo saliente pase por un dispositivo de seguridad perimetral.

\newpage

Capítulo 17: # Uso Compartido en Exchange Online

Ubicación y Alcance

La configuración de "Uso Compartido" (uso compartido de Exchange) se encuentra dentro de la sección de **Organización** del Centro de Administración de Exchange Online.

Es fundamental notar que, al hablar de "uso compartido" en este contexto, **no se refiere al correo electrónico**, sino exclusivamente a la funcionalidad del **calendario**.

1. Uso Compartido Federado (Compartición a Nivel de Organización)

El concepto principal en esta sección es el **uso compartido federado** (o uso compartido de Exchange).

Esta funcionalidad permite a su organización:

1. **Intercambiar información de calendario:** Permite que su empresa pueda ver la disponibilidad de otros usuarios que se encuentran en organizaciones externas, siempre y cuando estas estén configuradas para la federación.
2. **Escenarios de aplicación:** Esto es útil cuando su empresa necesita coordinarse con un socio, o si forman parte de un grupo de empresas y necesitan ver la disponibilidad de otros usuarios que están en otra de las empresas del grupo.
3. **Ambientes Híbridos:** También se utiliza en entornos de Exchange híbridos, donde parte de la infraestructura de correo está localmente (on-premise) y parte está en Exchange Online.

Configuración de la Federación

Para habilitar esta funcionalidad, se pueden agregar otras organizaciones con las que se desea federar (intercambiar información de disponibilidad).

Aunque a menudo es un proceso que requiere cierta complejidad técnica, en algunos casos se llega a configurar incluso mediante **PowerShell**. La política por defecto, sin embargo, ya permite a todos los usuarios compartir su calendario con gente externa.

2. Distinción de la Compartición Individual

Es importante diferenciar la configuración a nivel de organización de las opciones de uso compartido a nivel de usuario:

Tipo de Compartición	Nivel de Aplicación	Control	Datos Compartidos por Defecto
Uso Compartido Federado	Colectivo (Toda la organización)	Se gestiona desde el panel de administración de Exchange.	La **disponibilidad** (si están ocupados o no).
Uso Compartido Individual	Individual (Cada usuario)	Se gestiona directamente por el usuario desde Outlook o Outlook Web Access (OWA).	La **disponibilidad** (si están ocupados o no).

Por defecto, todos los usuarios de Exchange ya tienen habilitada la posibilidad de compartir su calendario con todos los demás. Lo que comparten es solo el estado de ocupado o no, aunque esta configuración se puede cambiar para incluir más detalles. Esta compartición individual la gestiona el propio usuario y se realiza desde el calendario en Outlook o OWA.

\newpage

Capítulo 18: # Resumen Moderno de SharePoint en Microsoft 365

I. El Rol Central de SharePoint en Microsoft 365

SharePoint Online es una de las **tres principales cargas de trabajo** o herramientas troncales de Office 365, junto con Exchange Online (correo) y Teams.

Su función principal es servir como **repositorio para archivos, documentación y comunicación**.

Relación con OneDrive y Teams:

1. **OneDrive:** A pesar de tener su propia interfaz, OneDrive se apoya completamente en SharePoint. De hecho, al ir a la URL de OneDrive, en realidad se está accediendo a SharePoint.
2. **Teams:** Teams actúa como una capa adicional que se construye sobre SharePoint. La colaboración en Teams utiliza un sitio de SharePoint por debajo para almacenar sus archivos. Es crucial entender que la información de Teams no se *sincroniza* con SharePoint; **es la misma información** vista desde una interfaz diferente.

II. La Naturaleza Fundamental de SharePoint

Históricamente, SharePoint (que data de 2003) nació para resolver las **limitaciones de las carpetas compartidas** tradicionales, donde el acceso al archivo quedaba bloqueado para otros usuarios si alguien estaba trabajando en él.

El concepto fundamental de SharePoint, aunque pueda parecer centrado en archivos, es que **todo son listas**. SharePoint es, en realidad, un conjunto de tablas de una base de datos SQL. Incluso los archivos que usted sube son tratados como elementos dentro de una lista.

III. La Evolución Arquitectónica: SharePoint Clásico vs. Moderno

Para entender la administración actual, debemos diferenciar los dos modelos que coexisten, aunque Microsoft promueve fuertemente el más reciente:

1. Modelo Clásico (Arquitectura Jerárquica)

Este modelo, anterior aproximadamente a 2015, se utilizaba para construir grandes **intranets corporativas**.

- **Estructura:** Estaba basado en una **jerarquía estricta** de sitios y subsitios, muy similar a la estructura de carpetas de un servidor de archivos.
- **Permisos:** Heredaban permisos (la herencia era un problema) y los permisos eran muy detallados y granulares (editor, revisor, etc.).
- **Diseño:** Los proyectos de implantación eran largos y requerían programación avanzada con herramientas como SharePoint Designer y código CSS para la funcionalidad y el aspecto visual.
- **Rigidez:** La estructura definida al inicio no podía cambiarse fácilmente. Mover un sitio o modificar su diseño era muy complicado.

2. Modelo Moderno (Arquitectura Plana y Flexible)

Microsoft desarrolló este modelo debido a que el clásico era demasiado complejo y la gente prefería seguir enviando archivos adjuntos por correo en lugar de colaborar. Este es el modelo que debemos usar:

- **Sitios Independientes:** Los sitios no tienen jerarquía estricta, operan como **islas independientes**.
- **Navegación Lógica (No Jerárquica):** La ilusión de que un sitio "cuelga" de otro (la jerarquía visual) se consigue simplemente **editando los menús de navegación** para vincularlos. Si cambia de opinión, simplemente cambia la URL en el menú.
- **Permisos Simplificados:** La filosofía es **dentro o fuera**. Si un usuario es miembro del sitio, tiene acceso; si no lo es, no lo tiene. Esta simplificación evita los problemas de romper permisos a nivel granular, lo cual causaba errores en el capa de Teams.
- **Tipos de Sitio Modernos:** Solo se recomiendan dos plantillas principales:
    - **Sitio de Colaboración:** Orientado a que todos los miembros editen y modifiquen contenido al mismo nivel. Este es el tipo de sitio que se crea automáticamente al formar un **Grupo de Office 365** o un **Team**.
    - **Sitio de Comunicación:** Orientado a la difusión (*one-to-many*), donde un pequeño grupo de personas edita contenido (noticias, catálogos, enlaces) y el resto de la organización solo lo visualiza. Es ideal para Intranets.

IV. La Doctrina: Colaboración a Través de Teams

La visión de Microsoft, denominada **Modern Workplace**, indica que se debe trabajar a favor de esta doctrina, ya que cualquier configuración que se aparte de ella tiende a volverse obsoleta o problemática.

En la práctica, esto significa que:

1. **Uso de Contenedores:** Se deben evitar las estructuras detalladas de permisos de carpetas (NTFS). Se recomienda crear **contenedores** separados (sitios de SharePoint o Teams) basados en la necesidad de aislamiento de permisos. Si un grupo de usuarios necesita acceso a un conjunto de información, se les da acceso completo al contenedor; si requieren permisos diferentes para otro conjunto, se crea un segundo contenedor.
2. **Teams para el Trabajo Diario:** Aunque SharePoint aloja los archivos, la forma más recomendada para que los usuarios interactúen con esos archivos y colaboren es a través de **Teams**. Esto se debe a que Teams ofrece un entorno más sencillo y unificado, incluyendo chat, planificación y otras aplicaciones, sin exponer la complejidad de la interfaz web de SharePoint.

V. Administración General (Panel de Administración de SharePoint)

Desde el Centro de Administración de SharePoint, el enfoque es principalmente la gestión de alto nivel y las políticas globales:

- **Sitios Activos:** Permite ver y gestionar todos los sitios creados, su uso de almacenamiento (el límite por defecto es 1 TB más 1 GB por usuario).
- **Directivas (Policies):** Aquí se establecen reglas globales para la compartición externa de SharePoint y OneDrive, como limitar la compartición a ciertos dominios o desactivar la compartición anónima para toda la organización.
- **Personalización a Nivel de Sitio:** Aunque las tareas detalladas de personalización se realizan en la propia interfaz de SharePoint (como editar menús o añadir bloques web), las propiedades administrativas (como la cuota de almacenamiento o si un sitio pertenece a un *Hub Site* o centro) se manejan desde el centro de administración.

En resumen, la introducción moderna a SharePoint implica una comprensión profunda de que la simplicidad del sistema de permisos (dentro/fuera) y el uso de Teams como interfaz principal son las claves para una colaboración exitosa y mantenible en Microsoft 365.

\newpage

Capítulo 19: # Arquitectura de Contenedores en Microsoft 365: Una Guía para el Diseño Efectivo

1. La Filosofía del Contenedor Moderno: De la Jerarquía a la Independencia

Históricamente, el SharePoint Clásico (que data de 2003 y versiones posteriores) se basaba en una arquitectura jerárquica de sitios y subsitios, donde los permisos se heredaban de arriba abajo, similar a los permisos NTFS de un servidor de archivos.

En el **modelo moderno** de SharePoint Online, esta estructura jerárquica se elimina. Los contenedores ya no dependen unos de otros, sino que cada sitio se convierte en una **"isla independiente"** que puede gestionar su propio idioma, cuota de espacio, y política de compartición externa.

Esta arquitectura moderna permite mayor flexibilidad y evita la parálisis de diseño que ocurría antes, ya que la estructura se puede cambiar a voluntad sin romper la herencia de permisos.

La clave está en los Sitios Centrales (Hub Sites): Aunque internamente no hay jerarquía, se puede crear una estructura visual (navegación y aspecto) utilizando menús y Sites Centrales. Esto permite que sitios relacionados (como diferentes departamentos) compartan un menú común y un esquema de colores, aunque sigan siendo entidades independientes.

2. Tipos de Contenedores y su Relación

Los contenedores en Microsoft 365 son interdependientes, y una capa se construye sobre otra.

Contenedor Principal	Propósito Primario	Base Subyacente
Microsoft Teams	Colaboración y comunicación diaria (chats, llamadas, apps).	Es una capa sobre un Grupo de M365, que a su vez es un Sitio de Grupo de SharePoint Online.
Grupos de Microsoft 365	Eje de colaboración, proporciona calendario, buzón compartido y repositorio de ficheros.	Sitio de Grupo de SharePoint Online.
Sitios de Grupo (Team Sites)	Colaboración interna, orientado a que todos los miembros modifiquen y editen.	Colección de Sitios (el concepto de sitio moderno).
Sitios de Comunicación	Comunicación "uno para muchos" (intranets, noticias, manuales).	No llevan un Grupo de M365 asociado.

El objeto fundamental para la colaboración es el **Grupo de Office 365**, el cual automáticamente crea un buzón compartido, un calendario, un OneNote y un repositorio de archivos que es, en realidad, un sitio de SharePoint Online. Teams añade una capa de comunicación a este Grupo.

3. Estrategia de Diseño y Permisos (El Criterio de Compartimentación)

El paso más importante al diseñar la estructura de contenedores es redefinir los permisos y hablar con los dueños de la información.

A. Permisos Basados en el Contenedor

Las organizaciones deben abandonar los permisos muy granulares (como "Editor," "Revisor," o permisos NTFS detallados) que existían en el modelo clásico.

En el modelo moderno, la filosofía es simple: **o estás dentro del contenedor, o estás fuera**. Si eres miembro de un Grupo de M365/Team, se espera que tengas control total sobre el contenido.

Esto lleva a una compartimentación de la información basada en la necesidad de aislamiento de permisos. Por ejemplo, lo que antes era una estructura jerárquica de carpetas se transforma en múltiples contenedores (sitios/Teams), y un usuario es miembro solo de los que necesita.

B. Uso de Contenedores según la Finalidad

1. **Contenedores de Colaboración (Teams/Sitios de Grupo):**
    - Se usan para el trabajo diario, proyectos o departamentos, donde la expectativa es que todos los miembros editen y modifiquen.
    - Si se requiere aislar un conjunto de datos dentro de un Team (por ejemplo, información confidencial para una subsección del equipo), Microsoft permite crear **Canales Privados**. Sin embargo, esta práctica crea, de hecho, un sitio de SharePoint completamente distinto y separado para esa información, lo que demuestra la necesidad de aislamiento a nivel de contenedor, no a nivel de carpeta.
2. **Contenedores de Comunicación (Sitios de Comunicación):**
    - Se usan para publicar información de "uno a muchos", como intranets corporativas, noticias o manuales.
    - Estos sitios están pensados para ser personalizados visualmente (mediante plantillas como las del Lookbook de Microsoft) y solo requieren permisos detallados para los editores/propietarios, mientras que la mayoría de los usuarios son "visitantes" (solo lectura).
    - Se puede utilizar la **identificación de audiencias** para segmentar el contenido (menús, noticias, etc.) según los grupos a los que pertenezca el usuario, sin necesidad de crear múltiples sitios.

C. Canales de Teams vs. Carpetas

Dentro de un Team, los canales se reflejan como carpetas en el SharePoint subyacente. Los canales no se usan para compartimentar permisos (salvo el canal privado), sino para organizar temas, documentos y aplicaciones extra (como listas, Planner o pizarras) relacionadas con ese tema, potenciando las capacidades nativas de M365.

4. Gobernanza y Creación de Contenedores

Para evitar la proliferación descontrolada de Teams y Sitios con nombres inadecuados (como "Manoli, Pepi, Antonio y yo"), las organizaciones establecen políticas de gobernanza.

1. **Restricción de Creación:** La práctica recomendada es **limitar quién puede crear un Team o un sitio** para que los usuarios normales no puedan hacerlo a voluntad.
2. **Flujo de Aprobación:** Para solicitar un nuevo Team, se suele implementar un formulario de solicitud que pregunta: quién es el dueño/propietario, el departamento, la finalidad del Team y si se requerirá acceso externo.
3. **Gestión de Propiedad:** Una vez creado el Team por el administrador, se asigna al solicitante como **Propietario del Team**. El propietario se hace responsable de la membresía y gestión interna del Team, liberando al administrador de la carga de añadir o quitar usuarios constantemente.
4. **Nomenclatura y Políticas:** Se pueden aplicar **Directivas de Nombres** (que requieren licencia P1) para asegurar que los Grupos sigan una nomenclatura específica (como prefijos de departamento) y evitar nombres poco serios o confusos.

En resumen, la estrategia moderna se centra en crear un sitio o Team por cada necesidad de aislamiento de permisos o colaboración específica, aprovechando la flexibilidad de la arquitectura plana y las herramientas de gestión (como el Panel de Administración de SharePoint o Intune) para controlar el acceso y la gobernanza.

\newpage

Capítulo 20: ### 1. El Paradigma de la Arquitectura Moderna: De la Jerarquía a la Estructura Plana

Para crear una buena intranet en M365, es fundamental comprender y aplicar el modelo de **SharePoint Moderno**, dejando atrás el modelo clásico basado en sitios y subsitios jerárquicos.

1. **Independencia del Sitio:** En el modelo moderno, se eliminan las jerarquías de herencia de permisos. Cada sitio es una **"isla independiente"**.
2. **Flexibilidad Total:** Esta independencia permite que cada sitio gestione su propio idioma, su cuota de espacio y sus políticas de compartición externa de manera individual. Además, se gana en flexibilidad, ya que si la organización desea reestructurar su navegación o eliminar un área, puede hacerlo sin provocar una parálisis de diseño ni romper la herencia de permisos, lo cual era un problema habitual en el modelo clásico.
3. **Contenedores como Unidades:** La arquitectura se enfoca en que cada necesidad de aislamiento de permisos o colaboración específica se traduzca en un nuevo "contenedor" (un sitio o un Team).

2. Clasificación de Contenedores y Plantillas

La primera decisión estratégica es definir el propósito del contenido que albergará la intranet, ya que esto determina el tipo de sitio a crear:

Tipo de Contenedor	Propósito	Base de Permisos

Tipo de Contenedor	Propósito	Base de Permisos
Sitios de Comunicación	Enfocados en comunicación "uno para muchos" (intranets, noticias, manuales, catálogos).	Diseñados para que un pequeño grupo edite y el resto de la organización solo visualice.
Sitios de Colaboración (Grupos de M365 / Teams)	Orientados al trabajo diario y proyectos, donde todos los miembros esperan editar y modificar el contenido.	Son la base para Microsoft Teams.

Un **Team** es una capa adicional de visualización e interacción que se construye sobre un Grupo de Office 365, y este a su vez es un sitio de SharePoint Online (colaboración).

3. Estrategia de Diseño para una Buena Intranet de Comunicación

La intranet corporativa se construye típicamente sobre Sitios de Comunicación. Aunque la arquitectura interna es plana, la organización necesita crear una estructura visualmente jerárquica para la navegación.

A. Navegación y Estructura Jerárquica Visual

1. **Página de Inicio (Landing Site):** Es fundamental establecer un sitio principal (Home Site o Landing Page) que sea la puerta de entrada para todos los usuarios.
2. **Sitios Centrales (Hub Sites):** Para agrupar visualmente sitios relacionados (por ejemplo, todos los sitios de un departamento), se utiliza la funcionalidad de Sitios Centrales.
    - Un sitio se define como un "Centro" (Hub).
    - Los sitios relacionados se asocian a ese Centro, heredando un **menú común** y un **esquema de colores** compartido.
    - **Importante:** Esta asociación es puramente visual y de navegación, **no** implica herencia de permisos, manteniendo la independencia de cada sitio.

B. Personalización Visual y Contenido Relevante

1. **Branding:** Es altamente recomendable utilizar el *branding* (logotipos, colores corporativos) para que el usuario sepa en qué área de la organización se encuentra. Microsoft ofrece herramientas para generar archivos XML (a menudo subidos vía PowerShell) para definir los temas y colores exactos que luego estarán disponibles en SharePoint.
2. **Utilidad:** La intranet debe ofrecer contenido que sea útil para el usuario (noticias relevantes, enlaces a procesos internos como solicitud de vacaciones, baja parental, etc.), de lo contrario, no será utilizada.
3. **Diseño Modular:** Los sitios de comunicación modernos son responsivos (se adaptan a diferentes dispositivos) y su edición es modular, similar a WordPress, utilizando *Web Parts* y bloques predefinidos (como los ejemplos vistos en el **Lookbook de Microsoft**).

C. Segmentación de Audiencias

Para evitar la creación de múltiples sitios idénticos con pequeñas variaciones, se debe habilitar la **Identificación de Audiencias** (Audience Targeting).

- Esta funcionalidad permite que diferentes elementos del sitio (como noticias, enlaces o menús) se muestren de forma personalizada, dependiendo de si el usuario pertenece o no a un grupo específico de Azure AD.

4. Gestión de la Colaboración y Repositorios

Aunque la intranet de comunicación pueda enlazar a repositorios, la mejor práctica en M365 es consumir los archivos y colaborar de manera indirecta.

1. **Teams como Interfaz Preferida:** Aunque los archivos residen en SharePoint, se recomienda que los usuarios accedan a los documentos colaborativos a través de **Teams**. Teams proporciona un entorno más simplificado para trabajar con ficheros y agrega funcionalidades clave como chat, videollamadas, Planner, y otras aplicaciones, ofreciendo una experiencia de colaboración completa.
2. **Principio de Permisos Simplificado:** En los sitios de colaboración, la filosofía de permisos debe ser simple: **"o estás dentro o estás fuera"**. Se debe evitar la asignación manual de permisos granulares a nivel de carpeta o archivo dentro del sitio de SharePoint subyacente a un Team, ya que esto está desfasado y puede causar problemas en la funcionalidad que presupone Teams.
3. **Gobernanza de la Creación de Contenedores:** Para evitar la proliferación descontrolada de Teams y sitios, las organizaciones suelen:
    - **Limitar la creación:** Restringir qué usuarios pueden crear Teams o Grupos de M365.
    - **Delegar la propiedad:** Utilizar formularios de solicitud para que el administrador cree el Team, pero luego asignarle la responsabilidad de la membresía y gestión interna al solicitante (el **Propietario del Team**).

5. Advertencia Didáctica: Evitar la Sincronización Local

Como experto, debo enfatizar una mala práctica que se debe evitar en un buen diseño de intranet:

- **Evitar la sincronización de archivos de sitios de colaboración (SharePoint/Teams) con el disco duro local (OneDrive):** Aunque existe el botón de "Sincronizar", se desaconseja su uso para archivos departamentales. La sincronización constante de grandes volúmenes de datos departamentales entre múltiples usuarios aumenta drásticamente la probabilidad de errores de sincronización y archivos duplicados o replicados incorrectamente. El método correcto es trabajar directamente en la nube, preferentemente a través de la interfaz de Teams.

\newpage

Capítulo 21: El Sitio de Comunicación, junto con el Sitio de Grupo (que es la base de Teams), constituye el núcleo de la arquitectura moderna de SharePoint.

---

1. Propósito Central y Orientación

El rol principal de un Sitio de Comunicación es la difusión de información, marcando una clara distinción con los sitios de colaboración:

1. **Comunicación Uno para Muchos (One-to-Many):** El Sitio de Comunicación está enfocado en la difusión masiva de información. Su diseño está pensado para que un grupo pequeño de personas administre y edite el contenido, mientras que el resto de la organización lo visualiza o consume.
2. **Uso Principal:** Estos sitios son la base ideal para crear la **intranet corporativa** de una organización, incluyendo la publicación de noticias, manuales, catálogos e información general.
3. **Utilidad:** Para que una intranet basada en Sitios de Comunicación sea exitosa, debe ser útil, proporcionando contenido relevante como noticias de cohesión corporativa o enlaces directos a procesos internos (como solicitudes de vacaciones), garantizando así su adopción por parte de los empleados.

2. Arquitectura y Diferencias Clave

En el modelo moderno de SharePoint, la arquitectura es plana, lo que significa que no existe la jerarquía rígida de sitios y subsitios que caracterizaba al SharePoint clásico.

El Sitio de Comunicación se distingue del Sitio de Colaboración (Team Site) en un aspecto fundamental:

- **Independencia del Grupo de Microsoft 365:** El Sitio de Comunicación **no** lleva asociado un Grupo de Microsoft 365. Esta independencia simplifica su gestión, permitiendo que cada sitio sea una "isla independiente" que puede gestionar su propio idioma, cuota de espacio y políticas de compartición externa.
- **Flexibilidad:** Gracias a esta arquitectura plana, la estructura de la intranet puede modificarse con facilidad (como cambiar enlaces o eliminar sitios), ya que no hay dependencias de herencia de permisos que se rompan.

3. Modelo de Permisos Simplificado

El modelo de permisos de un Sitio de Comunicación refleja su orientación al consumo de información, siendo típicamente más simple que el modelo granular del SharePoint clásico.

Aunque se puede acceder a la configuración de permisos avanzados (que muestra la interfaz antigua del SharePoint clásico), la práctica recomendada es utilizar el modelo simplificado, que clasifica a los usuarios en tres roles:

Rol	Capacidad	Propósito
Propietarios (Owners)	Control total.	Responsables de la administración completa del sitio.
Miembros (Members)	Capacidad de modificar y editar el contenido (control limitado).	El equipo de comunicación o editores del departamento.
Visitantes (Visitors)	Solo visualización (solo lectura).	La audiencia de la intranet (el resto de la organización).

En un Sitio de Comunicación, es totalmente aceptable y, de hecho, el uso previsto, que los visitantes tengan permisos de solo lectura para acceder a archivos y contenido, sin modificar la estructura o los datos del repositorio.

4. Características para Intranets y Personalización

El Sitio de Comunicación está diseñado para ser visualmente atractivo y altamente personalizable:

A. Estructura Visual y Navegación

Aunque la arquitectura subyacente es plana, la organización utiliza herramientas visuales para crear una estructura jerárquica para el usuario:

- **Sitio Central (Hub Site):** Se designa un sitio como "Centro" (Hub), y los sitios relacionados se **asocian** a él. Esta asociación es puramente visual, haciendo que los sitios hereden un **menú común de navegación transversal** y un **esquema de colores** compartido, lo que facilita la navegación y otorga una identidad gráfica consistente.
- **Landing Page:** Se recomienda establecer un sitio principal (*Home Site* o *Landing Page*) que sea el punto de entrada a la intranet, y se puede configurar un sitio específico para que sea la raíz de toda la estructura.
- **Diseño Moderno:** Los sitios de comunicación son **responsivos**, adaptándose correctamente al dispositivo con el que se visualizan (móviles, tabletas).

B. Componentes y Contenido

- **Plantillas y Web Parts:** La edición es modular, usando bloques predefinidos (Web Parts). Microsoft pone a disposición de las organizaciones ejemplos de diseño (como los que se encuentran en el Lookbook de Microsoft) que se pueden utilizar para crear sitios personalizados.
- **Identificación de Audiencias (Audience Targeting):** Esta es una funcionalidad clave. Permite que el contenido del sitio (como noticias, enlaces rápidos o elementos de menú) se muestre de forma personalizada según el grupo de Azure AD al que pertenece el usuario. Esto evita la necesidad de crear múltiples sitios paralelos para segmentar la información. Por ejemplo, se puede mostrar una opción de menú solo a los directivos.

C. Integración con Teams

La forma más moderna de consumir la intranet es directamente desde Microsoft Teams. Si bien la intranet se construye en SharePoint, su menú de navegación y contenido puede activarse y visualizarse dentro de la interfaz de Teams a través de la funcionalidad de *Home Site* (que requiere activación por PowerShell). Esto asegura que la intranet se convierta en una herramienta central accesible desde el entorno de colaboración diario.

\newpage

Capítulo 22: El Sitio de Colaboración es la piedra angular de la colaboración en Microsoft 365, definido por su propósito y por su arquitectura plana y dependiente del Grupo de Microsoft 365.

---

1. Definición y Propósito del Sitio de Colaboración

Un Sitio de Colaboración es una plantilla de sitio de SharePoint Online diseñada específicamente para el trabajo en equipo, proyectos o departamentos, donde la expectativa principal es la **participación activa y la edición de contenido por parte de todos los miembros**.

A diferencia del Sitio de Comunicación (*Communication Site*), que está orientado a la difusión de información de "uno para muchos" (donde la mayoría de los usuarios son visitantes de solo lectura), el Sitio de Colaboración está pensado para que **todos los usuarios trabajen al mismo nivel**.

2. Arquitectura: La Base del Ecosistema Moderno

La comprensión del Sitio de Colaboración es inseparable de la arquitectura moderna de Microsoft 365:

A. La Colección de Sitios Convertida en "Isla"

En el modelo de SharePoint moderno, la arquitectura jerárquica de sitios y subsitios del modelo clásico se elimina. El concepto de la antigua "colección de sitios" ha sido renombrado y simplificado: cada Sitio de Colaboración se comporta como un **ente independiente**, o una "isla".

Esta independencia implica que cada sitio gestiona de manera autónoma su cuota de espacio, su idioma y sus políticas de compartición externa, sin depender de la herencia de permisos de un sitio superior.

B. El Sitio de Colaboración es un Grupo de Microsoft 365

El objeto fundamental que da vida al Sitio de Colaboración moderno es el **Grupo de Office 365**. Cuando se crea un Sitio de Colaboración (Sitio de Grupo), automáticamente se le asocia un Grupo de M365. Este grupo actúa como un sistema de gestión de identidad y membresía que proporciona varios servicios unificados:

- **Repositorio de Ficheros (SharePoint):** El sitio de SharePoint en sí mismo, donde residen los documentos.
- **Buzón Compartido (Exchange):** Un buzón de correo centralizado para el equipo.
- **Calendario Compartido (Exchange):** Un calendario accesible para todos los miembros.
- **OneNote Compartido:** Un bloc de notas para el equipo.

C. Teams como la Capa Superior

La mayoría de las organizaciones no consumen el Sitio de Colaboración directamente desde el interfaz web de SharePoint, sino a través de **Microsoft Teams**.

- **Teams es la interfaz preferida:** Teams se construye como una capa adicional sobre el Grupo de M365 subyacente.
- **Funcionalidades añadidas:** Teams agrega funcionalidades clave que no están disponibles directamente en SharePoint, como el chat persistente, las videollamadas, y la integración sencilla de aplicaciones como Planner, Listas, Wikis o pizarras.
- **Mismo contenido, diferente vista:** Es fundamental entender que la información del Team **no está sincronizada** con SharePoint; es la *misma información* vista a través de una interfaz diferente. Por ejemplo, los canales de Teams se reflejan como carpetas dentro del sitio de SharePoint subyacente.

3. Modelo de Permisos y Compartimentación

La característica más definitoria del Sitio de Colaboración moderno es su filosofía de permisos simplificada.

- **"O estoy dentro o estoy fuera":** El enfoque moderno elimina la necesidad de permisos granulares y detallados (como permisos NTFS o los de "editor", "revisor" del SharePoint clásico). Si eres miembro del Grupo de M365/Team, tienes control completo sobre el contenido.
- **Consecuencias de la Granularidad:** Intentar aplicar permisos detallados manualmente en el sitio de SharePoint subyacente a un Team no es la forma correcta de trabajar según Microsoft, ya que la interfaz de Teams está diseñada bajo el presupuesto de que los miembros tienen acceso completo.
- **Aislamiento:** Si una organización necesita aislar información confidencial para un subconjunto de usuarios, la práctica correcta no es modificar los permisos de carpetas o archivos dentro del sitio, sino crear un **nuevo Team o contenedor separado** para esa información.

4. Gestión de Archivos y Buenas Prácticas

Aunque se utiliza principalmente para ficheros, los documentos en SharePoint se almacenan internamente como **listas**.

Recomendaciones de Acceso:

- **Trabajo en la Nube:** La práctica recomendada es trabajar directamente en la nube, accediendo a los archivos desde la interfaz de Teams o SharePoint.
- **Evitar la Sincronización Local:** Existe la opción de "Sincronizar" el repositorio de SharePoint/Teams con el disco duro local (a través de OneDrive), pero los expertos lo desaconsejan. La sincronización masiva aumenta la probabilidad de errores, de elementos duplicados, y puede interrumpir la colaboración en tiempo real, especialmente cuando hay muchos usuarios involucrados.

5. Gobernanza del Sitio de Colaboración

La creación descontrolada de Sitios de Colaboración (Teams) puede llevar a problemas de nomenclatura y gestión.

- **Limitación de Creación:** Se recomienda limitar quién puede crear Teams o Sitios de Grupo.
- **Delegación de Propiedad:** Se suele implementar un proceso donde el administrador crea el contenedor, pero asigna la responsabilidad de la gestión interna, la membresía, y el cumplimiento de las normas al **Propietario del Team**.
- **Nomenclatura:** Se pueden aplicar Directivas de Nombres para garantizar que los Grupos sigan una nomenclatura específica (aunque estas suelen requerir licencias Azure AD P1).

\newpage

Capítulo 23: # Centro de Administración de SharePoint: Guía Completa

Este panel ha evolucionado enormemente para adaptarse a la arquitectura moderna y plana que Microsoft promueve. A continuación, le explico detalladamente sus funcionalidades, su estructura y la filosofía que hay detrás de su administración.

1. La Filosofía del SharePoint Moderno y el Centro de Administración

Es fundamental entender que el Centro de Administración moderno está diseñado para gestionar sitios que son **"islas independientes"**, un concepto que rompe con la arquitectura jerárquica de sitios y subsitios del SharePoint clásico.

1. **Modelo Plano:** En el modelo moderno, se eliminó la herencia de permisos jerárquica. La administración ya no se centra en gestionar niveles profundos de un árbol, sino en supervisar y configurar colecciones de sitios individuales.
2. **Abandono del Clásico:** El centro de administración moderno ha quitado casi por completo las opciones y vistas del SharePoint clásico. Si bien aún existen remanentes por compatibilidad hacia atrás, estos se administran a través de interfaces antiguas y "horribles" a las que se accede con dificultad, ya que Microsoft desaconseja su uso y no quiere que los administradores utilicen la parte antigua.

2. Secciones Clave y Gestión de Sitios Activos

La sección principal del Centro de Administración es **Sitios Activos** (*Active Sites*), la cual ofrece una visión global de todos los contenedores de contenido creados en la organización, ya sean Sitios de Comunicación o Sitios de Grupo (los cuales son la base de los Teams).

A. Visión General y Propiedades

En esta lista es donde se visualizan y controlan los contenedores. Las columnas permiten ver información crítica de gobernanza:

- **URL y Nombre:** Identificación del sitio y posibilidad de cambiar la URL (lo cual, en el modelo moderno, se puede hacer sin que ocurran problemas).
- **Asociación a Teams/Grupos:** Indica si el sitio está conectado a un Team o si tiene un Grupo de Microsoft 365 por debajo.
- **Uso de Almacenamiento y Cuota:** Muestra el espacio ocupado y permite la gestión del límite de almacenamiento.
- **Sitio Central (Hub Site):** Indica si el sitio está asociado a un Centro o es un Centro en sí mismo (utilizado para heredar navegación visual y aspecto).
- **Administrador Principal y Creación:** Quién es el propietario del sitio, la fecha de creación, y si el sitio tiene aplicada alguna etiqueta de confidencialidad.

B. Gestión Individual de Sitios

Al seleccionar o hacer clic en un sitio individual, se accede a un panel lateral con opciones:

- **Edición:** Permite cambiar el nombre y la URL del sitio.
- **Permisos:** Desde aquí se puede ver quiénes son los propietarios del sitio o del Grupo de M365 subyacente, así como los administradores adicionales.
- **Directivas (Policies):** Permite configurar reglas específicas para ese sitio, como el control de uso compartido externo.

C. Sitios Eliminados

Esta sección permite la recuperación de sitios borrados. Los sitios eliminados se mantienen durante un periodo de hasta **93 días** antes de su purga permanente.

3. Políticas Globales y Controles de Gobernanza

La sección de **Directivas** (*Policies*) y **Configuración** (*Settings*) establece las reglas maestras de gobernanza para toda la organización, especialmente en lo que respecta a la seguridad de la información.

A. Directivas de Uso Compartido (Compartición Externa)

Esta es una de las configuraciones más importantes, ya que establece el nivel máximo de compartición externa para SharePoint y OneDrive. Es altamente recomendable configurarla por defecto:

1. **Límite de Compartición:** La práctica recomendada es limitar la compartición por defecto a "Invitados existentes o nuevos". Esto significa que nadie sin autenticación podrá acceder a los archivos de la empresa, evitando riesgos.
2. **Vínculos Anónimos:** Se desaconseja totalmente la compartición mediante **vínculos anónimos**, ya que representa un riesgo de seguridad.
3. **Permisos por Defecto:** Se recomienda configurar que los permisos por defecto para los enlaces de compartición sean de **solo lectura**, ya que los usuarios son "muy torpes" y a menudo otorgan permisos de escritura cuando solo pretenden que se visualicen los documentos.
4. **Caducidad de Enlaces:** Se puede configurar que el acceso de invitados y los enlaces caduquen automáticamente después de un periodo de tiempo (por ejemplo, 30 o 60 días).

B. Control de Acceso y Gestión de Dispositivos

Esta área contiene configuraciones que permiten restringir cómo y desde dónde se accede a SharePoint:

- **Restricción de Acceso:** Se puede restringir el acceso para que solo se permita la entrada a través de la web, bloqueando la descarga de archivos.
- **Dispositivos No Administrados:** Se puede denegar el acceso a dispositivos que no estén unidos al dominio o al Office 365, aunque el control más eficaz de los dispositivos (como el acceso condicional) se gestiona a través de Intune.

C. Configuración Global (Configuración)

Esta sección contiene ajustes que afectan a todos los sitios de SharePoint:

- **Creación de Sitios:** Permite limitar la creación de nuevos sitios a un grupo específico de usuarios, lo cual es una práctica clave de **gobernanza** para evitar la proliferación descontrolada de Teams y Sitios.
- **Sitio Principal (*Home Site*):** Se puede establecer un sitio específico como la página de aterrizaje (landing page) de la intranet de toda la organización.
- **Zona Horaria:** Es vital configurar correctamente la zona horaria predeterminada, ya que por defecto suele estar mal configurada (generalmente en la hora del Pacífico).
- **Límites de OneDrive:** Permite acotar la cuota de almacenamiento de OneDrive de cada usuario (por defecto 1 TB) para evitar que se saturen los discos locales y fomentar "mejor higiene" en el uso del espacio. También se pueden bloquear ciertos tipos de archivos para evitar que se suban películas o vídeos a OneDrive.

4. Herramientas de Migración y Aspectos Legacy

- **Herramienta de Migración (SMT):** El Centro de Administración enlaza a la **SharePoint Migration Tool** (SMT), una herramienta gratuita que facilita la copia de datos desde repositorios locales (como servidores de archivos) a SharePoint o OneDrive. Esta herramienta es crucial porque permite hacer la subida de datos en **varias pasadas incrementales** y escanea los archivos en el origen para detectar problemas de nomenclatura o longitud excesiva de los nombres.
- **Características Obsoletas:** Gran parte de las opciones fuera de la gestión de sitios y políticas son configuraciones antiguas que ya no se utilizan o que han sido reemplazadas por soluciones modernas de M365, como los sistemas de formularios (reemplazados por Power Apps) o la conectividad a bases de datos locales (BCS).

En resumen, el Centro de Administración de SharePoint es la herramienta esencial para mantener el control y la seguridad sobre los contenedores de la organización, asegurando que la arquitectura se mantenga plana y que el uso compartido de la información se adhiera a las políticas de gobernanza definidas.

\newpage

Capítulo 24: ### La Administración de Teams: Un Enfoque Experto y Didáctico

Teams es una de las tres herramientas principales o cargas de trabajo fundamentales de Microsoft 365, junto con Exchange Online (correo electrónico) y SharePoint (repositorio de archivos, documentación y comunicación). Teams actúa como un aglutinador de información y capacidad de comunicación, y su administración se lleva a cabo principalmente a través del **Centro de Administración de Teams**.

1. Arquitectura y Fundamentos de Teams

Para entender la administración de Teams, es fundamental comprender su estructura subyacente:

1. **Teams como capa visual:** Teams no es una entidad independiente, sino una capa adicional sobre otros servicios.
2. **Grupos de Microsoft 365 y SharePoint:** Cada vez que se crea un Team, automáticamente se crea por debajo un **Grupo de Office 365** (anteriormente llamados Grupos Modernos o Unificados). Este grupo, a su vez, es un **Sitio de SharePoint Online**.
3. **Administración Compartida:** Debido a esta dualidad, hay configuraciones que se gestionan directamente desde el Centro de Administración de Teams y otras que deben gestionarse desde el Centro de Administración de SharePoint (especialmente aquellas relacionadas con la capacidad de compartir con usuarios externos o la estructura de archivos).
4. **Sitios Ocultos:** Si bien cada Team tiene un Grupo y un Sitio de SharePoint subyacentes, el Grupo suele permanecer oculto en la interfaz tradicional de Grupos (Outlook/OWA) si ha sido creado como un Team. Esto se debe a que la funcionalidad de Teams es superior a la interfaz de Grupos antigua. Esta propiedad de ocultamiento puede modificarse mediante PowerShell.

Nota Didáctica: El objeto que gestiona la membresía y el acceso a un Team es el Grupo de Microsoft 365 que se encuentra debajo.

2. Gobierno y Gestión de Equipos

Una de las tareas de administración más importantes es el **Gobierno** (Governance) de la plataforma, especialmente para evitar la proliferación descontrolada de Teams, que puede llevar a la confusión (como el ejemplo del Team llamado "Manoli, Pepi, Antonio y yo").

- **Limitación de Creación:** La práctica recomendada es limitar quién puede crear Teams. Esto se logra limitando quién puede crear los Grupos de Microsoft 365.
- **Roles de Propietario:** Una vez creado el Team (normalmente mediante un proceso formal, como un formulario), se asigna un *Propietario* que se encarga de la membresía y de ajustar configuraciones internas del Team, liberando así al administrador general.

Desde el Centro de Administración de Teams, el administrador puede ver un listado de todos los equipos activos, modificar sus propiedades (como cambiar un equipo de público a privado), y gestionar miembros y canales sin necesidad de ser un propietario directo del Team. También es posible sacar informes detallados sobre el uso que se le da a cada Team (última actividad, tráfico de archivos, etc.) para ajustar licencias o tomar decisiones de limpieza.

3. Configuración por Directivas (Policies)

La configuración en Teams se basa en **Directivas**, lo cual permite una gestión granular y selectiva. Por defecto, existe una **Directiva Global (Estándar)** que se aplica a todos los usuarios, pero se pueden crear directivas específicas para conjuntos de usuarios (como comerciales o directivos) y asignarlas individualmente o por grupos.

Las Directivas abarcan numerosos aspectos de la experiencia de Teams:

- **Paquetes de Directivas (Policy Packages):** Para organizaciones complejas, los paquetes de directivas simplifican la administración al agrupar múltiples directivas (de llamadas, mensajería, reuniones, etc.) y aplicarlas conjuntamente a un grupo (ej. "Comercial").
- **Directivas de Equipo (Team Policies):** Controlan funcionalidades básicas dentro de un Team, como si los usuarios pueden o no crear canales privados.
- **Directivas de Mensajería:** Definen qué se permite en los chats. Esto incluye la activación o desactivación de funciones como el uso de GIFs, memes o si los usuarios pueden editar los mensajes enviados. También controlan el uso de **etiquetas** (*tags*), que permiten notificar rápidamente a un subconjunto específico de personas dentro de un Team numeroso.
- **Directivas de Reunión:** Gobiernan la experiencia de videoconferencia, incluyendo:
    - La posibilidad de unirse de forma anónima a una reunión.
    - Opciones de audio y video.
    - Restricciones sobre quién puede presentar o compartir pantalla.
    - La configuración de la caducidad automática de las grabaciones de reuniones (ej. a los 120 días) para gestionar el almacenamiento.
    - Si se permite el botón "Reunirse ahora" en los canales.
- **Directivas de Eventos en Directo:** Controlan los parámetros de los eventos en vivo (*Live Events*), que son presentaciones unidireccionales (como un webinar o una keynote) para grandes audiencias, incluyendo la posibilidad de apertura al público externo (que requiere tiempo de activación, un día aproximadamente).
- **Directivas de Actualización:** Permiten controlar la versión de Teams que reciben los usuarios, de modo que los usuarios más avanzados o técnicos puedan recibir las características de vista previa más rápidamente, mientras que otros usuarios pueden esperar a versiones más estables.

4. Aplicaciones y Personalización de Interfaz

La administración de aplicaciones es otro componente clave, dado que Teams permite integrar miles de aplicaciones de terceros (como Adobe Acrobat o Trello) y aplicaciones de Microsoft.

- **Configuración Global:** Se pueden establecer reglas para toda la organización, como prohibir el uso de aplicaciones de terceros o aplicaciones personalizadas.
- **Configuración por Aplicación:** El administrador puede decidir, aplicación por aplicación, cuáles se permiten o se bloquean.
- **Personalización del Interfaz:** Mediante las **Directivas de Configuración**, el administrador puede definir qué aplicaciones aparecen en el panel izquierdo de Teams y en qué orden (solo caben seis aplicaciones en ese panel). Esto es útil para simplificar el entorno o destacar herramientas corporativas esenciales, como una aplicación de gestión de turnos.

5. Gestión de Acceso Externo y Colaboración

- **Acceso de Invitados (Guests):** Se refiere a la configuración de lo que puede hacer una persona externa (invitada) que ha sido agregada a un Team. Por defecto, los invitados tienen capacidad de lectura y escritura, no son actores de solo lectura. Las directivas controlan si se permite esta funcionalidad y bajo qué parámetros.
- **Acceso Externo (External Access):** Se refiere a la capacidad de los usuarios de comunicarse (chatear) con usuarios que se encuentran en otras organizaciones de Teams o que aún usan Skype. Se puede limitar este acceso solo a dominios específicos.

6. Administración Adicional y Consideraciones

- **Telefonía y Voz (Voice):** Gran parte del Centro de Administración de Teams está dedicado a la funcionalidad de voz sobre IP (VoIP), ya que Teams puede actuar como una centralita completa. Opciones como el correo de voz, la directiva de llamadas o los planes de mercado requieren la compra de licencias y complementos adicionales. Si estas funcionalidades no se usan, estas opciones pueden ignorarse.
- **Correo Electrónico a Canales:** Es posible asociar una dirección de correo electrónico a un canal específico, permitiendo que los correos enviados a esa dirección aparezcan como publicaciones dentro del canal (con los archivos adjuntos guardados en una carpeta especial).
- **PowerShell:** Aunque la interfaz web es robusta, hay tareas avanzadas (como algunas configuraciones complejas de reuniones o la gestión masiva de datos) que solo se pueden realizar mediante comandos de PowerShell. Existe un módulo de administración específico de Teams para PowerShell.

\newpage

Capítulo 25: # Directivas de Reunión en Microsoft Teams

Configuraciones Recomendadas en las Directivas de Reunión de Teams

Configuración	Recomendación/Práctica	Justificación/Detalles

Configuración	Recomendación/Práctica	Justificación/Detalles
"Reunirse ahora" en canales	**Desactivar** (Quitar el botón).	Los usuarios a menudo no entienden que al usar la opción "Reunirse ahora" en un canal, se convoca una reunión para *todos* los miembros de ese equipo.
Programación de reuniones en canales	**Activar** (Permitir).	Es útil para canales cuyos miembros se reúnen de manera regular, ya que al programarla en el canal, se invita automáticamente a todos los miembros, evitando el tedio de tener que agregar las direcciones de correo electrónico una a una, ya que Teams no lo hace automáticamente.
Grabación en la nube: Caducidad automática	**Configurar** una caducidad automática (ej. 120 días/horas).	Se recomienda para gestionar el espacio de almacenamiento, ya que muchas grabaciones de reuniones no se usan después de grabarse.
Unión de personas anónimas	**Desactivar** (Quitar el permiso para la mayoría de los usuarios/directivas).	Esto evita que personas sin autenticación ni identidad conocida puedan unirse a reuniones. Es especialmente importante si se va a tratar información confidencial.
Reenvío de reuniones	**Desactivar** (Restringir o prohibir).	Previene que las invitaciones a reuniones se reenvíen indiscriminadamente, lo que podría permitir el acceso de personas anónimas a la reunión.
Uso Compartido de Pantalla	**Limitar** a "Compartir solo una aplicación" (compartir una sola aplicación).	Esto hace mucho más difícil que los usuarios compartan accidentalmente información confidencial que podría estar visible en otras ventanas de su escritorio.
Filtros de video (Fondos)	**Limitar o restringir** (como fondos predeterminados o corporativos).	Puede ser necesario para mantener una imagen de seriedad de la empresa, evitando fondos inapropiados o no profesionales (como la referencia a Bob Esponja). Existe una funcionalidad en desarrollo para cargar imágenes de fondo corporativas predeterminadas para toda la empresa.
Activación de transcripción	**Revisar/Configurar** según las necesidades de la organización.	La transcripción en reuniones no está activa por defecto en las directivas que organiza el administrador.
Eventos en directo (Live Events)	**Cambiar** la configuración de acceso con anticipación (aprox. 1 día).	Por defecto, solo los miembros de la organización pueden unirse a Eventos en Directo (webinars, keynotes). Si se requiere que el evento sea público o abierto a gente externa, esta política debe modificarse con tiempo, ya que tarda un día en activarse.
Reuniones privadas (One-on-one calls)	**Restringir/Desactivar** si es necesario.	En ciertos casos, la organización puede querer deshabilitar las llamadas uno a uno si ya se está utilizando otro software o plan de un tercero para ese tipo de comunicación.

Consideraciones Adicionales sobre Directivas

Es importante recordar que la gestión de directivas en Teams opera de manera modular y selectiva:

1. **Directiva Global (Estándar):** Siempre existe una directiva base que se aplica a todos los usuarios que no tienen una directiva específica asignada.
2. **Granularidad:** Al ser directivas, usted puede crear configuraciones específicas (por ejemplo, "Directiva VIP" o "Directiva Comerciales") y aplicarlas a un conjunto de usuarios en particular, permitiendo un nivel de control distinto al del resto de la organización.
3. **Paquetes de Directivas (Policy Packs):** Para simplificar la administración, especialmente en organizaciones complejas, se pueden crear *paquetes de directivas* que agrupan varias configuraciones (de voz, chat, reuniones, etc.) y se asignan a grupos de usuarios (como el grupo "Comercial").
4. **Tiempo de Propagación:** Es crucial tener en cuenta que los cambios realizados en las directivas de Teams **no tienen un efecto inmediato**. Normalmente, estos cambios pueden tardar hasta un día en aplicarse.

\newpage

Capítulo 26: # Directivas de Mensajería en Microsoft Teams

Configuraciones Recomendadas en las Directivas de Mensajería de Teams

Configuración	Recomendación/Práctica	Justificación/Detalles
Activación del Chat (Global)	**Activado** (Por defecto).	La directiva de mensajería controla si el chat está activado o no. Desactivarlo negaría la funcionalidad principal de comunicación de Teams, lo cual es inusual a menos que haya requisitos específicos que lo prohíban.
Uso de Memes, GIFs y Pegatinas (Stickers)	**Activado** (Si el entorno lo permite).	Aunque parezcan triviales, el uso de estos elementos ayuda a la comunicación, ya que el texto plano (mediocrito) es "mucho más árido". Si bien algunos administradores pueden eliminarlos por considerar que no son serios, la tendencia es mantenerlos para fomentar una comunicación dinámica.
Creación de Mensajes de Voz	**Configurar** según la necesidad del usuario.	Las directivas permiten gestionar si los usuarios pueden crear mensajes de voz. Esto es especialmente relevante para el uso de Teams en dispositivos móviles.
Visualización de Contenido (Reciente vs. Favoritos)	**Configurar** según el perfil del usuario (ej. mostrar favoritos primero para *frontline workers*).	Se puede definir si en dispositivos móviles lo más reciente aparece arriba o si se priorizan los favoritos. En roles como *Frontline Worker* (trabajadores de primera línea), donde el uso es mínimo, se suelen aplicar directivas que muestran solo lo básico.
Respuestas Sugeridas	**Activado** (Si se desea simplificar la comunicación).	Permiten simplificar el proceso de respuesta al ofrecer opciones rápidas sin necesidad de teclear.

Configuración	Recomendación/Práctica	Justificación/Detalles
Roles dentro del Chat (Permisos)	**Configurar** según el perfil (Si la organización lo requiere).	La directiva puede controlar si se permite poner distintos roles dentro de un chat, asegurando que no todo el mundo tenga el mismo nivel de capacidad de comunicación.
Administración de Etiquetas (Tags)	**Permitir** a los propietarios administrar etiquetas.	Las etiquetas son cruciales para notificar rápidamente a un subconjunto específico de personas dentro de un Team grande (ej. solo a los directores en un Team de 200 personas). La directiva de configuración de Teams permite que los propietarios administren y sugieran estas etiquetas.

Aspectos Clave de la Gestión de Directivas de Mensajería

Las directivas de mensajería, al igual que otras directivas en Teams (como las de reunión, aplicación o equipo), operan bajo un principio de granularidad que es crucial para una administración eficaz:

1. **Directiva Global (Estándar):** Siempre existe, al menos, una directiva **Global (Estándar)** que se aplica por defecto a todos los usuarios de la organización.
2. **Granularidad:** Usted puede crear directivas personalizadas, como una "Directiva VIP" o "Directiva Comercial", con configuraciones específicas (por ejemplo, permitir o restringir ciertas funcionalidades de chat) y asignarlas a usuarios o grupos particulares.
3. **Paquetes de Directivas (Policy Packs):** Para organizaciones complejas, la forma más eficiente de asignar configuraciones es mediante **Paquetes de Directivas**. Un paquete agrupa múltiples directivas (incluyendo las de mensajería/chat, llamadas, reuniones, etc.) y se asigna al usuario o a un grupo. Esto estandariza la configuración para roles específicos (como comerciales o profesores), simplificando la incorporación de nuevos usuarios.

Advertencia Didáctica: Es vital recordar que los cambios realizados en las directivas de Teams no son inmediatos; normalmente, tardan hasta un día en surtir efecto. Por ello, se recomienda la paciencia tras aplicar cualquier modificación.

\newpage

Capítulo 27: # Seguridad y Cumplimiento en Microsoft 365

La Administración de Seguridad y Cumplimiento en Microsoft 365

La gestión de la seguridad y el cumplimiento se lleva a cabo principalmente en dos centros de administración separados, aunque relacionados, debido a la diferencia en los roles que los administran (administradores de TI versus personal legal o auditores).

1. **Centro de Administración de Seguridad (Microsoft Defender):** Orientado a la gestión activa de amenazas, la protección de puntos de conexión y la configuración de políticas.

2. **Centro de Administración de Cumplimiento (Microsoft Purview):** Orientado a las obligaciones legales, el gobierno de datos, auditorías y gestión de riesgos, área que Microsoft ha renombrado recientemente a **Microsoft Purview**.

1. Arquitectura y Dependencia de Licencias

La disponibilidad de las funcionalidades de seguridad y cumplimiento está estrechamente ligada a la licencia que se posea. Por ejemplo, si se tiene la licencia **Business Premium** (la cual el experto recomienda por su relación calidad-precio), esta incluye funcionalidades avanzadas:

- **Microsoft Defender for Business:** Esta es una versión ligera (*light*) del costoso Microsoft Defender for Endpoint, que proporciona capacidades importantes como la **Detección y Respuesta de Puntos de Conexión (EDR)**. EDR y la investigación automatizada de amenazas están incluidas y son muy valiosas.
- **Intune (Endpoint Manager):** Permite la gestión de dispositivos (PC, iPad, macOS, Android).
- **Azure AD P1:** Necesaria para habilitar funcionalidades clave de identidad, como el **Acceso Condicional**.

Es importante notar que muchas funcionalidades de seguridad requieren licencias avanzadas (como Azura AD P1) y si bien el panel de administración puede permitir la configuración, su uso real puede depender de que todos los usuarios dispongan de la licencia adecuada.

2. Seguridad de la Plataforma y la Identidad

La protección comienza en la identidad y el acceso, gestionado en parte por Azure AD:

- **Puntuación de Seguridad (Secure Score):** Una herramienta esencial que evalúa el estado de seguridad del *tenant* (entorno de Office 365) y ofrece una lista de acciones recomendadas para mejorar la seguridad (como habilitar la MFA para todos los usuarios o configurar la restricción de reenvío de correo). Las acciones se priorizan según cuánto mejorarían la seguridad.
- **Valores Predeterminados de Seguridad (*Security Defaults*):** Configuración de seguridad básica y no administrable que Microsoft impone por defecto. Microsoft ha anunciado que esto será obligatorio, asegurando que incluso los usuarios que no han implementado MFA lo tengan activado de alguna forma.
- **Acceso Condicional (*Conditional Access*):** Es una funcionalidad poderosa que permite crear reglas estrictas basadas en el riesgo, la ubicación o el dispositivo del usuario. Por ejemplo, se puede exigir la autenticación multifactor (MFA) si el usuario inicia sesión fuera de la red corporativa, o bloquear el acceso si se detecta un "viaje imposible" (inicios de sesión distantes en poco tiempo).

3. Políticas de Protección de Correo (Policies & Rules)

El correo electrónico es el principal vector de ataque, por lo que las directivas de protección son fundamentales:

- **Antimalware:** Las políticas de *Antimalware* son estrictas ya que "con el malware no se negocia". Se recomienda ser extremadamente estricto con las extensiones de archivos adjuntos y bloquear formatos que son comunes en los ataques de *ransomware* y *malware* (como `.ISO`, `.LNK`, `.CMD`, `.BAT`).
- **Antispam y Antifishing:** Permiten configurar umbrales de agresividad (puntuación) para el *spam* y el *phishing*.

    - **Bloqueo por Origen:** Es posible aumentar la puntuación de riesgo si el correo proviene de países o lenguajes específicos con los que la empresa no trabaja.
    - **Controles de Dominio (SPF, DKIM, DMARC):** Estos mecanismos refuerzan la seguridad del correo y evitan la suplantación de identidad (spoofing).
        - **SPF (Sender Protection Framework):** Publica qué servidores están autorizados a enviar correo en nombre de su dominio.
        - **DKIM (DomainKeys Identified Mail):** Firma digitalmente los correos electrónicos para que el receptor verifique la legitimidad del emisor.
        - **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Indica al receptor qué hacer con los correos que fallan las comprobaciones SPF o DKIM (rechazarlos, ponerlos en cuarentena o aceptarlos) y permite solicitar informes sobre cómo se reciben los correos de su dominio.
- **Reenvío de Correo (*Forwarding*):** Es una configuración de alto riesgo que debe controlarse y justificarse, ya que es la técnica más común utilizada por los atacantes para mantener el acceso y recibir copias de los correos incluso después de que las credenciales de la víctima han sido restablecidas. Existen alertas para detectar reenvíos automáticos a cuentas externas.
- **Cuarentena (*Quarantine*):** Las políticas de cuarentena modernas permiten definir si los usuarios comunes tienen acceso a ver los mensajes retenidos y qué acciones pueden realizar (como solicitar su liberación, sin poder liberarlos directamente).

4. Cumplimiento, Retención y Auditoría (Purview)

Estas funcionalidades se centran en el gobierno de la información para cumplir con requisitos legales:

- **Retención (*Retention*) y Suspensión por Litigio (*Litigation Hold*):** Es crucial entender que Office 365 no ofrece copias de seguridad (*backup*) del correo; en su lugar, ofrece **retención**. *Litigation Hold* es una funcionalidad de licencia avanzada que permite conservar todos los cambios históricos en un buzón de correo (o archivos/chats de Teams) de forma permanente, de modo que el contenido nunca se pierde, incluso si el usuario lo borra.
- **Auditoría (*Auditing*):** Permite registrar detalladamente las acciones realizadas por usuarios y administradores (por ejemplo, quién modificó un fichero). En *tenants* antiguos, la auditoría puede no estar activada por defecto y debe habilitarse manualmente.
- **Descubrimiento Electrónico (*eDiscovery*):** Herramienta que permite a los equipos legales crear búsquedas y extraer contenido específico (correos, documentos, etc.) de la plataforma en un formato que es legalmente aceptable para ser presentado ante un tribunal.
- **Etiquetas de Confidencialidad (*Confidentiality Labels*):** Sellos de seguridad adicionales que se aplican a los documentos (sitios de SharePoint, OneDrive, chats de Teams) para controlar los derechos de uso, independientemente de la ubicación del archivo. Estas etiquetas pueden impedir la impresión, la descarga o hacer que el documento caduque automáticamente. Requieren licenciamiento avanzado.

\newpage

Capítulo 28: # Directiva de Retención en Office 365

1. El Concepto Fundamental: Retención vs. Copia de Seguridad

Es crucial entender que **Office 365 no incluye una copia de seguridad (backup) del correo**. La estrategia de Microsoft se basa en la **retención** y la **disponibilidad** del correo.

Microsoft garantiza que el servicio de correo estará disponible con una caída máxima de 4 horas y una pérdida máxima de elementos de correo de 2 horas. Esto se logra manteniendo cuatro copias de cada base de datos de buzones, tres replicadas y una cuarta en otro país con un desfase de 2 horas.

2. Retención por Defecto y Pérdida de Datos

Aunque no hay un backup tradicional, Office 365 retiene los cambios que sufren los buzones de correo por un tiempo.

- **Proceso de Eliminación:** Cuando un usuario borra un correo y lo elimina permanentemente (de la carpeta de elementos eliminados), Office 365 lo mantiene internamente guardado por un periodo.
- **Período por Defecto:** Por defecto, el tiempo de retención de estos elementos eliminados permanentemente es de **15 días**, aunque puede ampliarse a **30 días**.
- **Pérdida Permanente:** Una vez superados los 30 días, si no se ha aplicado ningún mecanismo de retención adicional, la información se pierde de forma permanente, lo que implica que no hay forma de recuperar ese correo, incluso si fuera necesario por temas legales.

3. Mecanismos Avanzados de Retención y Cumplimiento

Para cumplir con requisitos legales o regulatorios (compliance), existen mecanismos que aseguran que el contenido se mantenga indefinidamente o por un tiempo prolongado.

A. Suspensión por Litigio (Litigation Hold)

Esta funcionalidad, a la que se accede a través del centro de administración de Exchange, permite activar un buzón para que **todos los cambios siempre se registren y nunca se elimine nada**.

- **Efecto:** El usuario puede percibir que ha borrado el contenido, pero internamente el sistema mantiene guardadas todas las versiones del buzón, permitiendo a los administradores o equipos legales volver a una versión específica en el tiempo.
- **Licenciamiento y Costo:** La suspensión por litigio requiere una **licencia avanzada**. Al activarse, aunque el contenido eliminado esté oculto para el usuario, este consume espacio en la base de datos subyacente (no en la cuota visible del buzón), lo que implica un costo a nivel de licenciamiento.

B. Buzón de Archivado (Archive Mailbox)

El buzón de archivado es una solución para gestionar grandes volúmenes de correo y evitar que el buzón principal consuma excesivo espacio.

- **Capacidad:** El buzón de archivado tiene por defecto **100 GB** de capacidad, la cual puede ampliarse incluso a **Terabytes**, dependiendo de la licencia.
- **Uso:** Los usuarios pueden utilizarlo directamente, y se pueden establecer reglas automáticas para mover al buzón de archivado el contenido más antiguo (por ejemplo, con las directivas MRM).
- **Ventaja Técnica:** El contenido del buzón de archivado no se descarga en el archivo de caché local (OST) del usuario, lo que aligera la carga de los equipos y permite mantener información histórica sin afectar el rendimiento diario.

C. Directivas de Retención de Registros de Mensajes (MRM)

Estas son configuraciones más antiguas, heredadas de Exchange, que permiten la **autogestión del contenido** dentro del buzón.

- **Funcionalidad:** Permiten configurar reglas (políticas de archivo o retención) para que el contenido de las carpetas de correo se autogestione, por ejemplo, eliminando automáticamente lo que llega a la bandeja de entrada después de un mes, o purgando elementos eliminados cada 3 meses.
- **Aplicación:** Los usuarios pueden aplicar estas políticas de retención manualmente desde Outlook o OWA (Outlook Web Access).

D. Etiquetas de Retención y Confidencialidad (Microsoft Purview)

En el modelo moderno de Microsoft, las directivas de cumplimiento y seguridad se gestionan a través del centro de **Microsoft Purview** (anteriormente Compliance). Aquí se definen las etiquetas de retención y confidencialidad (Retention Labels y Sensitivity Labels).

- **Alcance Amplio:** Las etiquetas de retención ya no se limitan solo al correo, sino que tienen un alcance mucho más global, aplicándose a: **sitios de SharePoint, OneDrive y chats de Teams**.
- **Propósito Legal:** Permiten definir que el contenido marcado con dicha etiqueta no se pueda borrar de forma permanente hasta que haya transcurrido un tiempo específico (por ejemplo, 5 años) porque así lo exija la ley.
- **Requisito de Licencia:** Es importante notar que aunque las opciones para crear estas etiquetas pueden ser visibles, para que sean funcionales y aplicables en el entorno, se requiere una **licencia superior** como E3 o su equivalente.

E. Retención de Registros de Auditoría (Audit Logs)

Dentro del centro de cumplimiento (Compliance), las políticas de auditoría (Audit Policy) permiten especificar el tiempo que se desea conservar los registros de actividad (logs de auditoría). Por ejemplo, es posible configurar que estos registros se mantengan hasta por 10 años.

\newpage

Capítulo 29: ### 1. Nomenclatura y Licenciamiento: Entendiendo los Tiers

Es esencial distinguir las diferentes versiones de Defender, ya que su funcionalidad depende directamente del plan de licenciamiento que posea:

A. Defender for Business (Negocios)

Esta es la versión que Microsoft ha incluido recientemente en la licencia **Business Premium** (para organizaciones de hasta 300 usuarios). Esta inclusión ha hecho que la licencia Premium sea altamente valiosa.

- **Capacidades Incluidas:** Defender for Business ofrece una plataforma de seguridad muy avanzada que normalmente sería costosa. Incluye funcionalidades de:
    - **Antivirus y Protección de Próxima Generación:** Un antivirus avanzado.

- **EDR (Endpoint Detection and Response):** Esta es una función crucial. Un antivirus tradicional se basa en firmas; EDR analiza el comportamiento y correlaciona eventos entre distintos equipos. Permite realizar investigaciones y respuestas automatizadas ante amenazas, incluso si el malware no tiene una firma conocida.
- **Administración de Vulnerabilidades:** Ayuda a identificar y priorizar los puntos débiles en los dispositivos.
- **Investigación y Respuesta Automatizada:** Permite seguir una línea de tiempo de lo que ocurrió durante un incidente de seguridad, aislar equipos y aplicar remediaciones automáticas.

B. Defender for Endpoint (Enterprise)

Esta es la solución de seguridad para grandes empresas (Enterprise) y está disponible en los planes E5 o como complemento avanzado. Microsoft Defender for Business es, esencialmente, una versión "light" de este producto, aunque incluye características de alto nivel que antes solo estaban en el plan más caro (Plan 2) de Defender for Endpoint.

C. Defender for Office 365

Esta parte se centra en la protección del correo electrónico, una vía de entrada común para los ataques cibernéticos. En las licencias **Business Standard**, muchas de las funciones avanzadas de Defender for Office 365 (como el Plan 1) no están disponibles.

---

2. Funcionalidades Clave en el Centro de Seguridad

La gestión de Defender se lleva a cabo principalmente en el Centro de Seguridad, ahora parte de **Microsoft Purview** (Cumplimiento).

2.1 Puntuación de Seguridad (Secure Score)

Esta herramienta proporciona una métrica de la postura de seguridad de su entorno de Microsoft 365.

- **Evaluación y Recomendaciones:** Muestra un porcentaje que refleja cuántas de las configuraciones de seguridad recomendadas tiene activas. Si no tiene la **Autenticación Multifactor (MFA)** activada para todos los usuarios, por ejemplo, esto reducirá su puntuación.
- **Acciones Correctivas:** Sugiere acciones específicas para mejorar la seguridad, proporcionando guías sobre cómo implementarlas (aunque a veces las guías pueden llevar a interfaces antiguos o confusos). Incluso le permite marcar un riesgo como "aceptado" si es necesario para un proceso de negocio.

2.2 Protección Avanzada de Correo Electrónico

Defender administra políticas críticas que reducen drásticamente la exposición a amenazas:

- **Vínculos Seguros (Safe Links):** Una directiva que protege contra enlaces maliciosos en correos electrónicos. Cuando un usuario hace clic en un enlace, Safe Links lo redirige y lo prueba en un entorno seguro antes de permitir el acceso, mitigando el riesgo de *phishing*.
- **Análisis de Amenazas (Threat Analytics):** Proporciona información detallada sobre las últimas campañas de ataques cibernéticos (como ransomware o TrickBot). Esta sección alerta si su organización

ha sido el objetivo de correos maliciosos asociados a esas campañas. Los informes detallan las metodologías de ataque (acceso inicial, robo de credenciales, movimiento lateral, etc.).

2.3 Administración de Aplicaciones y Dispositivos (Requiere Intune)

Las características de Defender relacionadas con la gestión de dispositivos y aplicaciones dependen de que su licencia incluya **Intune** (como la Business Premium).

- **Inventario y Riesgo de Dispositivos:** Permite visualizar los dispositivos inscritos (PCs, iPads, macOS, Android) y evaluar su nivel de exposición y vulnerabilidad.
- **Defender for Cloud Apps:** Monitorea las autorizaciones que los usuarios otorgan a aplicaciones de terceros (por ejemplo, al conectar Adobe o SAP). Esto es vital, ya que una técnica de ataque común es engañar al usuario para que autorice una "aplicación malware" para acceder y robar información de Office 365.

---

3. Defender y las Directivas de Seguridad

Defender trabaja a través de la aplicación de diversas **directivas** (policies) que definen el comportamiento de la seguridad:

- **Directivas de Anti-Phishing y Anti-Spam:** Permiten definir el umbral de agresividad del filtro de correo. La configuración anti-malware, por ejemplo, no se negocia: si detecta malware, se elimina, aunque se puede configurar para notificar. Es posible bloquear adjuntos que representan un riesgo (como archivos .ISO o ejecutables LNK/CMD).
- **Directivas de Cuarentena:** Permiten crear políticas específicas sobre cómo se manejan los correos en cuarentena. Es posible dar acceso limitado a los usuarios para que puedan revisar los mensajes, pero sin darles permiso para liberarlos, evitando que un usuario "torpe" libere inadvertidamente un correo peligroso.
- **Directivas de Cumplimiento:** Aunque la gestión principal de las **Etiquetas de Confidencialidad (Sensitivity Labels)** y **Etiquetas de Retención (Retention Labels)** se realiza en Purview, estas políticas de cumplimiento (que requieren licencia E3 o superior) trabajan de la mano con Defender para asegurar la protección de datos sensibles. Las etiquetas de confidencialidad pueden, por ejemplo, impedir la impresión de documentos o hacer que el acceso caduque después de cierto tiempo.
- **Auditoría (Audit Logs):** Por defecto, la plataforma registra todas las actividades (quién modificó un archivo, quién lo compartió, quién inició sesión), lo cual es crucial para la seguridad. Estas bitácoras se pueden retener hasta por 10 años, según la política de auditoría configurada.

\newpage

Capítulo 30: # Directivas de Confidencialidad en Office 365

Propósito y Funcionalidad

El objetivo principal de estas etiquetas es ofrecer un mecanismo granular para proteger datos sensibles que va más allá de los permisos básicos de acceso que se configuran en sitios o grupos.

Las funcionalidades de protección clave que se pueden aplicar mediante estas etiquetas incluyen:

1. **Control de Acceso Riguroso:** La etiqueta puede establecer que, para abrir un documento, un usuario debe pertenecer a un grupo específico, haciendo que los permisos de acceso tradicionales sean irrelevantes. Un usuario no podrá abrir el archivo si no es miembro del grupo definido en la etiqueta.
2. **Gestión de Derechos Digitales:** Permiten controlar acciones que el usuario puede realizar con el contenido una vez que tiene acceso a él. Por ejemplo, se pueden establecer reglas para **impedir la impresión de un documento**.
3. **Caducidad del Contenido:** Se puede configurar que el acceso al archivo "caducue" después de un tiempo determinado, como a los tres días, tal "como los yogures".
4. **Cifrado y Marcado:** Las etiquetas de confidencialidad se utilizan para marcar elementos con un **nivel de protección más alto**, asegurando que si la información sale del entorno de la organización, se mantenga protegida según las políticas establecidas.

Alcance de las Etiquetas

Es importante notar que estas etiquetas no se limitan solo al correo electrónico, sino que tienen un alcance global dentro de la plataforma de Microsoft 365, abarcando una capa mucho más amplia que la gestión de registros de mensajes (MRM) de Exchange:

- **Correo electrónico**.
- **Sitios de SharePoint**.
- **OneDrive**.
- **Chats de Teams**.

Al aplicar una etiqueta, esta viaja con el contenido, asegurando que la política de confidencialidad se respete sin importar dónde se almacene o se comparta.

Administración y Licenciamiento (Detalles Cruciales)

La gestión de las Directivas de Confidencialidad y de Retención se centraliza en el Centro de Administración de Cumplimiento (Compliance), ahora conocido como **Microsoft Purview**.

Dentro de Purview, estas etiquetas se crean en la sección de **Clasificación de datos** (Data Classification) y están estrechamente ligadas a la funcionalidad de **Information Protection**.

Requisito de Licenciamiento:

Como experto, debo ser **detallista** sobre la licencia requerida, ya que esta es una funcionalidad avanzada que no se incluye en los planes base:

- **Licencia Requerida:** Para que las etiquetas de confidencialidad sean funcionales y se apliquen efectivamente, se requiere una **licencia superior**, como **E3 o un equivalente**.
- **Visibilidad vs. Funcionalidad:** Es común que, aunque un administrador pueda ver las opciones para crear estas etiquetas en el panel de Purview, no serán operativas en el entorno si la organización no dispone del licenciamiento adecuado. Si se intenta activar en licencias estándar, la funcionalidad "no sirve, no protege nada".

\newpage

Capítulo 31: ## Microsoft Defender para Office 365: El Escudo Antimalware

Microsoft Defender for Office 365 es la solución de seguridad que protege la infraestructura de correo electrónico de su organización. A diferencia de un antivirus de puesto de cliente, Defender actúa sobre el correo **mientras está en tránsito** dentro de la plataforma Microsoft 365.

Esta plataforma incluye funcionalidades esenciales como:

1. **Antispam y Antimalware:** Políticas que escanean el tráfico de correo para bloquear o poner en cuarentena amenazas conocidas. En el caso del *malware*, la política es clara: "no se negocia", el archivo debe eliminarse o ponerse en cuarentena.
2. **Antifishing:** Políticas avanzadas que utilizan inteligencia artificial para detectar la suplantación de identidad (spoofing), incluso ofreciendo indicadores visuales al usuario cuando recibe un correo por primera vez de un remitente específico.
3. **Cuarentena y Revisiones:** El centro de seguridad permite a los administradores revisar los correos que han sido detenidos por estas políticas.

Para que esta protección sea efectiva, es fundamental que el sistema pueda verificar que el correo que recibe o envía es legítimo. Aquí es donde entran en juego los tres protocolos de autenticación de correo.

La Tríada de Autenticación de Correo Electrónico: SPF, DKIM y DMARC

Estos tres protocolos se configuran mediante registros en el DNS público de su dominio y permiten a los servidores de correo receptores (de terceros) verificar la legitimidad de los correos enviados por su organización.

1. SPF (Sender Protection Framework)

El SPF es el mecanismo más básico y antiguo.

- **Propósito:** Identificar cuáles son los servidores de correo autorizados para enviar mensajes en nombre de su dominio. Esto ayuda a evitar que un atacante utilice su dominio para enviar spam o correos maliciosos.
- **Mecanismo:** Se implementa mediante un registro de tipo **TXT** en su DNS público. Este registro lista las direcciones IP o nombres de host de todos los servicios (incluido Office 365, proveedores de marketing, etc.) que están permitidos para originar correo de su dominio.
- **Importancia en Defender:** Cuando un correo entra, Defender (o el servidor receptor) verifica si el servidor de envío está en la lista SPF del dominio remitente. Si falla, es una señal de alerta.

> Como nota detallista, debe tenerse **mucho cuidado** al activar políticas que rechacen correos por fallar el SPF. La realidad es que muchas empresas, incluso grandes, tienen registros SPF mal configurados, y rechazar automáticamente estos correos legítimos puede provocar problemas de comunicación con clientes o proveedores.

2. DKIM (DomainKeys Identified Mail)

DKIM aporta una capa de seguridad criptográfica.

- **Propósito:** Firmar digitalmente los correos electrónicos para que el receptor pueda verificar que el mensaje no ha sido alterado en tránsito y que realmente proviene del dominio que afirma ser.
- **Mecanismo:** La firma digital se genera utilizando una **clave privada** (gestionada por Office 365) y se verifica utilizando una **clave pública** que se publica en su DNS, generalmente bajo registros llamados `selector1` y `selector2`.
- **Importancia en Defender:** Microsoft Defender utiliza estas firmas para aumentar la confianza en los correos salientes y entrantes. Si un correo no está firmado digitalmente (DKIM desconocido) o la firma es inválida, se eleva su nivel de riesgo.

3. DMARC (Domain-based Message Authentication, Reporting, and Conformance)

DMARC es el protocolo de política y monitoreo que unifica el uso de SPF y DKIM.

- **Propósito:** Indica al servidor receptor qué acción debe tomar si un correo que afirma ser de su dominio **falla** las comprobaciones de SPF y/o DKIM.
- **Mecanismo (Política):** Se implementa mediante un registro **TXT** en el DNS, donde se define la política de acción:
  - **None (p=none):** No tomar ninguna acción (aceptar), pero se utiliza para monitorear.
  - **Quarantine (p=quarantine):** Marcar el correo como sospechoso y ponerlo en cuarentena.
  - **Reject (p=reject):** Rechazar completamente el correo.
- **Mecanismo (Reportes):** DMARC también incluye campos (`RUA` y `RUF`) que permiten a los servidores receptores enviar informes de vuelta a su organización. Estos informes (a menudo en formato XML) detallan si los correos enviados desde su dominio pasaron o fallaron las comprobaciones de SPF y DKIM.

> **Dato Didáctico:** La construcción del registro DMARC le permite al emisor decirle al receptor cómo comportarse. Esto es vital para proteger su identidad de posibles suplantaciones, ya que le asegura que si alguien más intenta usar su dominio de forma ilegítima, el correo será rechazado.

Gestión de Políticas de Correo en Defender

Dentro del portal de seguridad (Microsoft Purview), la administración utiliza las políticas de Defender para Office 365 para determinar cómo se interactúa con estos chequeos de autenticación:

1. **Políticas Antifishing:** Estas políticas pueden ser configuradas para ser más agresivas si los correos fallan SPF o DKIM. El administrador puede configurar umbrales de seguridad y activar funciones de inteligencia artificial para monitorear usuarios y dominios específicos susceptibles de ser suplantados (suplantación de usuarios internos).
2. **Configuración de Autenticación:** El administrador puede confirmar si DKIM está habilitado para el dominio a través de la sección de autenticación de correo.
3. **Cuarentena:** Los mensajes que fallan estos chequeos de autenticación y superan los umbrales de riesgo son colocados en cuarentena. Las políticas de cuarentena pueden ser ajustadas para dar acceso limitado a los usuarios estándar para revisar mensajes (solo vista previa), sin darles permiso para liberarlos, lo cual protege contra la liberación accidental de correos peligrosos.
4. **Simulaciones de Ataque:** Defender también facilita la creación de políticas para que ciertas IP de simulaciones de phishing sean ignoradas por los filtros normales, permitiendo a la organización probar

la resistencia de sus usuarios ante ataques reales.

\newpage

Capítulo 32: ### 1. Marco General de las Directivas de Correo

Todas las configuraciones de seguridad en Microsoft 365, incluyendo la protección del correo, se gestionan mediante **Directivas** (Policies). Estas directivas actúan sobre el correo **mientras está en tránsito** dentro de la plataforma Microsoft 365, antes de que llegue al buzón del usuario.

Mecanismo de las Directivas

1. **Directiva Estándar (Global):** Por defecto, siempre existe una directiva estándar o global que se aplica a toda la organización.
2. **Directivas Personalizadas:** El administrador puede crear nuevas directivas específicas (por ejemplo, "Directiva B" o "Directiva VIP") y asignarlas a usuarios o grupos concretos. Esto permite configuraciones de seguridad más estrictas para usuarios de alto perfil sin afectar al resto de la organización.
3. **Análisis de Configuración:** Herramientas como el *Configuration Analyzer* permiten revisar las políticas existentes y ofrecen recomendaciones activas para mejorar la postura de seguridad, a menudo sugiriendo que se reduzca el número de entradas de permitido a cero, lo que aumenta la protección.

2. Tipos Fundamentales de Directivas de Amenazas

Existen tres tipos principales de directivas que gestionan el flujo de correo: Antiphishing, Antispam y Antimalware.

A. Directiva Antiphishing (Antisuplantación de Identidad)

Se enfoca en proteger a los usuarios de correos que buscan suplantar la identidad de un remitente de confianza (interna o externa), siendo una defensa clave contra el compromiso de correo.

- **Configuración:** Permite activar un motor de Inteligencia Artificial (IA) para la detección automática de suplantación.
- **Usuarios Protegidos:** Se pueden especificar listas de usuarios o dominios que requieren una vigilancia y protección más exhaustiva debido a su alto riesgo de ser objetivo de suplantación.
- **Acciones de Protección:** El administrador define qué hacer con los mensajes detectados como suplantación: enviarlos a la **Cuarentena** o directamente a la carpeta de **Correo no Deseado** del usuario.
- **Indicadores de Seguridad:** Se pueden habilitar avisos visuales para el usuario, como mostrar un signo de interrogación o el texto "vía" cuando se detecte que el correo se envió usando una dirección distinta a la que afirma ser el remitente.

B. Directiva Antimalware (Antivirus)

Esta directiva gestiona el bloqueo de archivos maliciosos y virus.

- **Regla General:** Con el *malware* **"no se negocia"**. El comportamiento por defecto es eliminar o poner en cuarentena el adjunto malicioso.
- **Notificaciones:** Aunque el archivo sea eliminado, se puede configurar para que el administrador sea notificado de que un ataque de *malware* se intentó.
- **Filtro de Adjuntos Comunes (Common Attachment Filter):** Esta es una configuración crítica. Permite bloquear tipos de archivos que, aunque no contengan un virus conocido, son frecuentemente utilizados en ataques de ingeniería social o *ransomware*. Ejemplos de extensiones que se recomienda bloquear incluyen:
    - Archivos de *script* (.CMD, .BAT).
    - Accesos directos de Windows (.LNK).
    - Imágenes de disco (.ISO), utilizadas en ataques donde contienen archivos LNK para iniciar una intrusión.
    - Macros de Office.

C. Directiva Antispam (Anticorreo Masivo)

Gestiona el correo no deseado y los envíos masivos (*bulk* mail).

- **Umbrales de Correo Masivo:** Permite subir o bajar el umbral de puntuación para determinar qué tan estricto debe ser el filtro con el correo masivo.
- **Chequeos de Contenido:** El sistema puntúa negativamente a los correos que contengan elementos sospechosos, como URL que usan direcciones IP en lugar de nombres de dominio, o que provienen de dominios asociados a prácticas maliciosas.
- **Filtros Geográficos y Lingüísticos:** Es posible aumentar la puntuación de *spam* o incluso bloquear correos que provengan de países o que estén escritos en idiomas con los que la organización no trabaja habitualmente.

3. Directivas de Cuarentena (Policies on Quarantine)

Una funcionalidad moderna que permite al administrador definir cómo se gestionan los correos retenidos. Esta es crucial para controlar el acceso del usuario a los mensajes que podrían ser peligrosos.

- **Acceso Limitado:** Se pueden crear políticas de cuarentena que otorgan **acceso limitado** a los usuarios estándar ("usuario patata"). Esto les permite previsualizar el mensaje y solicitar su liberación, pero **no les permite liberar el mensaje por sí mismos**, evitando que accidentalmente liberen contenido malicioso.
- **Vista Previa y Borrado:** Los usuarios, dependiendo de la política, pueden previsualizar los mensajes, borrarlos de la cuarentena, o bloquear al emisor.
- **Notificaciones:** Se puede configurar la frecuencia con la que se envían notificaciones por correo a los usuarios informándoles sobre el contenido de su cuarentena (por ejemplo, una vez al día).

4. Directivas de Autenticación de Correo (SPF, DKIM, DMARC)

Aunque estos protocolos se configuran en el DNS, Microsoft Defender los utiliza para reforzar sus directivas de seguridad.

- **SPF (Sender Protection Framework):** El sistema más básico. Verifica que la dirección IP de origen del correo esté autorizada para enviar en nombre del dominio, buscando un registro TXT en el DNS público del remitente.

- **DKIM (DomainKeys Identified Mail):** Aporta autenticación criptográfica. Firma digitalmente el correo para que el receptor pueda verificar que el mensaje no ha sido manipulado en tránsito y que el remitente es legítimo. La clave pública se publica en el DNS.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Este protocolo unifica SPF y DKIM y permite al dominio emisor (por ejemplo, el suyo) indicar a los dominios receptores **qué acción deben tomar** si un correo falla las comprobaciones (ejemplo: **Reject**, **Quarantine**, o **None**).
    - *Reportes:* DMARC es también utilizado para solicitar informes detallados (RUA/RUF) de vuelta, que le permiten saber cómo su correo se ve desde la perspectiva de los servidores externos.

> **Nota de Experto:** Es fundamental, pero riesgoso, configurar políticas que rechacen correos basándose en fallos de SPF o DMARC, ya que muchas organizaciones no tienen estos registros configurados correctamente, lo que podría llevar al bloqueo de correos legítimos de clientes o proveedores. Las políticas de Defender para Office 365 permiten ajustar qué tan estrictos somos con estos fallos.