Reporte ENISA: Seguridad defensiva en Microsoft 365 y Azure

Práctica integradora

Cáceres Zapata, Kevin Luis

Índice

Resumen ejecutivo

Este reporte presenta una estrategia de seguridad defensiva aplicada a un tenant de Microsoft 365 y Azure de tamaño mediano ([aprox. 300-500]) siguiendo lineamientos de ENISA, NIST SP 800-63B y el marco MITRE ATT&CK.

Se identificaron tres riesgos principales:

1. Compromiso de identidad mediante phishing y abuso de cuentas válidas.
2. Exfiltración de información sensible a través de SharePoint, OneDrive y Teams.
3. Persistencia de atacantes mediante manipulación de roles y aplicaciones OAuth.

Para mitigarlos se recomiendan los siguientes controles prioritarios:

- Autenticación multifactor resistente a phishing con passkeys/FIDO2.
- Políticas de Conditional Access basadas en riesgo y dispositivo.
- Privilegios mínimos con administración Just-In-Time y Privileged Identity Management (PIM).
- Configuración segura de correo con Safe Links, Safe Attachments y anti-phishing.
- Protección de datos con etiquetas de sensibilidad y políticas DLP.

Los resultados esperados incluyen la reducción significativa de la probabilidad de compromisos de cuentas, mayor control sobre la exfiltración de datos y una capacidad de detección temprana reforzada mediante telemetría centralizada en Azure/M365.

Alcance y contexto

El alcance de este reporte se limita a un tenant de Microsoft 365 y Azure con aproximadamente 500 usuarios. La organización utiliza los siguientes servicios principales:

- **Azure Active Directory (Entra ID)** Como proveedor de identidad y control de acceso.
- **Exchange Online** Para correo electrónico corporativo.
- **SharePoint Online y OneDrive for Business** Para almacenamiento y colaboración de documentos.
- **Microsoft Teams** Como herramienta de comunicación y colaboración.
- **Azure Security y Defender for Office 365** Como capas de protección adicionales.

El contexto de amenaza considerado incluye actores externos avanzados (APT) con capacidad de realizar ataques de phishing, abuso de credenciales válidas, escalación de privilegios y exfiltración de datos en entornos cloud.

Marcos y estándares Internacionales

El marco MITRE ATT&CK se emplea para mapear tácticas y técnicas relevantes a este escenario.

El estándar NIST SP 800-63B se utiliza como guía para definir los niveles de autenticación y políticas de credenciales apropiadas.

Las recomendaciones que ENISA proporciona a las buenas prácticas y estilo de reporte.

Metodología

La elaboración del presente reporte se realizó siguiendo el enfoque estructurado:

1. **Identificación de activos y servicios críticos** En Microsoft 365 y Azure (identidad, correo, almacenamiento y colaboración).

2. **Análisis de riesgos** Basado en escenarios de amenazas relevantes y tácticas del marco MITRE ATT&CK.

3. **Revisión de estándares aplicables** NIST SP 800-63B (niveles de aseguramiento de autenticación), ENISA (buenas prácticas de ciberseguridad en la nube) y guías técnicas de Microsoft.

4. **Definición de controles de seguridad** En Entra ID/M365/Azure alineados con dichos estándares.

5. **Mapeo de cada control a técnicas ATT&CK y riesgos mitigados** Para asegurar trazabilidad.

6. **Evaluación del riesgo residual y priorización de acciones** Considerando balance entre seguridad y productividad.

Este enfoque garantiza que las recomendaciones no son genéricas, sino que están fundamentadas en marcos reconocidos y en la realidad operativa de un tenant mediano de Microsoft 365/Azure.

Hallazgos

El análisis inicial evidenció los siguientes puntos críticos en el entorno Microsoft 365/Azure evaluado:

- La autenticación actual se basa en contraseñas y en algunos casos MFA básico por SMS, lo cual no cumple con los requisitos de AAL2/AAL3 de NIST SP 800-63B.
- No existen políticas de acceso condicional consolidadas, lo que expone a la organización a accesos desde ubicaciones geográficas no confiables y a dispositivos no gestionados.
- La rotación y el control de identidades privilegiadas se realizan de forma manual, sin mecanismos de "Just-In-Time" ni "Privileged Identity Management".
- La telemetría disponible es limitada, con auditoría parcial de actividades en Exchange y SharePoint, lo que dificulta la detección temprana de técnicas ATT&CK como T1078 (Valid Accounts) o T1567 (Exfiltration Over Web Services).
- La configuración de "Defender for Office 365" se encuentra incompleta, con "Safe Links" y "Safe Attachments" deshabilitados en parte de los buzones.
- No se aplican etiquetas de sensibilidad ni políticas de "Data Loss Prevention" (DLP) en SharePoint, OneDrive y Teams, lo que incrementa el riesgo de exfiltración de información sensible.

En conjunto, estas brechas representan una superficie de ataque significativa para adversario que busquen comprometer identidades, mantener persistencia y exfiltrar datos en entornos de nube.

Análisis y mapeo MITRE ATT&CK

Tácticas y técnicas relevantes

Táctica	Técnica	ID MITRE	Relevancia en M365/Azure
Initial Access	Spearphishing Attachment	T1566.001	Envío de adjuntos maliciosos a usuarios de Exchange.
Initial Access	Spearphishing Link	T1566.002	Enlaces maliciosos en correos hacia O365.
Credential Access	Valid Accounts	T1078	Uso de credenciales robadas en Entra ID.
Credential Access	Password Spraying	T1110.003	Intentos masivos con contraseñas comunes.
Persistence	Account Manipulation	T1098	Creación/modificación de cuentas y roles en Azure AD.
Defense Evasion	Application Consent Abuse (OAuth)	T1098.003	Consentimiento malicioso en apps registradas.
Collection	Mail Items Accessed (Exchange Online)	T1114.002	Acceso a correos en buzones comprometidos.
Exfiltration	Exfiltration Over Web Services (OneDrive)	T1567.002	Descarga de documentos sensibles desde SPO/OD.

Controles defensivos propuestos y mapeo ATT&CK

- **Autenticación multifactor con FIDO2/passkeys**
  - Mitiga T1078 (Valid Accounts) y T1110.003 (Password Spraying).
- **Bloqueo de autenticación heredada (legacy protocols)**
  - Mitiga T1078 y T1110.003 al impedir ataques por POP/IMAP/EAS.
- **Privileged Identity Management (PIM) con Just-In-Time**
  - Reduce persistencia (T1098) y abuso de roles (T1098.003).
- **Políticas de Conditional Access basadas en riesgo y dispositivo**
  - Limitan accesos sospechosos desde ubicaciones no confiables (T1078).
- **Safe Links y Safe Attachments en Defender for Office 365**
  - Mitigan spearphishing con adjuntos (T1566.001) y enlaces (T1566.002).
- **Etiquetas de sensibilidad y DLP en SPO/OneDrive/Teams**
  - Reducen la probabilidad de exfiltración (T1567.002).
- **Activación de auditoría y telemetría extendida**
  - Permite detección temprana de T1078, T1098 y T1567.

NIST SP 800-63B

IAL, AAL, FAL y niveles objetivo

- **IAL (Identity Assurance Level)** Grado de certeza en la verificación de identidad de un usuario.
- **AAL (Authenticator Assurance Level)** Robustez de los mecanismos de autenticación.
- **FAL (Federation Assurance Level)** Protección de las aserciones de identidad en escenarios federados (ej. SSO).

Niveles propuestos para un tenant M365 mediano (500 usuarios):

Nivel	Descripción	Elección recomendada	Justificación
IAL	Verificación de identidad	IAL2	Verificación remota y documentación básica para empleados y contratistas.
AAL	Autenticación	AAL2 para todos los usuarios, AAL3 para administradores	MFA obligatorio (OTP + FIDO2). AAL3 para admins críticos usando passkeys resistentes a phishing.
FAL	Federación de identidad	FAL2	Tokens firmados con protección contra replay, adecuado para SSO en aplicaciones críticas.

Riesgos de elegir niveles inferiores: - IAL1: cuentas creadas sin validación suficiente → riesgo de identidades falsas.
- AAL1: contraseñas solas → vulnerabilidad frente a password spraying y phishing.
- FAL1: tokens sin protección → posibilidad de replay y robo de sesión.

Política de contraseñas conforme 63B

La política de contraseñas definida para el tenant debe alinearse con las recomendaciones de NIST SP 800-63B, evitando prácticas obsoletas y priorizando controles efectivos:

Requisitos mínimos: - Longitud mínima: 12 caracteres (NIST indica mínimo 8, se eleva a 12 por política interna).
- Permitir el uso de gestores de contraseñas y el copiado/pegado en campos de autenticación.
- Almacenamiento mediante algoritmos seguros de hashing (bcrypt, scrypt o Argon2 con sal aleatoria).

Prácticas a aplicar: - Verificar nuevas contraseñas contra listas de credenciales comprometidas, comunes o por defecto.
- Monitorear intentos de "credential stuffing" y alertar ante múltiples fallos de inicio de sesión.
- Bloquear pistas de contraseña ("password hints") y preguntas de seguridad triviales.

Prácticas a prohibir: - Rotación periódica obligatoria sin evidencia de compromiso.
- Complejidad forzada basada en reglas arbitrarias (ej. exigir mayúscula, número y símbolo obligatorios).
- Almacenamiento en texto plano o reutilización no controlada.

Justificación: Estas medidas se alinean con el principio de facilitar contraseñas largas y fáciles de recordar, pero resistentes a ataques de fuerza bruta. Al mismo tiempo, se evita la fatiga del usuario por cambios innecesarios y se incrementa la seguridad mediante la detección de credenciales comprometidas.

MFA, FIDO2/passkeys y cuentas break-glass

Autenticación multifactor (MFA): - Implementar MFA obligatorio para todos los usuarios.
- Adoptar **métodos resistentes a phishing**, en particular **FIDO2/passkeys** y **Windows Hello for Business**.
- Definir "Authentication Strengths" en Entra ID para aplicar MFA resistente en aplicaciones y roles críticos.

Cuentas privilegiadas: - Exigir AAL3 para administradores globales y cuentas con acceso a datos sensibles.
- Los administradores deben autenticarse preferentemente con passkeys o FIDO2 en lugar de SMS/OTP.

Cuentas break-glass: - Mantener dos cuentas de emergencia ("break-glass"), cloud-only y con contraseñas robustas (>20 caracteres, aleatorias).
- Estas cuentas deben estar **excluidas de las políticas de Conditional Access** para garantizar acceso en caso de caída del servicio de MFA.
- Monitorear y generar alertas inmediatas si alguna break-glass es utilizada.
- Las credenciales deben almacenarse fuera de banda (cofre físico o gestor seguro) y revisarse periódicamente.

Justificación:

El uso de MFA resistente a phishing mitiga ataques como **Password Spraying (T1110.003)** y **Valid Accounts (T1078)**, mientras que las cuentas break-glass aseguran continuidad operativa sin exponer el sistema a abusos indebidos.

Conditional Access propuesto

Se definen las siguientes políticas de Conditional Access para reducir riesgo sin afectar la productividad:

1. **Bloqueo de autenticación heredada (Legacy Authentication)**
   - Control: Bloquear POP, IMAP, SMTP AUTH y Exchange ActiveSync heredado.
   - Riesgo mitigado: ataques de Password Spraying y credenciales válidas.
   - ATT&CK: T1110.003 (Password Spraying), T1078 (Valid Accounts).
2. **MFA resistente a phishing para administradores**
   - Control: Exigir Authentication Strength = Phishing-resistant (FIDO2/WHfB) para roles Global Admin, Security Admin y Privileged Role Admin.
   - Riesgo mitigado: robo de credenciales y tokens.

- ATT&CK: T1078 (Valid Accounts), T1550 (Use of Web Session Cookie).

3. **Acceso condicionado por riesgo de inicio de sesión**
   - Control: Si el riesgo de inicio de sesión es mayor o igual a Medio → exigir MFA; si el riesgo de usuario es Alto → bloquear acceso.
   - Riesgo mitigado: accesos desde ubicaciones anómalas o ataques automatizados.
   - ATT&CK: T1078 (Valid Accounts), T1110 (Brute Force).
4. **Ubicaciones y dispositivos confiables**
   - Control: Requerir dispositivos compliant con Intune fuera de la red corporativa.
   - Riesgo mitigado: acceso desde BYOD o dispositivos comprometidos.
   - ATT&CK: T1557 (Adversary-in-the-Middle), T1078 (Valid Accounts).
5. **Restricciones de sesión en aplicaciones de Office 365**
   - Control: Limitar descarga/imprimir/copiar de documentos en SharePoint, OneDrive y Teams cuando se accede desde dispositivos no gestionados Riesgo mitigado: exfiltración de información sensible desde entornos no confiables. ATT&CK: T1567.002 (Exfiltration Over Web Services).

Telemetría y auditoría: logs y detecciones

Para una detección efectiva de amenazas en Microsoft 365 y Azure se recomienda habilitar y centralizar los siguientes registros:

Fuente de log	Descripción	Técnica ATT&CK detectada
Azure AD Sign-in logs	Registra todos los intentos de inicio de sesión, métodos de autenticación y ubicación.	T1078 (Valid Accounts), T1110.003 (Password Spraying)
Azure AD Audit logs	Cambios en roles, grupos y aplicaciones en Entra ID.	T1098 (Account Manipulation), T1098.003 (Consent Abuse)
Microsoft 365 Unified Audit Log	Actividad en Exchange, SharePoint, OneDrive y Teams.	T1566 (Phishing), T1567.002 (Exfiltration Over Web Services)
Exchange Online Message Trace	Flujo de correos, detección de spam/phishing, estado de políticas de protección.	T1566.001 (Spearphishing Attachment), T1566.002 (Spearphishing Link)
SharePoint/OneDrive file activity	Creación, descarga y compartición de archivos.	T1537 (Exfiltration to Cloud Storage), T1567.002 (Exfiltration Over Web Services)

Recomendaciones adicionales: - Centralizar estos registros en **Microsoft Sentinel** o en un SIEM externo (ej. Splunk).
- Definir alertas automáticas ante inicios de sesión anómalos, escalaciones de privilegios y descargas masivas de datos.
- Usar consultas KQL para hunting

DLP, clasificación y control de dispositivos

La protección de datos en Microsoft 365 debe implementarse mediante un enfoque combinado de clasificación, etiquetas de sensibilidad y políticas DLP:

- **Etiquetas de sensibilidad (Sensitivity Labels):**
  - Aplicación automática a documentos y correos según contenido sensible (ej. datos financieros, PII).
  - Permiten cifrado, restricción de reenvío y marcas visuales en documentos.
  - Asociadas a políticas de retención y protección en SharePoint, OneDrive y Teams.
- **Políticas de Data Loss Prevention (DLP):**
  - Previenen la salida de información crítica fuera de la organización.
  - Bloquean o advierten cuando un usuario intenta compartir datos sensibles mediante correo, Teams o almacenamiento en la nube.
  - Configuración específica para datos personales, financieros y de salud.
- **Control de dispositivos no gestionados:**
  - Uso de "App-enforced restrictions" en SharePoint y OneDrive.
  - Permite acceso web a documentos, pero bloquea la descarga, impresión o sincronización si el dispositivo no está gestionado por Intune.
  - Garantiza equilibrio entre colaboración y protección de la información.

Relación con MITRE ATT&CK: - Mitiga **T1537 (Exfiltration to Cloud Storage)** y **T1567.002 (Exfiltration Over Web Services)** al impedir la extracción masiva de archivos desde entornos no controlados.

Identidades de servicio y apps

Las identidades de servicio y las aplicaciones registradas en Azure AD representan un vector de riesgo si no se gestionan de forma adecuada. Para reducir este riesgo se recomiendan las siguientes prácticas:

- **Uso de identidades administradas (Managed Identities):**
  - Sustituir secretos estáticos por credenciales gestionadas por Azure.
  - Elimina la necesidad de almacenar contraseñas o keys en código.
- **Rotación periódica de secretos y certificados:**
  - En los casos donde sea necesario usar secretos, establecer rotación automática.
  - Priorizar certificados frente a contraseñas por su mayor seguridad.
- **Principio de privilegios mínimos:**

- Revisar y limitar los permisos de aplicaciones y servicios.
- Evitar el consentimiento excesivo a aplicaciones de terceros.
- Implementar revisiones periódicas de permisos en Entra ID.

- **Supervisión y auditoría:**
  - Habilitar logs de auditoría en Entra ID para cambios en aplicaciones y Service Principals.
  - Detectar creación de credenciales adicionales o consentimientos sospechosos.

Riesgos mitigados: - Abuso de aplicaciones OAuth para obtener persistencia (**T1098.003**).
- Uso indebido de cuentas de servicio con permisos excesivos (**T1078**).
- Filtración de secretos en repositorios (**T1552**).

Estas medidas fortalecen la postura defensiva en entornos con múltiples integraciones y automatizaciones.

Sección especial: APT elegido

Descripción del actor y motivación

El actor seleccionado es **APT29**, también conocido como *Cozy Bear* o *Midnight Blizzard*. Está vinculado al Servicio de Inteligencia Exterior de la Federación Rusa (SVR).

- **Motivación principal:** Espionaje cibernético a largo plazo, con especial interés en gobiernos, organismos diplomáticos, empresas tecnológicas y organizaciones internacionales.
- **Sectores objetivo:** Ministerios de relaciones exteriores, organismos gubernamentales, empresas de defensa, tecnología e instituciones de investigación.

  Este actor es relevante para Microsoft 365/Azure debido a campañas documentadas contra entornos en la nube, incluyendo el uso de phishing sofisticado, abuso de credenciales válidas y persistencia mediante aplicaciones OAuth y roles privilegiados.

TTPs mapeadas a ATT&CK

Las principales tácticas y técnicas atribuidas a APT29, según el marco MITRE ATT&CK, incluyen:

Táctica	Técnica	ID MITRE	Uso por APT29
Initial Access	Spearphishing Link	T1566.002	Campañas de correos electrónicos con enlaces maliciosos dirigidos a usuarios de O365.
Initial Access	Password Spraying	T1110.003	Intentos masivos de contraseñas débiles en cuentas de Entra ID.
Credential Access	Valid Accounts	T1078	Uso de credenciales robadas para acceder a portales de Azure AD.
Persistence	Account Manipulation (Roles/OAuth Consent)	T1098.003	Registro de aplicaciones maliciosas con permisos excesivos.

Táctica	Técnica	ID MITRE	Uso por APT29
Defense Evasion	Use of Web Session Cookie	T1550.004	Robo y reutilización de cookies de sesión para evadir MFA.
Collection	Mail Items Accessed	T1114.002	Acceso directo a buzones de Exchange Online comprometidos.
Exfiltration	Exfiltration Over Web Services	T1567.002	Descarga masiva de documentos desde OneDrive y SharePoint.

Vectores sobre Azure/M365

En el contexto de Microsoft 365 y Azure, APT29 ha sido observado empleando los siguientes vectores de ataque:

- **Phishing dirigido (Spearphishing O365):** Envío de enlaces y adjuntos maliciosos para robar credenciales de usuarios corporativos y acceder a Exchange Online (T1566.001, T1566.002).
- **Password Spraying:** Intentos masivos contra cuentas de Entra ID utilizando contraseñas débiles o filtradas (T1110.003).
- **Abuso de aplicaciones OAuth:** Registro de aplicaciones maliciosas en Azure AD y solicitud de consentimientos excesivos para acceder a correos y archivos (T1098.003).
- **Uso indebido de cuentas privilegiadas:** Obtención de credenciales de administradores globales para persistencia y escalación de privilegios (T1078, T1098).
- **Exfiltración en la nube:** Descarga de volúmenes significativos de documentos desde SharePoint Online y OneDrive for Business, a menudo desde dispositivos no gestionados (T1567.002).
- **Robo de tokens/cookies de sesión:** Reutilización de tokens web para evadir MFA y mantener acceso prolongado (T1550.004).

Controles defensivos (ENISA, NIST 63B, M365/Azure)

Para mitigar las tácticas empleadas por APT29 se recomiendan los siguientes controles:

- **Autenticación multifactor resistente a phishing**
  - Implementar passkeys/FIDO2 y Windows Hello for Business.

    - Alineado con NIST SP 800-63B AAL2/AAL3.
    - Mitiga T1078 (Valid Accounts) y T1110.003 (Password Spraying).
- **Bloqueo de autenticación heredada (Legacy Auth)**
    - Deshabilitar protocolos POP, IMAP y SMTP AUTH heredado.
    - Mitiga T1078 y ataques de password spraying.
- **Privileged Identity Management (PIM) con Just-In-Time**
    - Requerir aprobaciones para roles críticos y limitar la duración del privilegio.
    - Alineado con el principio ENISA de privilegios mínimos.
    - Reduce persistencia y abuso de roles (T1098, T1098.003).
- **Políticas de Conditional Access basadas en riesgo**
    - MFA reforzado en inicios de sesión de riesgo medio y bloqueo de riesgo alto.
    - Limita accesos desde ubicaciones anómalas o dispositivos no gestionados.
    - Mitiga T1078 y T1550.
- **Protección de correo en Defender for Office 365**
    - Safe Links y Safe Attachments habilitados en todos los buzones.
    - Mitiga spearphi

IoCs y señales en logs

La detección temprana de campañas asociadas a APT29 en entornos Microsoft 365/Azure puede apoyarse en los siguientes indicadores y señales en registros:

- **Azure AD Sign-in logs**
    - Inicios de sesión desde ubicaciones geográficas inusuales o imposibles (impossible travel).
    - Uso de protocolos heredados (POP/IMAP) en intentos de autenticación.
    - Multiplicidad de intentos fallidos → indicativo de Password Spraying (T1110.003).
- **Azure AD Audit logs**
    - Creación de nuevas aplicaciones con consentimientos excesivos.
    - Asignación no autorizada de roles privilegiados.
    - Cambios en políticas de acceso condicional o MFA.
- **Microsoft 365 Unified Audit Log**
    - Actividad sospechosa en Exchange Online: reglas de reenvío automático creadas sin autorización.
    - Acceso masivo a buzones de correo (MailItemsAccessed).
    - Descargas anómalas de archivos en SharePoint/OneDrive (T1567.002).
- **Message Trace en Exchange Online**
    - Picos inusuales de correos salientes desde cuentas comprometidas.

    - Envío de phishing interno.
- **IoCs externos**
    - IPs, dominios y hashes reportados por agencias (ej. CISA, ENISA, Microsoft Threat Intelligence) vinculados a campañas de APT29.

Estas señales deben integrarse en un SIEM (Microsoft Sentinel, Splunk u otro) para generar alertas automáticas y permitir hunting proactivo frente a adversarios avanzados.

Verificación de eficacia

Para asegurar que los controles implementados frente a APT29 mantienen su efectividad, se recomienda el siguiente plan de verificación:

- **Pruebas en modo "Report-only" de Conditional Access:**
    - Validar que las políticas no bloquean productividad antes de aplicarlas en modo activo.
    - Comprobar que MFA resistente se aplica correctamente a roles críticos.
- **Simulaciones de phishing (phishing simulations):**
    - Evaluar la capacidad de detección y respuesta de usuarios frente a correos maliciosos.
    - Medir efectividad de Safe Links y Safe Attachments en Defender for Office 365.
- **Pruebas de elevación Just-In-Time (PIM):**
    - Revisar que el flujo de solicitud, aprobación y expiración de privilegios se cumple sin bypass.
    - Asegurar que todas las actividades elevadas quedan registradas en auditoría.
- **Hunting queries en SIEM (Sentinel/Splunk):**
    - Ejecutar consultas periódicas para detectar intentos de password spraying, consentimientos sospechosos y descargas masivas.
    - Validar que alertas automáticas se disparan con umbrales definidos.

Revisión periódica de logs y alertas:
- Analizar cada mes patrones de sign-ins, cambios de roles y tráfico de correo.
- Contrastar con IoCs actualizados de APT29 publicados por CISA, ENISA o Microsoft.

Este plan permite comprobar de forma continua que los controles aplicados son eficaces, trazables y actualizados frente a amenazas avanzadas como APT29.

Riesgo residual y priorización

Tras la implementación de los controles propuestos, se identifican los siguientes riesgos residuales:

- **Zero-day en servicios de Microsoft 365/Azure**: vulnerabilidades desconocidas que aún no cuentan con parche.
- **Errores de configuración por parte de administradores**: políticas aplicadas de forma incompleta o con excepciones excesivas.
- **Acceso de usuarios externos/invitados (B2B)**: nivel de aseguramiento inferior frente a empleados internos.
- **Ingeniería social avanzada**: escenarios en los que el atacante logra engañar al usuario a pesar de controles técnicos.

Estos riesgos no se eliminan por completo, pero se mitigan mediante revisiones periódicas, actualización de IoCs y entrenamiento de usuarios.

Priorización de acciones inmediatas: 1. Implementar MFA resistente a phishing en todos los usuarios de alto impacto (administradores, finanzas, RRHH).
2. Bloquear protocolos de autenticación heredada y habilitar auditoría unificada.
3. Desplegar PIM con Just-In-Time para roles privilegiados.
4. Configurar DLP y restricciones de acceso en dispositivos no gestionados.
5. Asegurar Safe Links y Safe Attachments activos en toda la organización.

Con estas prioridades se maximiza la reducción del riesgo en el corto plazo, equilibrando seguridad y continuidad operativa.

Conclusiones

El presente reporte demuestra que la seguridad defensiva en un entorno Microsoft 365/Azure de tamaño mediano requiere un enfoque integral basado en estándares reconocidos (ENISA, NIST SP 800-63B) y en el mapeo de tácticas y técnicas de adversarios avanzados mediante MITRE ATT&CK.

La aplicación de controles como MFA resistente a phishing con FIDO2, bloqueo de autenticación heredada, acceso condicional basado en riesgo, Privileged Identity Management con Just-In-Time, protección del correo electrónico (Safe Links y Safe Attachments) y políticas de DLP con etiquetas de sensibilidad permiten reducir significativamente la probabilidad de éxito de ataques de grupos APT como APT29.

Si bien persisten riesgos residuales (zero-days, errores de configuración, ingeniería social), el diseño propuesto establece una base sólida de seguridad, con controles preventivos, detectivos y de respuesta. La telemetría centralizada y la verificación periódica de eficacia aseguran la mejora continua de la postura defensiva.

En conclusión, la organización mejora su resiliencia frente a amenazas avanzadas y establece un marco de protección trazable y alineado con buenas prácticas internacionales.

Referencias

- ENISA. *Cloud Security Guide for SMEs*. European Union Agency for Cybersecurity (2015)
- ENISA. *Cloud Computing – benefits, risks and recommendations for information security* (2009)
- NIST. *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B)*. NIST, 2020
- NIST. *Digital Identity Guidelines: Enrollment and Identity Proofing (SP 800-63A)*. NIST, 2020
- NIST. *Digital Identity Guidelines: Federation and Assertions (SP 800-63C)*. NIST, 2020
- MITRE ATT&CK®. *APT29 Adversary Group (G0016)*. MITRE Engenuity
- Microsoft. *Best Practices for Conditional Access in Azure Active Directory*. Microsoft Learn Docs
- Microsoft. *Manage emergency access accounts in Azure AD ("break-glass" accounts)*. Microsoft Learn Docs
- Microsoft. *Protect identities and enforce phishing-resistant MFA with Authentication Strengths*. Microsoft Learn Docs
- Microsoft. *Sensitivity labels and Data Loss Prevention in Microsoft 365*. Microsoft Purview Docs
- Microsoft. *About Safe Links in Microsoft Defender for Office 365*. Microsoft Docs
- Microsoft. *Safe Attachments in Microsoft Defender for Office 365*. Microsoft Docs
- CISA. *Advisory: Russian SVR Exploiting Microsoft 365 Environments*. Cybersecurity & Infrastructure Security Agency, 2023

Anexos técnicos

Anexo A — Tabla de trazabilidad de controles

Control propuesto	Riesgo mitigado	Técnica ATT&CK	Norma de referencia (NIST/ENISA)	Producto M365/Azure
MFA con FIDO2/passkeys	Uso de credenciales válidas	T1078, T1110.003	NIST SP 800-63B (AAL2/AAL3)	Entra ID
Bloqueo de autenticación heredada	Password spraying y accesos inseguros	T1110.003, T1078	ENISA Cloud Security Guidelines	Entra ID
PIM con Just-In-Time	Abuso de roles privilegiados	T1098, T1098.003	ENISA Principle of Least Privilege	Entra ID/Azure AD
Conditional Access basado en riesgo	Accesos desde ubicaciones anómalas	T1078, T1550	ENISA Risk-Based Authentication	Entra ID
Safe Links y Safe Attachments	Phishing y malware en correo	T1566.001, T1566.002	ENISA Secure Email	Defender for O365
DLP y etiquetas de sensibilidad	Exfiltración de datos	T1537, T1567.002	ENISA Data Protection	SharePoint/OneDrive
Auditoría de aplicaciones y consentimientos	Abuso de OAuth	T1098.003	ENISA Audit & Monitoring	Entra ID

Anexo B — Ejemplos de consultas KQL (Microsoft Sentinel)

1. Intentos de password spraying:

```
SigninLogs
| where ResultType == "50126"   // Credenciales inválidas
| summarize FailedLogins = count() by UserPrincipalName, IPAddress, bin(TimeGenerated, 1h)
| where FailedLogins > 20
```

2. Descargas masivas en OneDrive/SharePoint:

```
AuditLogs
| where Operation == "FileDownloaded"
| summarize Downloads = count() by UserId, bin(TimeGenerated, 1h)
| where Downloads > 100
```

3. Creación sospechosa de aplicaciones con permisos elevados:

```
AuditLogs
| where Operation == "AddServicePrincipal"
| where Result == "Success"
| summarize count() by AppId, UserId, bin(TimeGenerated, 1h)
```

Anexo C — Ejemplo de flujo PIM (Just-In-Time)

- Usuario solicita elevación a rol de administrador global.
- Debe proporcionar justificación y seleccionar duración máxima (ej. 1 hora).

- El sistema envía la solicitud para aprobación por parte de un supervisor.
- Una vez aprobado, se concede el privilegio temporal.
- Todas las acciones quedan registradas en logs de auditoría.

Anexo D – Ejemplo de política de Conditional Access (JSON simplificado)

```
{
  "conditions": {
    "users": {
      "includeRoles": [ "Global Administrator" ]
    },
    "locations": {
      "includeLocations": "All",
      "excludeLocations": "TrustedNetwork"
    }
  },
  "grantControls": {
    "operator": "OR",
    "builtInControls": [ "mfa", "compliantDevice" ]
  },
  "sessionControls": {
    "applicationEnforcedRestrictions": true
  }
}
```