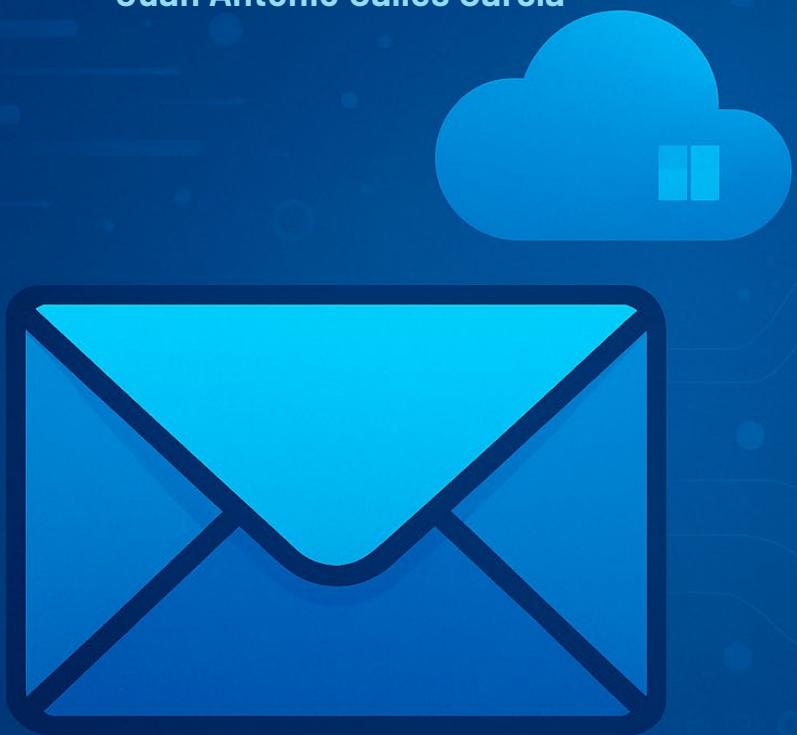


Análisis Forense de Correos Electrónicos en Office 365

1^a edición

(mayo 2025)

Juan Antonio Calles García



Índice

Índice.....	16
Prólogo	20
Motivación.....	24
Capítulo 1: Fundamentos del Análisis Forense Digital.....	30
Orientación hacia la prueba	33
Principios fundamentales	36
La evidencia digital	38
Normativa aplicable	42
Fases del análisis forense	46
El perfil del perito forense	56
La UNE 197001 y la estructura del informe pericial	61
Capítulo 2: Introducción a Microsoft 365	66
El ecosistema Microsoft 365	67
Registros de Auditoría Unificada de Microsoft 365	70
Los logs de Entra ID	74
Portales disponibles para la consulta de logs.....	75

Microsoft Purview eDiscovery (Content Search, Standard y Premium)	80
Sentinel y la retención de logs	83
Centro de Cumplimiento e Insider Risk	85
Nueva interfaz para Microsoft Purview	88
Capítulo 3: Marco Legal y Pericial.....	90
El análisis forense como medio de prueba.....	90
Marco normativo aplicable	91
Acceso legítimo al correo electrónico	95
Cesión de medios corporativos a empleados	97
Capítulo 4: Herramientas para el Análisis de Emails	100
Estructura y elementos clave de un email	100
Microsoft Outlook como visor forense.....	104
Microsoft Purview eDiscovery (Premium)	105
Aid4Mail.....	107
Editores de texto y visores	111
Riesgos del uso de plataformas web externas.....	113
Capítulo 5: Investigaciones en Microsoft Purview eDiscovery.....	116
Requisitos previos y configuración	118
Trazabilidad para la cadena de custodia	118
Electronic Discovery Reference Model.....	120
Microsoft Graph.....	139
PowerShell	140
Verificación de una cabecera por Graph	141

Automatización de tareas con PowerShell	142
Consideraciones legales y de trazabilidad	143
Reflexión sobre Purview eDiscovery	144
Capítulo 6: Análisis de Evidencias Exportadas.....	146
Contenido exportado desde Microsoft Purview	146
Apertura y análisis del archivo PST.....	148
Hallazgos y preparación del informe	151
Capítulo 7: Cadena de Custodia, Informe y Defensa	154
Fundamentos de la cadena de custodia	154
Trazabilidad dentro de Purview	156
Validez judicial de la cadena de custodia digital	157
Ejemplo de formulario de cadena de custodia.....	157
Redacción del Informe.....	158
Principios rectores del informe forense.....	159
Estructura del informe.....	160
Recomendaciones prácticas de redacción	162
Ratificación del informe en sede judicial	163
Capítulo 8: Cierre del Caso y Lecciones Aprendidas.....	166
Casos reales investigados con Purview	168
Capítulo 9: Las contrapericiales.....	174
Recomendaciones metodológicas.....	185
Objeciones frecuentes.....	187
Enfoque Jurídico-Procesal.....	195
Capítulo 10: Buenas prácticas en M365 previas a un incidente...	200

Configuración de Microsoft 365 con enfoque forense	203
Microsoft Sentinel y la convergencia SIEM/SOAR en la nube ..	207
Aplicación de la ISO/IEC 27040:2024.....	210
Conclusiones finales	214
Glosario	216
Referencias.....	232

Este libro constituye una guía práctica y exhaustiva sobre el análisis forense de correos electrónicos en entornos Microsoft 365, dirigida a peritos, auditores, profesionales de la ciberseguridad y a todo el personal del ámbito jurídico. A lo largo de sus 10 capítulos se abordan con profundidad todos los aspectos clave de una investigación forense digital: desde los fundamentos teóricos y el principio de Locard, hasta el uso de herramientas como Microsoft Purview eDiscovery, Outlook, PowerShell y Microsoft Graph API. El lector aprenderá a identificar, preservar, extraer y analizar evidencias digitales respetando la cadena de custodia, validando la integridad de los datos y redactando informes técnicamente sólidos y jurídicamente válidos, basados en estándares internacionales. Con numerosos ejemplos, escenarios reales y metodologías contrastadas, esta obra se convierte en una referencia esencial para abordar con rigor y eficacia cualquier incidente que afecte al ecosistema Microsoft 365 en general, y al correo electrónico en particular.

Título: Análisis Forense de Correos Electrónicos en Office 365

Autor: Juan Antonio Calles García

Tipo: Guía profesional

Temática: Ciencias Forenses y de la Computación

Nivel: Medio-Alto



978-84-09-72674-5



9 788409 726745