

EDS

INFORMÁTICA

Seguridad · Forense
Desarrollo Digital

ANÁLISIS FORENSE DIGITAL



CADENA DE CUSTODIA ✓

// EVIDENCIA DIGITAL · INFORMÁTICA FORENSE

EVIDENCIA DIGITAL

SIN TECNICISMOS

Nada se borra, todo se prueba

— MAGALI DOS SANTOS · CEO EDS INFORMÁTICA

Tabla de Contenidos

Sobre este libro	2
Tabla de Contenidos	4
Introduccion: Vivimos rodeados de evidencia digital — y la mayoría no lo sabe	11
Un mundo que graba todo	11
Por que este libro ahora	12
Quien deberia leer este libro.....	13
Capitulo 1 — Que es la evidencia digital?	15
Definicion y características únicas	15
Por que es diferente a cualquier otra prueba	15
1. Es extremadamente volátil	16
2. Es fácilmente duplicable sin pérdida de calidad	16
3. Puede ser alterada sin dejar rastros visibles.....	16
4. Tiene gran volumen y contexto	17
5. No tiene fronteras físicas.....	17
Tipos de evidencia digital	17
Evidencia almacenada.....	18
Evidencia de red	18
Evidencia volátil	18
Metadatos	18
Donde existe la evidencia digital sin que lo sepas.....	19
En tus dispositivos personales	19
En los sistemas corporativos.....	19
En la nube.....	20
En las redes sociales.....	20
En terceros que ni conoces.....	20
Capitulo 2 — Todo deja rastro	22
Huellas en dispositivos personales.....	22
El celular: la caja negra del siglo XXI	22
La computadora: un registro permanente de actividad	23
Sistemas corporativos: el ecosistema de datos empresariales.....	24
Correo electrónico corporativo	24
Sistemas de gestión empresarial (ERP, CRM)	25
Sistemas de control de acceso y videovigilancia.....	25
Mensajería instantánea y redes sociales.....	25
WhatsApp: el rey de la evidencia en LATAM	25

Telegram, Signal y otras apps de mensajería	26
Correo electrónico personal	27
Metadatos: el dato detrás del dato	28
Metadatos en imágenes y fotos	28
Metadatos en documentos de oficina	29
Metadatos en correos electrónicos	29
Logs, accesos y registros de actividad	29
Logs de servidores web	29
Logs de sistemas operativos.....	30
Logs de redes corporativas.....	30
Capítulo 3 — Nada se borra del todo.....	32
Como funciona realmente el borrado.....	32
La analogía del libro de biblioteca	32
Por qué la sobreescritura no es garantía	32
Formateo, borrado remoto y recuperación	33
El formateo: otro mito común	33
El borrado remoto: la ilusión del control total	34
Recuperación de datos: hasta donde puede llegar	34
El mito del modo incógnito	35
Que hace el modo incógnito (y que no hace).....	35
El mito de las VPN	36
Lo que una VPN hace	36
Lo que una VPN no hace	36
Que pasa con los datos de un empleado que se va	37
El problema del dispositivo corporativo.....	37
El problema del correo electrónico y los accesos	38
Los dispositivos personales: el territorio más complejo	38
Capítulo 4 — La cadena de custodia digital	40
Que es la cadena de custodia	40
Por qué la cadena de custodia es crítica en lo digital	41
Que rompe la cadena de custodia	41
Acceso al dispositivo o archivo original sin documentación.....	41
Transferencia sin verificación criptográfica	42
Almacenamiento inadecuado.....	42
Análisis sin herramientas forenses certificadas	43
El abogado que 'manipula' la evidencia para entenderla	43
Buenas prácticas desde el momento cero.....	43

1. No tocar el dispositivo o archivo original.....	43
2. Documentar el estado actual.....	43
3. Preservar el entorno	44
4. Llamar a un especialista antes de actuar	44
5. Registrar todo por escrito.....	44
Marco normativo en Latinoamerica	45
Argentina	45
Colombia	45
Mexico	45
Chile.....	46
Brasil.....	46
Capitulo 5 — Evidencia digital en el mundo empresarial.....	47
Fraudes internos, filtraciones y conflictos laborales.....	47
Fraude interno: el enemigo dentro	47
Indicadores digitales de fraude.....	48
Filtraciones de informacion: el activo mas valioso en riesgo.....	48
Conflictos laborales: donde la evidencia digital es mas frecuente	49
Auditorias digitales: que se busca y como	49
Tipos de auditoria digital en el contexto empresarial	50
El proceso de una auditoria digital bien hecha	50
Cuando llamar a un especialista y cuando ya es tarde	51
Los momentos criticos de intervencion.....	51
Cuando ya es tarde: los escenarios de no retorno	52
El rol del area de IT versus el perito externo.....	52
El area de IT: capacidades y limitaciones.....	52
El perito informatico forense: que aporta	53
Capitulo 6 — Como se obtiene correctamente	55
Extraccion forense versus captura de pantalla.....	55
La captura de pantalla.....	55
La extraccion forense	56
Herramientas de extraccion forense.....	57
Que hace (y que no hace) un perito informatico	57
Lo que hace un perito forense.....	57
Lo que NO hace un perito forense	58
Errores que contaminan la prueba antes de usarla	58
Error 1: Encender un dispositivo apagado	58
Error 2: Copiar archivos con herramientas convencionales	59

Error 3: Acceder a las cuentas con las credenciales del investigado.....	59
Error 4: Presentar capturas de pantalla sin corroboracion.....	59
Error 5: No preservar la evidencia de terceros a tiempo.....	60
Capitulo 7 — Errores frecuentes que cuestan caro	61
Errores del abogado	61
Error 1: Actuar sobre la evidencia antes de preservarla.....	61
Error 2: Confiar en capturas de pantalla como evidencia principal	61
Error 3: No solicitar medidas cautelares de preservacion a tiempo	62
Error 4: Subestimar los metadatos	62
Error 5: No anticipar la evidencia digital en la etapa de preparacion	63
Errores de la empresa	63
Error 1: Borrar los datos del empleado que se va por rutina	63
Error 2: Permitir que el area de IT conduzca investigaciones internas.....	63
Error 3: No tener politicas de uso de tecnologia documentadas	64
Error 4: No contratar ciberseguro con cobertura para incidentes forenses	64
Error 5: Confundir una investigacion forense con una auditoria de IT.....	65
Errores del area de IT	65
Error 1: Responder a un incidente de seguridad sin pensar en la evidencia	65
Error 2: No mantener logs con suficiente retencion	65
Error 3: Dar credenciales compartidas.....	66
Casos reales ilustrativos.....	66
Caso 1: El correo que se borro pero no desaparecio	66
Caso 2: Los metadatos que traicionaron la fecha	67
Caso 3: El WhatsApp que probo el acoso	67
Caso 4: El log que ubico al sospechoso	67
Lista de control para no fallar.....	68
Capitulo 8 — Plataformas digitales: guia especifica por herramienta	70
WhatsApp: el mas relevante en Latinoamerica.....	70
Arquitectura de datos de WhatsApp.....	70
Tipos de extraccion forense en WhatsApp	70
El estado de los 'ticks': evidencia en si misma.....	71
Grupos de WhatsApp como evidencia	72
Email: el veterano de la evidencia digital.....	72
Por que el email sigue siendo el rey de la evidencia corporativa	72
Cabeceras de correo: la huella invisible.....	73
Como se solicita evidencia de correo a los grandes proveedores	¡Error!
Marcador no definido.	

LinkedIn: evidencia profesional con peso legal	73
Que evidencia genera LinkedIn	73
Solicitud de datos a LinkedIn	74
Instagram y Facebook (Meta).....	74
El ecosistema Meta como fuente de evidencia	74
Mensajes directos de Instagram como evidencia	75
Contenido publicado y borrado	75
TikTok: la nueva fuente de evidencia	75
TikTok en el contexto forense	75
Google Workspace y Microsoft 365: evidencia corporativa en la nube	76
El administrador como primer recurso	76
eDiscovery: el proceso formal de obtencion de evidencia corporativa en la nube	76
Plataformas de videoconferencia: Zoom, Teams y Meet	77
Las reuniones virtuales como evidencia	77
La funcion de chat en reuniones: evidencia subestimada.....	78
Almacenamiento en la nube: Dropbox, Google Drive, OneDrive	78
La nube como extension del dispositivo	78
Sincronizacion y metadatos en la nube	79
Conclusion: El futuro de la evidencia digital	80
Inteligencia artificial y la crisis de autenticidad.....	80
Deepfakes y la autenticacion de contenido digital	81
Amenazas internas en la era de la nube	82
Blockchain como evidencia.....	82
La formacion como la mejor inversion.....	83
Glosario de Terminos Clave.....	85
A.....	85
B.....	85
C.....	85
D	86
E.....	86
F	86
H	87
I.....	87
L.....	88
M.....	88
P	88
R.....	88

S	89
V.....	89
W.....	89
Apendice A — Guia rapida segun tu perfil	91
Si sos abogado o asesora legal	91
Lista de verificacion para abogados.....	91
Si sos empresario o director de empresa.....	92
Lista de verificacion para empresas.....	93
Si sos una persona particular.....	93
Lista de verificacion para personas particulares	94
Apendice B — Preguntas frecuentes.....	95
Sobre los mensajes de WhatsApp.....	95
Un juez puede pedir los mensajes de WhatsApp directamente a la empresa?	95
Los mensajes borrados de WhatsApp son recuperables?	95
Una captura de pantalla de WhatsApp sirve como prueba?	96
Sobre el borrado de datos	96
Si borro mis mensajes y archivos antes de que empiecen los problemas, estoy protegido?.....	96
Si formateo el telefono antes de entregarlo, quedan mis datos?	96
Sobre la privacidad en el trabajo	97
Mi empleador puede revisar mis correos corporativos?	97
Puedo usar el modo incognito para evitar que IT vea mis actividades en la red corporativa?.....	97
Sobre las capturas de pantalla como evidencia.....	97
Puedo presentar capturas de pantalla de conversaciones como prueba en un juicio?	97
La otra parte puede presentar capturas de pantalla de mis conversaciones privadas?	98
Sobre las redes sociales.....	98
Las publicaciones en redes sociales sirven como evidencia?	98
Si borro una publicacion de Instagram, desaparece?.....	98
Apendice C — Protocolo de primer respuesta ante evidencia digital	99
Fase 1: Contencion inicial (primeros 15 minutos).....	99
1.1 Identificar y aislar el area del incidente.....	99
1.2 Documentar el estado inicial	100
1.3 Decidir: encendido o apagado	100
Fase 2: Notificacion y movilizacion (primeros 30 minutos).....	101
2.1 Notificar a las personas correctas	101

2.2 Establecer un perimetro de informacion.....	101
2.3 Preparar la informacion para el perito	102
Fase 3: Preservacion forense (una vez que el perito llega)	102
3.1 Briefing con el perito	102
3.2 Creacion de imagenes forenses.....	102
3.3 Documentacion de la cadena de custodia.....	103
Fase 4: Analisis y reporte.....	103
4.1 El analisis forense.....	103
4.2 El informe pericial.....	104
4.3 Preparacion para el proceso legal	104
Consideraciones especiales por tipo de incidente.....	104
Cuando el sospechoso es un empleado activo	104
Cuando hay una intrusion externa	105
Cuando la evidencia esta en la nube	105
Apendice D — Recursos y lecturas recomendadas	107
Organizaciones y certificaciones.....	107
ACFE — Association of Certified Fraud Examiners	107
IACIS — International Association of Computer Investigative Specialists	107
SANS Institute.....	107
EC-Council	107
Herramientas forenses de referencia	108
Autopsy.....	108
Cellebrite UFED	108
EnCase Forensic	108
Marco normativo: documentos de referencia	108
Ley Modelo de la CNUDMI sobre Comercio Electronico.....	108
Convenio de Budapest sobre Ciberdelincuencia	108
RFC 3227 — Guidelines for Evidence Collection and Archiving.....	109
Lecturas recomendadas	109
Recursos en espanol.....	109