Sobre los autores

Dos trayectorias complementarias al servicio de un mismo objetivo.

Este libro nace del trabajo conjunto de dos profesionales cuyos perfiles se complementan de forma natural: la seguridad ofensiva y operativa, por un lado, y la dirección de proyectos, el gobierno y el cumplimiento, por otro. Esa combinación —la de quien ataca para aprender a defender y la de quien ordena, planifica y lleva las medidas hasta su ejecución— es la que sostiene el enfoque práctico de estas páginas.

Juan Miguel Rosa Mondragón

Cofundador de Jaymon Security, S.L. y Comandante en la Unidad de Ciberdefensa del Ejército del Aire y del Espacio, acumula más de quince años de experiencia en guerra electrónica, enlaces tácticos de datos y ciberseguridad.

En el ámbito profesional ha dirigido operaciones de Red Team, auditorías de intrusión en modalidad caja negra, gris y blanca, actividades de inteligencia de amenazas (CTI/OSINT) e investigaciones forenses de incidentes de *ransomware* y APT, desempeñando asimismo funciones de perito forense judicial.

En el ámbito militar ha participado en ejercicios y misiones de la OTAN, entre ellos NATO Locked Shields —como líder del equipo de respuesta a incidentes (*blue team*) de sistemas Windows— y la misión Baltic Air Policing (Lituania). Es titular de una habilitación personal de seguridad del máximo nivel.

Su formación incluye dos másteres en ciberseguridad, ambos con matrícula de honor, y un programa superior universitario en ciberseguridad industrial. Entre sus certificaciones figuran CRTO II, eCPPT, eWPTX, eCDFP, CCSP y CDPP, además de acreditaciones en análisis forense (INCIBE) y en ciberinteligencia y fuentes abiertas (CCN).

Situado en el 1 % superior de la plataforma nacional Atenea del CCN-CERT, es autor de más de un centenar de artículos técnicos y formador en ciberseguridad e Inteligencia Artificial orientada a operaciones ofensivas.

Fernando Romero Urdiain

Cofundador y Director de Jaymon Security, S.L.

Ingeniero Superior en Informática por la Universidad Politécnica de Madrid (UPM) y *Project Management Professional* (PMP) certificado por el Project Management Institute (PMI), acumula más de veinte años de experiencia en la dirección de proyectos de tecnologías de la información, fundamentalmente en el sector público.

Su trayectoria profesional como consultor, jefe de proyecto, director técnico y asesor ministerial se ha caracterizado por el rigor técnico y una marcada orientación al cliente, abarcando el ciclo completo del proyecto: desde la detección de necesidades hasta la garantía de calidad en la entrega.

En el ámbito de la ciberseguridad, su especialización comprende el *pentesting*, el análisis de riesgos, el *compliance* y las auditorías de seguridad, complementada con formación específica en técnicas de intrusión controlada.

Aporta a esta obra una perspectiva imprescindible y con frecuencia desatendida: cómo se transforma una recomendación técnica

en un proyecto ejecutable, presupuestado y sostenible en el tiempo dentro de una organización real.

Sobre Jaymon Security

Ambos autores son cofundadores de Jaymon Security, S.L., empresa española de ciberseguridad especializada en ciberinteligencia, operaciones *red team*, *pentesting*, análisis forense digital y cumplimiento. Buena parte de los procedimientos, casos y lecciones aprendidas que recoge este libro proviene de la práctica diaria de sus proyectos con clientes de distintos sectores y tamaños.

Agradecimientos

Los autores queremos dejar constancia de nuestro sincero agradecimiento al suboficial de Transmisiones del Ejército de Tierra Francisco Javier Rosa Mondragón, cuya aportación ha enriquecido de forma notable el contenido de esta obra.

Su experiencia profesional en el ámbito de las transmisiones militares —un terreno donde la disponibilidad, la integridad y la seguridad de las comunicaciones no son conceptos teóricos, sino la diferencia entre el éxito y el fracaso de una operación— ha aportado a estas páginas una perspectiva de campo difícil de encontrar en la literatura técnica. Varios de los criterios y procedimientos que aquí se exponen se han beneficiado de su conocimiento y de su generosidad al compartirlo.

Gracias por el tiempo dedicado, por el rigor de sus observaciones y por recordarnos, una vez más, que detrás de toda buena defensa técnica hay siempre personas comprometidas con hacer bien su trabajo.

Fernando Romero Urdiain y Juan Miguel Rosa Mondragón.

Esta obra ha sido elaborada con el propósito de servir como guía operativa para profesionales y responsables de ciberseguridad en organizaciones. La información, los procedimientos y las referencias normativas que contiene están actualizados a la fecha de cierre de la edición. La rápida evolución del panorama de amenazas y de los marcos regulatorios aconseja contrastar siempre las recomendaciones con las fuentes oficiales vigentes en el momento de su aplicación.

Las marcas comerciales, productos y servicios mencionados a lo largo del libro pertenecen a sus respectivos titulares. Su mención tiene fines exclusivamente didácticos y descriptivos; no implica recomendación, patrocinio ni vinculación contractual con la editorial.

INTRODUCCIÓN

Del incidente inevitable a la organización preparada

Durante años, la conversación sobre ciberseguridad en la empresa giró en torno a una promesa implícita: que con suficiente inversión en tecnología era posible «estar seguro», entendido como un estado estable al que se llega y en el que uno permanece. La experiencia operativa ha desmentido esa promesa de forma contundente. La seguridad no es un estado, sino un proceso; y no se mide por la ausencia de incidentes —que ninguna organización puede garantizar—, sino por la capacidad de anticiparse a ellos, detectarlos pronto, responder con orden y recuperarse con el menor daño posible.

Este libro parte de esa premisa. No promete inmunidad, porque sería deshonesto hacerlo. Lo que ofrece es algo más útil: un procedimiento claro para cada uno de los incidentes que, según la evidencia acumulada en informes anuales como los de ENISA, INCIBE-CERT, el DBIR de Verizon o el Cost of a Data Breach de IBM, tienen mayor probabilidad de afectar a una organización en los próximos años. La diferencia entre la empresa que supera un incidente y la que naufraga en él rara vez está en el presupuesto: está en haber decidido, antes de que llegue el momento, qué se va a hacer y en qué orden.

Por qué un enfoque de ciclo de vida

Cada uno de los capítulos que siguen se estructura alrededor de una misma idea: un incidente no es un instante, sino una secuencia con un antes, un durante y un después. Por eso el tratamiento de los diecinueve casos se organiza en cuatro momentos alineados con las funciones del NIST Cybersecurity Framework 2.0 —*Identify*, *Protect*, *Detect*, *Respond* y *Recover*, bajo la nueva función transversal *Govern*.

- Acciones preventivas, que reducen la probabilidad de que el incidente ocurra o limitan su alcance si ocurre.
- Acciones correctivas, el procedimiento paso a paso para actuar mientras el incidente está en curso, cuando el tiempo apremia y las decisiones improvisadas son las que más caras se pagan.
- Acciones postincidente, la fase que más organizaciones descuidan y que convierte un episodio costoso en la inversión que evita el siguiente.
- Conclusiones, que destilan las tres o cuatro ideas que el lector debe llevarse de cada capítulo.

Esta estructura no es un artificio editorial. Responde a cómo se desarrollan realmente los incidentes sobre el terreno y a cómo se gestionan en la práctica del análisis forense y la respuesta a incidentes. Un procedimiento que solo cubre la prevención deja a la organización desarmada cuando la prevención falla y, antes o después, alguna capa falla.

Un marco común para un panorama fragmentado

El responsable de seguridad de hoy no se enfrenta a una única exigencia, sino a un mosaico de marcos técnicos y regulatorios que a menudo se perciben como cargas independientes: el RGPD y la LOPDGDD en materia de datos personales; la Directiva NIS2 y su transposición en España; el Reglamento DORA para el sector financiero; el Esquema Nacional de Seguridad en el ámbito público; ISO/IEC 27001:2022 como estándar de gestión; y MITRE ATT&CK como lenguaje común para describir las tácticas y técnicas del adversario.

Uno de los objetivos de este libro es mostrar que esos marcos no son compartimentos estancos, sino distintas perspectivas sobre un mismo problema. Un control bien diseñado —MFA resistente al *phishing*, segmentación de red, copias de seguridad inmutables,

cifrado de disco— responde simultáneamente a varias de estas exigencias. A lo largo de los capítulos se señala, en cada procedimiento, a qué marco responde cada medida, de modo que el lector pueda construir un único programa coherente en lugar de tantos proyectos aislados como normas le apliquen. Cabe advertir, no obstante, que el panorama regulatorio evoluciona con rapidez —la propia transposición de NIS2 en España sigue completándose mientras se cierra esta edición—, por lo que las recomendaciones deben contrastarse siempre con las fuentes oficiales vigentes en el momento de aplicarlas.

Cómo leer este libro

Aunque puede leerse de principio a fin, la obra está pensada como manual de consulta: cada capítulo es autosuficiente y puede abrirse directamente el día en que se produce el incidente correspondiente, o cuando la organización decide reforzar un control concreto. Los diagramas de flujo —preventivo, correctivo y postincidente— permiten seguir el procedimiento de un vistazo cuando no hay tiempo para releer el texto completo. El capítulo final, dedicado a la madurez, es la excepción y conviene dejarlo para el cierre: integra el resto en un modelo de evaluación y mejora continua que da unidad al conjunto.

Las técnicas de ataque se describen únicamente con la profundidad necesaria para comprender las defensas, nunca para reproducirlas. Las herramientas comerciales que se citan —EDR, SIEM, MDM, gestores de contraseñas y demás— aparecen a título descriptivo, como referencia concreta para la decisión, jamás como recomendación de compra.

Una última idea antes de empezar: la mayoría de los incidentes graves que hemos analizado a lo largo de estos años no se debieron a la sofisticación del atacante, sino a la ausencia de un procedimiento previamente acordado para escenarios perfectamente previsibles. Este libro existe para cubrir precisamente ese hueco. Nuestra aspiración es que llegue a sus manos antes de que llegue el incidente.

PRÓLOGO

Por qué este libro y para quién

La ciberseguridad ha dejado de ser una disciplina exclusiva de grandes corporaciones con departamentos especializados. El panorama de amenazas se ha democratizado tanto que hoy una pyme con quince empleados, un despacho profesional o una administración local pueden encontrarse, en cuestión de horas, ante un ataque de *ransomware*, una brecha de datos personales o un fraude por correo electrónico, sin saber exactamente qué hacer. Lo que diferencia a las organizaciones que superan estos incidentes de las que naufragan en ellos no es el presupuesto: es disponer, cuando más se necesita, de procedimientos claros, probados y compartidos por todo el equipo.

Este libro nace de esa observación. Durante veinticinco años trabajando en ciberseguridad —en auditorías, respuesta a incidentes, formación y diseño de programas defensivos— hemos comprobado que los errores más costosos no los cometen las organizaciones que carecen de tecnología, sino las que carecen de procedimientos: decisiones tomadas con prisa, comunicaciones contradictorias, evidencias borradas sin querer, plazos regulatorios incumplidos. Cada uno de esos errores podría haberse evitado con preparación previa.

Para quién está pensado

El libro se dirige a varios perfiles:

- Responsables de seguridad y CISO que buscan una referencia operativa para estructurar o revisar sus procedimientos.
- Equipos de TIC y administradores de sistemas que asumen funciones de ciberseguridad sin contar con un equipo dedicado.
- Consultores y auditores que necesitan un marco común para evaluar la madurez defensiva de sus clientes.
- Direcciones generales y comités ejecutivos que quieren entender qué hace —o debería hacer— su organización frente a las amenazas que protagonizan constantemente las noticias.
- Estudiantes y profesionales en formación que buscan un punto de partida operativo y aplicado, no exclusivamente teórico.

Qué encontrará el lector

El volumen reúne diecinueve casos prácticos —los más frecuentes según los informes anuales de ENISA, INCIBE-CERT, Verizon DBIR e IBM Cost of a Data Breach—, todos estructurados con el mismo esquema de cuatro momentos: acciones preventivas, acciones correctivas, acciones postincidente y conclusiones. Cada capítulo incorpora diagramas de flujo que permiten seguir el procedimiento de un vistazo cuando no hay tiempo para releer el texto completo. El capítulo final integra el conjunto en un modelo de evaluación, un análisis de brechas y un plan de mejora con horizonte de tres años.

Qué lo distingue

Tres rasgos diferencian este libro de otros en el mismo ámbito:

- Operativo, no académico. Cada capítulo responde a la pregunta «qué hacer hoy». Las técnicas de ataque se describen únicamente con la profundidad necesaria para comprender los controles defensivos, nunca para reproducirlas. Las herramientas que se citan —EDR, SIEM, MDM, gestores de contraseñas— aparecen a título descriptivo, jamás como recomendación de compra.
- Estructura uniforme. La misma plantilla en los diecinueve capítulos hace el libro consultable, no solo legible: puede abrirse directamente en el capítulo correspondiente el día en que se produce un incidente.
- Enfoque integrador. El capítulo final cierra el círculo con un modelo de madurez que da unidad a los dieciocho anteriores y los convierte en un programa.

Quienes lo hemos escrito esperamos que llegue a sus manos antes de que llegue el incidente.

Organización temática

Aunque cada capítulo es autosuficiente, el libro está organizado en cinco bloques temáticos que pueden leerse de forma independiente. Esta agrupación resulta útil tanto para la lectura secuencial como para la consulta puntual.

I. Ataques de impacto inmediato	1, 2, 5	*Ransomware*, exfiltración de datos y denegación de servicio. Incidentes que paralizan la operación o sustraen información de forma deliberada y a gran escala.
II. Identidad y autenticación	6, 7, 8, 14	*Phishing*, robo de credenciales, fuerza bruta y *Business Email Compromise*. La identidad como nuevo perímetro y el conjunto de ataques con mayor coste agregado a nivel mundial.
III. Medio físico y movilidad	9, 10, 11, 13, 16, 17	Ataques *man-in-the-middle*, dispositivos infectados, redes *wifi* públicas, dispositivos de *hacking* físico, *smartphones* y medios de almacenamiento. Amenazas que explotan la proximidad física o el trabajo fuera del perímetro corporativo.
IV. Factor humano e información corporativa	3, 12, 15, 18	*Software* no autorizado, amenazas internas, secuestro de redes sociales y prevención de pérdida de datos. Los riesgos vinculados al comportamiento humano y a la protección sistemática de la información.
V. Resiliencia y madurez	4, 19	Copias de seguridad y madurez en ciberseguridad. Los controles transversales que sostienen la capacidad de recuperación y la mejora continua del programa defensivo.

CAPÍTULO 1.
RANSOMWARE CON EXFILTRACIÓN DE DATOS

En este capítulo se describe cómo proceder en el caso de que nuestros sistemas hayan sido comprometidos por un *ransomware*, algo muy habitual en estos últimos tiempos. El ataque ya no se limita al cifrado de archivos: la modalidad estándar desde 2019-2020 incluye también la exfiltración previa de información sensible y la amenaza de publicarla, lo que se conoce como «doble extorsión». El ataque debe tratarse como lo que es, una intrusión en toda regla con cifrado al final, no un simple problema de virus.

Un *ransomware* se define como un tipo de programa dañino (*malware*) que secuestra los datos informáticos de aquellas máquinas infectadas y solicita un rescate económico —generalmente en criptomonedas (Bitcoin, Monero, etc.)— a cambio de quitar esta restricción y devolver a la víctima el acceso a los datos. En la modalidad de doble extorsión que hoy es la norma, los datos se exfiltran a la infraestructura del atacante antes de cifrarlos, y el rescate cubre dos cosas: obtener la clave de descifrado y evitar la publicación en los *leak sites* que estos grupos mantienen en la *dark web*.

Un ataque por *ransomware* supone a las empresas pérdidas económicas de cierta consideración, ya que de no tener planes de recuperación para poder retomar la actividad del negocio, se quedan paralizadas durante varias semanas, o incluso meses, hasta que recuperan el estado en el que estaban antes del ataque (si es que llegan a recuperarlo), sin perjuicio de los costes que puedan ocasionar las contrataciones de servicios externos —como pueden ser el análisis forense digital para esclarecer lo ocurrido y saber cuál ha sido la brecha de seguridad— o las multas que pueda conllevar la actuación de la Agencia Española de Protección de Datos (AEPD) en aplicación del RGPD.

Este capítulo aborda el asunto desde tres frentes complementarios: prevención (qué controles montar antes de que llegue el ataque), respuesta (cómo actuar cuando el ataque está en curso o ya consumado) y lecciones aprendidas. La estructura se alinea con las funciones del NIST Cybersecurity Framework 2.0 (Govern, Identify, Protect,

Detect, Respond, Recover), con los controles de la norma ISO/IEC 27001:2022, con el Esquema Nacional de Seguridad (Real Decreto 311/2022) y con la Directiva NIS2 transpuesta en España por el Real Decreto-ley 7/2025.

1. CARACTERIZACIÓN DEL ATAQUE

1.1. ¿Cómo es un ataque de *ransomware*?

El orden de ataque de un *ransomware* moderno con doble extorsión generalmente es el siguiente:

1

Acceso inicial. El sistema víctima se infecta. Esto puede ocurrir por varias vías: por explotación del protocolo RDP de escritorio remoto debido a una mala configuración de seguridad del servicio expuesto, por *phishing* con adjunto malicioso o enlace a una descarga *drive-by*, por instalación de *software* pirata, por explotación de un servicio expuesto sin parchear (VPN, MOVEit, Fortinet, Citrix, ManageEngine), o por un *insider* que tiene acceso físico a un equipo desbloqueado y le instala el *ransomware* mediante un *BadUSB*.

2

Persistencia y reconocimiento. El atacante establece persistencia (creación de cuentas, tareas programadas, abuso de PsExec, PowerShell, WMI) y reconoce la red interna mediante herramientas como BloodHound, ADRecon, Advanced IP Scanner. En esta fase se identifican los activos de mayor valor: controladores de dominio, servidores de archivos, repositorios de código, servidores de *backup*.

3

Movimiento lateral y escalada. Mediante credenciales obtenidas con Mimikatz, LSASS *dumping*, DPAPI o *Kerberoasting*, el atacante pivota a otras máquinas de la red y escala privilegios hasta comprometer Active Directory.

4

Exfiltración previa al cifrado. Antes de cifrar nada, el atacante exfiltra información sensible hacia infraestructura propia o a servicios *cloud* legítimos (MEGA, OneDrive personal, Dropbox) que se mimetizan en el tráfico saliente normal. Esta fase puede durar días o semanas y es la más silenciosa del ataque.

5

Cifrado masivo. Una vez exfiltrada la información, el *ransomware* se ejecuta en el sistema víctima, trata de cifrar todos los archivos del equipo y posteriormente —paralelamente— pivota hacia el resto de los equipos que estén interconectados. De esta manera, el *ransomware* puede llegar a comprometer una organización empresarial al completo realizando movimientos horizontales (pivotando) y verticales (escalando privilegios). Antes del cifrado se eliminan las copias de Volume Shadow Copy y se desactiva el antivirus.