FECHA	25 de mayo de 2026
ASUNTO	Documentación técnica – Ransomware: Qué es, cómo funciona y cómo defenderse
AUTOR	D. Ignacio Valderrama, INFORMATICA LOS LLANOS SL

Ransomware — Qué es, cómo funciona y cómo defenderse

El ransomware es un tipo de malware que **cifra los archivos de la víctima y exige un rescate económico** a cambio de la clave de descifrado. Es la amenaza más devastadora para una micropyme porque puede paralizar completamente la actividad en cuestión de minutos y los daños son frecuentemente irreversibles.

El nombre combina *ransom* (rescate) y *software*.

Por qué es especialmente peligroso para micropymes

Las grandes empresas tienen equipos de respuesta, backups robustos y seguros específicos. Las micropymes habitualmente no tienen ninguna de las tres cosas, lo que las convierte en objetivos atractivos: suficiente dinero para pagar y pocas defensas.

Según datos del INCIBE, más del **70% de los ataques de ransomware** en España afectan a pymes y micropymes. El rescate medio exigido a pequeñas empresas oscila entre **5.000 y 50.000 euros**, pero el coste real del incidente — incluyendo tiempo de inactividad, recuperación y reputación — suele ser muy superior.

Cómo funciona un ataque de ransomware

El ataque sigue habitualmente estas fases:

Entrada → Persistencia → Reconocimiento → Cifrado → Extorsión

Fase 1 — Entrada El atacante accede al sistema mediante alguno de estos vectores:

Vector	Cómo ocurre
Phishing	Empleado abre adjunto malicioso o hace clic en enlace
Credenciales robadas	Contraseña débil o reutilizada, sin MFA
RDP expuesto	Escritorio remoto accesible desde internet sin protección
Vulnerabilidad sin parchear	Software desactualizado con fallo de seguridad conocido
Credenciales robadas	Contraseña débil o reutilizada, sin MFA
RDP expuesto	Escritorio remoto accesible desde internet sin protección
Vulnerabilidad sin parchear	Software desactualizado con fallo de seguridad conocido
Proveedor comprometido	El atacante entra a través de un tercero con acceso

Fase 2 — Persistencia El malware se instala de forma que sobreviva a reinicios y pasa desapercibido el mayor tiempo posible.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Fase 3 — Reconocimiento Antes de cifrar, el atacante explora la red para identificar todos los sistemas accesibles, las copias de seguridad y los datos más valiosos. Esta fase puede durar días o semanas.

Fase 4 — Cifrado En cuestión de minutos, el ransomware cifra todos los archivos accesibles: documentos, bases de datos, correos, copias de seguridad conectadas. El usuario ve sus archivos renombrados con una extensión desconocida y aparece una nota de rescate.

Fase 5 — Extorsión El atacante exige el pago, habitualmente en criptomoneda, a cambio de la clave de descifrado. Los grupos más sofisticados aplican además **doble extorsión**: amenazan con publicar los datos robados si no se paga.

Ejemplo real adaptado a micropyme

Lunes, 9:15h. Una empleada de una gestoría de 4 personas recibe un correo que simula ser de la Agencia Tributaria con un PDF adjunto titulado *"Requerimiento_AEAT_2024.pdf"*. Lo abre.

Lunes, 9:16h. El archivo ejecuta un script oculto que descarga el ransomware en segundo plano. El antivirus no lo detecta porque es una variante nueva.

Lunes, 9:17h — Miércoles 11:00h. El malware permanece silencioso durante 44 horas, explorando la red local. Encuentra el NAS donde están los backups, que está montado como unidad de red. Encuentra el servidor con las carpetas de clientes. Encuentra el equipo de la gerente.

Miércoles, 11:01h. Comienza el cifrado. En 8 minutos están cifrados 47.000 archivos en cuatro equipos y el NAS.

Miércoles, 11:09h. Aparece en todos los equipos una pantalla con la nota de rescate: *"Todos tus archivos han sido cifrados. Paga 12.000€ en Bitcoin en 72 horas o los publicaremos."*

Resultado: tres semanas de inactividad parcial, pérdida de datos de los últimos 3 días (el backup del NAS también fue cifrado), coste de recuperación de 8.000€ con un especialista externo, notificación a la AEPD por brecha de datos personales de clientes.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

El problema de las copias de seguridad conectadas

El ejemplo anterior ilustra el error más crítico: **el backup estaba montado como unidad de red**, accesible desde los mismos sistemas que el ransomware cifró. Esto inutiliza la principal línea de defensa.

Para que una **COPIA DE SEGURIDAD** sea efectiva contra el ransomware debe cumplir al menos una de estas condiciones:

Condición	Por qué protege
Offline	Disco desconectado físicamente después de la copia
Inmutable	El servicio cloud no permite modificar ni borrar archivos durante un periodo definido
Cuenta separada	Credenciales distintas, inaccesibles desde los sistemas de producción
Air-gapped	Completamente aislado de la red, sin conexión posible

¿Se debe pagar el rescate?

Es la pregunta que toda micropyme se hace cuando ocurre. La respuesta es **no**, por varias razones:

- **No hay garantía** de recibir la clave de descifrado tras el pago
- **Financia** a organizaciones criminales y perpetúa el modelo de negocio
- **No elimina** el malware ni cierra la vulnerabilidad de entrada
- En algunos países y con ciertos grupos, **puede ser ilegal** (si están en listas de sanciones)
- Pagar convierte a la empresa en un objetivo conocido como **pagador**, aumentando el riesgo de nuevos ataques

La única defensa real es tener backups correctos y actualizados.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Medidas de prevención para micropymes

Organizadas de mayor a menor impacto:

Críticas — sin estas nada más importa:

Medida	Por qué
Backups offline o inmutables verificados	Es la única recuperación posible si todo lo demás falla
MFA en todas las cuentas	Bloquea el acceso con credenciales robadas
No exponer RDP a internet	Elimina uno de los vectores de entrada más explotados
Formación contra phishing	Reduce la probabilidad de ejecución del vector más frecuente

Importantes — reducen significativamente el riesgo:

Medida	Por qué
Mantener software actualizado	Cierra vulnerabilidades conocidas y explotadas activamente
Antivirus/EDR actualizado	Detecta variantes conocidas antes de que ejecuten
Principio de mínimo privilegio	Limita el alcance del cifrado si un usuario es comprometido
Segmentación de red	Evita que el ransomware salte de un equipo a toda la red
Filtrado de adjuntos en el correo	Bloquea los vectores de entrada más comunes

Qué hacer si el ransomware ya ha atacado

Siguiendo el procedimiento de incidentes ya desarrollado, las acciones específicas para ransomware son:

Primeros 5 minutos — contención:

1. Desconectar de la red todos los equipos afectados (cable de red y WiFi) **SIN APAGARLOS (*)**
2. Identificar qué equipos están cifrados y cuáles no
3. Desconectar físicamente los soportes de backup si aún no han sido cifrados
4. No intentar descifrar nada todavía

(*) ¿Por qué no apagar? Apagar puede destruir evidencias en memoria RAM que podrían ayudar a identificar la variante y encontrar una solución de descifrado. Solo se apaga si no hay otra opción. Detallado al final del documento.

Primeras horas — evaluación:

- Identificar la variante del ransomware (la nota de rescate suele indicarlo)
- Consultar **No More Ransom** (*nomoreransom.org*), proyecto europeo con herramientas gratuitas de descifrado para variantes conocidas
- Contactar con INCIBE (017) para orientación

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

- Evaluar el estado de las copias de seguridad
- Notificar a gerencia y activar el plan de comunicación

Primeras 72 horas — obligaciones legales:

- Si hay datos personales afectados, notificar a la AEPD antes de que se cumplan las 72 horas desde el conocimiento del incidente
- Documentar todo: qué sistemas, qué datos, desde cuándo, qué acciones se han tomado

Recuperación:

- Reinstalar el sistema operativo en los equipos afectados desde cero (no restaurar sobre el sistema infectado)
- Restaurar datos desde la copia de seguridad más reciente verificada
- Identificar y cerrar el vector de entrada antes de reconectar a la red
- Verificar que no queda malware en los equipos no afectados

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Recurso clave: No More Ransom

nomoreransom.org es un proyecto impulsado por Europol, la Policía Nacional Holandesa y empresas de ciberseguridad. Ofrece:

- Herramientas gratuitas de descifrado para más de 160 variantes de ransomware
- Identificación de la variante a partir de la nota de rescate o un archivo cifrado
- Disponible en español

Es el primer sitio al que acudir antes de considerar cualquier otra opción.

Integración en el plan director

Entregable	Cómo se integra
Registro de riesgos	R-006: ransomware sobre sistema de backup como riesgo alto
Plan de tratamiento	T-006: política de backup 3-2-1 con copias offline o inmutables
Procedimiento de incidentes	Fase 3 de contención: desconexión inmediata de red sin apagar
Procedimiento de backups	Sección 9: copias en cuenta separada, inaccesibles desde producción
Política de uso aceptable	Sección 4: no abrir adjuntos no solicitados
Formación del personal	Módulo específico de reconocimiento y reacción ante ransomware

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Ampliación — Por qué NO apagar un equipo infectado por ransomware

Cuando alguien ve la pantalla de rescate, el instinto natural es apagar el equipo inmediatamente. Es una reacción lógica: si lo apago, paro el daño. Sin embargo, en la mayoría de los casos **apagar es un error** que puede dificultar o imposibilitar la recuperación.

Razón 1 — La RAM contiene evidencias críticas

Cuando el ransomware está ejecutándose, mantiene en la **memoria RAM** del equipo información que desaparece en el momento en que se apaga:

Qué hay en RAM	Para qué sirve
La clave de cifrado activa	En algunos casos permite descifrar sin pagar
El proceso malicioso en ejecución	Permite identificar la variante exacta
Conexiones de red activas	Revela el servidor de mando y control del atacante
Archivos temporales del malware	Puede contener fragmentos del código original

Un especialista forense puede volcar la memoria RAM del equipo encendido y extraer esta información. Si se apaga, se pierde para siempre.

Razón 2 — Algunos ransomware tienen solución, pero solo con el equipo encendido

Ciertas variantes de ransomware tienen fallos en su implementación del cifrado. Los investigadores de seguridad han desarrollado herramientas que pueden aprovechar esos fallos para recuperar los archivos, pero algunas de esas herramientas requieren que el proceso malicioso siga activo en memoria para funcionar.

El proyecto **No More Ransom** ha logrado así recuperar datos de cientos de miles de víctimas de forma gratuita.

Razón 3 — El cifrado puede haber terminado ya

Otro motivo para no apagar es que en muchos casos **el cifrado ya ha concluido** cuando aparece la nota de rescate. El ransomware moderno cifra a gran velocidad: puede procesar decenas de miles de archivos en pocos minutos.

Apagar el equipo en ese momento no deshace nada. Solo destruye las evidencias que podrían ayudar a la recuperación.

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

Entonces, ¿cuándo sí se apaga?

Apagar el equipo tiene sentido en estas situaciones concretas:

Situación	Motivo
El cifrado está claramente en curso y hay archivos críticos aún no cifrados	Cortar el proceso puede salvar algo
No hay ningún especialista disponible y el equipo sigue propagando el malware por la red	Priorizar contención sobre evidencias
El equipo no puede desconectarse de la red de otra forma	Caso extremo sin alternativa

En todos los demás casos, la prioridad es **desconectar de la red** manteniendo el equipo encendido. Desconectar de la red detiene la propagación y la comunicación con el servidor del atacante, sin destruir las evidencias en memoria.

Ignacio Valderrama
Colegiado 3120021W CPITINA

Estella, a 25 de mayo de 2026

Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com