Ransomware V3

entender el ataque antes de que sea demasiado tarde

07:30 — encuentras un mensaje de cifrado.
¿Qué haría hoy su organización?

Operaciones
vuelve al papel

Finanzas
no puede facturar

Clientes
empiezan a llamar

Directorio
pregunta cuánto dura

Ejemplos reales de mensajes de cifrado

La resiliencia empieza antes del incidente.

Primer hallazgo visible: la nota de rescate

Lo primero que ve la organización suele ser un mensaje de cifrado, temporizadores y una exigencia de pago.

Ejemplo 1 — temporizador y pago

Ejemplo 2 — amenaza y cuenta regresiva

Ejemplo 3 — portal de rescate

Cifrado de archivos

Los datos quedan inaccesibles y en manos del atacante.

Interrupción operativa

Se detienen procesos críticos y servicios clave.

Presión de tiempo

Los temporizadores buscan forzar decisiones apresuradas.

Extorsión económica

Exigen pagos elevados bajo amenaza de pérdidas mayores.

El mensaje visible es solo el último síntoma: el ataque comenzó mucho antes.

TRAYECTORIA DEL DISERTANTE

Ricardo Rodríguez

CISO • Negofin S.A.E.C.A.

- Magíster en Ciberseguridad por la Universitat de Barcelona
- Especialista en cifrado • EC-Council Certified Encryption Specialist v3
- 12+ años en ciberseguridad, riesgo tecnológico y prevención de fraude
- Experiencia en sector financiero y fintech
- OWASP Paraguay • liderazgo y comunidad
- LinkedIn: linkedin.com/in/ricardorrd

EMPRESAS Y COMUNIDAD

NegoFiN S.A.E.C.A. | ueno bank | itaú | OWASP PARAGUAY

¿Qué está pasando?

Ransomware explicado para negocio, riesgo y tecnología.

COMPRENSIÓN

Ransomware es un secuestro digital de la capacidad de operar.

Cifrado
bloquea archivos y sistemas

Robo de datos
expone información sensible

Extorsión
presiona con pago o publicación

Interrupción
detiene procesos críticos

El malware puede ser técnico; el impacto **siempre es de negocio.** >>>

Ransomware moderno

MODELO

Ya no significa solamente cifrar archivos.

1. **Intrusión**
   credencial o exploit
2. **Persistencia**
   mantener acceso
3. **Lateralidad**
   moverse adentro
4. **Privilegios**
   tomar control
5. **Exfiltración**
   robar datos
6. **Cifrado**
   interrumpir
7. **Extorsión**
   presionar

Doble extorsión

cifrado + amenaza de publicar datos

Triple extorsión

cifrado + datos + presión a clientes/proveedores

El atacante estuvo dentro antes del incidente

REVELACIÓN

El cifrado es el momento visible; la preparación ocurrió antes.

La organización tardó segundos en ver el cifrado.
El atacante necesitó semanas para prepararlo.

Cómo entra —

ENTRADA

Principales vectores explicados sin exceso técnico.

Credenciales
usuarios o VPN válidos

Phishing
engaño para capturar acceso

Vulnerabilidades
servicios expuestos sin parche

Accesos remotos
RDP/VPN mal protegidos

Terceros
proveedores como puerta lateral

Dispositivos
endpoint o móvil comprometido

No necesitan “hackear todo”: **muchas veces les alcanza una credencial válida y tiempo suficiente.**

Métricas clave de ransomware 2026

Mundo, Latinoamérica, costos de recuperación y variantes dominantes

1 Panorama global 2026

2.122
víctimas publicadas en sitios de filtración en Q1 2026

71%
de las víctimas concentradas en el Top 10 de grupos

Qilin
lidera con 338 víctimas reportadas

La actividad se mantiene en niveles históricamente altos.

2 Latinoamérica bajo presión

3.149
ataques semanales por organización

+13%
interanual

Región más atacada en mayo 2026

La presión regional crece más rápido que la madurez defensiva.

3 Costo e impacto

USD 4,99 M
Costo promedio global de una brecha

USD 1,7 M
Costo promedio de recuperación ransomware

USD 769 mil
Pago mediano de rescate

Impacto principal: indisponibilidad operativa y pérdida de negocio

El costo mayor no es el rescate: es la interrupción del negocio.

4 Tiempo de recuperación e impacto operativo

Minutos–horas	4–24 h	24–72 h	Días–semanas
detección	contención inicial	restauración de servicios críticos	normalización total

Sin BIA (Análisis de Impacto al Negocio), PCN (Plan de Continuidad del Negocio), PCNT (Plan de Contingencia Tecnológica) y backups probados, el tiempo real se extiende.

5 Principales variantes / grupos 2026

1	2	3	4	5	6
Qilin	**The Gentlemen**	**LockBit 5.0**	**Akira**	**Cl0p**	**Medusa**
liderazgo sostenido	grupo emergente	regreso con fuerza	alto impacto en sectores con downtime costoso	campañas masivas por explotación	doble extorsión; foco actual por advisory IC3/CISA

2026 confirma una tendencia: **menos actores dominan más impacto,** y el verdadero costo se mide en **indisponibilidad, recuperación y gobernanza.**

Fuentes: Check Point Research Q1 2026 • IBM Cost of a Data Breach 2026 • Sophos State of Ransomware 2026 • IC3/CISA Medusa 2026

Gobernanza, BIA y resiliencia

La resiliencia no se improvisa: se gobierna, se mide y se prioriza.

DECISIÓN

1. GOBERNANZA

- **Directorio / Comité** — supervisión y aprobación estratégica
- **CISO / Seguridad** — estrategia, gobierno, riesgos y desempeño
- **Dueños de proceso** — ejecutan y son dueños de los controles

3 LÍNEAS DE DEFENSA

1. **1ª Operación** — ejecuta y opera controles
2. **2ª Riesgo / Seguridad** — define, asesora y monitorea
3. **3ª Auditoría** — evalúa de forma independiente

2. BIA EJECUTIVO

Proceso	Owner	Proveedores / terceros	Herramientas / sistemas	Criticidad	Impacto al negocio	Costo por indisponibilidad	RTO	RPO
Ventas	Gerencia Comercial	CRM Cloud, pasarela de pagos	Salesforce, Outlook, Power BI	Alta 🔴	Pérdida de ventas y atención	USD 120K–200K por día	4 h	15 min
Compras / Abastecimiento	Gerencia de Compras	Bancos, ERP, proveedores críticos	SAP / ERP, portal de compras	Media-Alta 🟠	Quiebre de stock y retrasos	USD 60K–100K por día	8 h	1 h
Facturación / Cobranzas	Gerencia Financiera	Clientes, ERP financiero	ERP financiero, facturación electrónica	Media-Alta 🟠	Retraso de ingresos y caja	USD 40K–80K por día	12 h	4 h
Operaciones	Gerencia de Operaciones	Proveedores, logística, subcontratistas	Core operativo, BI, SharePoint	Alta 🔴	Paralización operativa y sobrecostos	USD 150K–300K por día	8 h	1 h

3. PCN / PCNT

- **escenarios críticos** — identificación y priorización
- **responsables** — roles y contactos clave
- **canales de comunicación** — internos y externos
- **pruebas 2–3 veces al año** — simulacros y lecciones aprendidas
- **mejora continua** — actualización y optimización

CONTROLES DE PREVENCIÓN Y RECUPERACIÓN

- **Regla 3-2-1:** 3 copias, 2 medios, 1 offsite/offline
- Backups inmutables
- Pruebas de restauración
- Segmentación
- MFA
- Monitoreo y detección temprana

El BIA convierte tecnología en prioridades de recuperación, responsables, controles y montos para decidir.

BIA = Análisis de Impacto al Negocio | RTO = Tiempo Objetivo de Recuperación | RPO = Punto Objetivo de Recuperación | PCN = Plan de Continuidad del Negocio | PCNT = Plan de Continuidad del Negocio Tecnológico

Frameworks y gobierno

la base para prevenir, responder y recuperarse

1. Gobierno y riesgo

- **ISO/IEC 27001** — Sistema de Gestión de Seguridad de la Información
- **NIST CSF** — Cybersecurity Framework

2. Respuesta y detección

- **NIST SP 800-61** — Respuesta a Incidentes
- **MITRE ATT&CK** — tácticas y técnicas del atacante

3. Continuidad y resiliencia

- **ISO 22301** — Sistema de Gestión de Continuidad del Negocio
- **PCN** — Plan de Continuidad del Negocio
- **PCNT** — Plan de Continuidad del Negocio Tecnológico

4. Priorización y métricas

- **BIA** — Business Impact Analysis / Análisis de Impacto al Negocio
- **RTO** — Tiempo Objetivo de Recuperación
- **RPO** — Punto Objetivo de Recuperación
- **MTTD** — Tiempo Medio de Detección
- **MTTR** — Tiempo Medio de Recuperación

El gobierno es clave: directorio, CISO y dueños de proceso deben definir **prioridades, responsables, presupuesto y pruebas.**

CIERRE

Conclusiones ejecutivas

el gobierno es clave

1. Ransomware no es solo malware: es interrupción del negocio.
2. La prevención empieza antes del cifrado: identidad, accesos, vulnerabilidades y terceros.
3. Sin BIA, sin PCN y sin PCNT, la recuperación se improvisa.
4. Backups sin prueba no equivalen a resiliencia.
5. Lo que no se mide ni se gobierna, no mejora.

Capacidades clave

DETECTAR ANTES
— reducir el tiempo invisible

RESISTIR DURANTE
— limitar movimiento e impacto

RECUPERARSE DESPUÉS
— restaurar servicios críticos

Mensaje final: la resiliencia se diseña, se prueba y se gobierna antes del incidente.