UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Retos y Estrategias: Las Consideraciones de los Ataques de Ransomware en las Américas

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Retos y Estrategias: Las Consideraciones de los Ataques de Ransomware en las Américas

Informe Técnico de Evaluación Estratégica para la Alta Dirección

Fuente Original: OEA & AWS White Paper Series (Edición 10)	**Ámbito Geográfico:** América Latina y el Caribe
Elaborado Por: Especialista Senior en Ciberseguridad & Gestión de Riesgos	**Destinatarios:** Comité Ejecutivo, CISOs, CIOs, Directores Jurídicos

1. Contexto Estratégico y Diagnóstico Regional

El ransomware ha dejado de ser una simple amenaza informática de impacto localizado para consolidarse como una de las interrupciones de negocio más severas y de mayor impacto financiero y reputacional para las organizaciones públicas y privadas en el continente americano. Documentos técnicos elaborados en conjunto por la Organización de los Estados Americanos (OEA) y Amazon Web Services (AWS) confirman que la rápida transformación digital en América Latina ha superado la velocidad de adopción de controles de ciberseguridad y la madurez de las prácticas de higiene digital.

Esta disparidad ha creado un entorno táctico sumamente propicio para el crimen organizado transnacional y grupos hacktivistas, quienes explotan brechas tecnológicas y sesgos de comportamiento humano con un nivel de efectividad alarmante.

> **Ecuación Económica del Cibercrimen Moderno**
> *El cibercrimen actual opera bajo una ecuación de alta eficiencia: búsqueda del máximo anonimato con la mínima evidencia, aprovechamiento de la máxima ambigüedad jurídica regional y*

> *consecución de la máxima efectividad operativa con el menor esfuerzo técnico posible.*

1.1. Hallazgos Clave del Diagnóstico Regional

- **Amenaza Sistémica Continua:** El ransomware representa un riesgo sistémico que desestabiliza tanto la continuidad operativa empresarial como las capacidades esenciales de respuesta e infraestructura del Estado.
- **Crecimiento Exponencial:** La aceleración en la frecuencia de los ataques es drástica. Se proyecta que para el año 2031 se materializará un ataque de ransomware cada 2 segundos a nivel global, en contraste con el intervalo de 11 segundos registrado en 2021.
- **Vectores de Ataque Predominantes:** Los vectores de entrada principales no responden a vulnerabilidades exóticas no descritas, sino a fallas de gestión básica: campañas de phishing altamente dirigidas, explotación de vulnerabilidades conocidas no parcheadas y servicios expuestos sin protección adecuada (especialmente el protocolo RDP).
- **Impacto Socio-Político y Operativo:** En América Latina y el Caribe, el ataque trasciende el impacto financiero primario. Genera parálisis institucional, fuga masiva de datos confidenciales del Estado, crisis reputacionales prolongadas y la alteración directa de servicios ciudadanos críticos.

2. El Dilema Ejecutivo de Respuesta y la Anatomía de un Ataque

Cuando la materialización de un ransomware se confirma a nivel directivo, la organización entra inmediatamente en un estado de alta tensión y fricción interna. La falta de protocolos probados suele desatar un 'juego de atribución de responsabilidades' entre las áreas de tecnología, ciberseguridad, asuntos legales y la alta gerencia. Este escenario de incertidumbre es intencionalmente buscado y provocado por el adversario para retrasar la contención y maximizar su capacidad de extorsión.

2.1. El Dilema del Pago del Rescate

Una de las decisiones más críticas a las que se enfrenta el comité de crisis es si se debe negociar y pagar el rescate exigido en criptomonedas. La postura unánime de los marcos internacionales (ENISA, CISA, FBI, NoMoreRansom) y del presente análisis es NO PAGAR. Las razones operativas y normativas son contundentes:

- **Sin Garantía Técnica:** Pagar no garantiza en absoluto la recuperación completa ni íntegra de la información cifrada. Los desencriptadores provistos por atacantes suelen presentar fallas técnicas que corrompen archivos grandes.
- **Financiación del Delito:** El pago financia directamente las operaciones del crimen organizado transnacional, permitiéndoles desarrollar herramientas más complejas y reincidir contra la misma víctima.
- **Blanco Reincidente:** Las organizaciones que pagan quedan catalogadas en la Dark Web como 'objetivos pagadores', multiplicando la probabilidad de sufrir reincidencias por parte del mismo o de otros grupos cibernéticos.
- **Riesgo de Ilegalidad y Sanciones:** En múltiples jurisdicciones internacionales, el pago a grupos criminales sancionados constituye un delito grave por violación de leyes contra el lavado de activos y financiamiento del terrorismo.

2.2. Anatomía Táctica del Ransomware

Comprender la cadena de ataque (Cyber Kill Chain) del ransomware es indispensable para establecer controles de detección temprana en cada fase operativa:

Etapa del Ataque	Tácticas y TÉCNICAS del Adversario	Mecanismos de Contención
1. Despliegue e Inserción	Ingeniería social, phishing, enlaces fraudulentos, descargas drive-by, explotación de RDP y	Filtrado de correo, autenticación MFA/2FA rigurosa, bastionado de RDP y concientización

	macros maliciosas.	continua.
2. Instalación y Movimiento	Ejecución del payload, ofuscación de código, elevación de privilegios, inyección de procesos y conexión a C2 (Comando y Control).	Protección EDR/XDR, arquitectura de Zero Trust, segmentación de red y bloqueo de tráfico C2.
3. Ejecución e Impacto	Exfiltración sigilosa de datos sensibles, desactivación de agentes de seguridad, cifrado masivo paralelos y nota de extorsión.	Backups inmutables e independientes (3-2-1), DLP (Data Loss Prevention) y aislamiento automático de endpoints.

3. Modelos de Extorsión Evolutiva

El modelo de negocio de los ciberdelincuentes se ha sofisticado drásticamente. De la simple inhabilitación de archivos, han migrado a esquemas de extorsión multinivel diseñados para anular la efectividad de las copias de seguridad tradicionales.

- **1. Extorsión Sencilla:** Cifrado no autorizado de la información para bloquear el acceso de la víctima y exigir rescate a cambio de la clave de descifrado.
- **2. Doble Extorsión:** Robo previo de datos confidenciales (exfiltración) combinado con cifrado. Si la víctima restaura mediante backups y no paga, el atacante amenaza con publicar información privada o venderla en la Dark Web (Doxing).
- **3. Triple Extorsión:** Añade a la doble extorsión el lanzamiento simultáneo de ataques de Denegación de Servicio Distribuida (DDoS)

contra la infraestructura de la víctima para paralizar completamente sus operaciones durante la negociación.

- **4. Cuádruple Extorsión:** El adversario contacta directamente a los clientes, proveedores, reguladores o accionistas de la víctima, informándoles que sus datos personales o comerciales han sido comprometidos para forzar una presión mediática e interna insostenible sobre la empresa.

4. Casos de Estudio Regionales: Guacamaya vs. Conti

El análisis comparativo de las amenazas presentes en América Latina demuestra que los tomadores de decisión enfrentan dos perfiles de adversarios completamente opuestos en sus motivaciones pero igualmente destructivos en sus ejecuciones:

Atributo de Análisis	Grupo GUACAMAYA	Grupo CONTI
Naturaleza del Grupo	Hacktivismo ideológico / Político	Crimen Organizado Transnacional
Motivación Principal	Denuncia socio-ambiental, anti-imperialismo, transparencia obligada.	Lucro económico a gran escala, extorsión masiva.
Sectores Objetivo	Fuerzas Armadas, Ministerios de Defensa, Gobiernos, Sector Extractivo (Minero/Petrolero).	Infraestructura crítica estatal, Ministerios de Hacienda, Sector Salud, Educación, Grandes Empresas.
Tácticas y Vectores	Explotación de vulnerabilidades conocidas no parcheadas en servidores de correo y	Phishing con adjuntos maliciosos, compra de accesos (RDP), reclutamiento de personal interno,

	sistemas operativos.	vulnerabilidades del sistema.
Modus Operandi	Exfiltración masiva de correos y archivos confidenciales (Terabytes) y publicación abierta en el portal Enlace Hacktivista.	Doble extorsión: exfiltración, cifrado masivo de sistemas, solicitud de rescate multimillonario en criptomonedas.
Impactos Destacados	Filtraciones masivas de seguridad nacional en Chile, México (SEDENA), Perú, Colombia y El Salvador.	Ataque catastrófico al Ministerio de Hacienda de Costa Rica (2022) provocando la Declaratoria de Estado de Emergencia Nacional.

5. Estrategias de Mitigación y Recomendaciones Tácticas

Para enfrentar con éxito esta amenaza, las organizaciones deben abandonar el enfoque reactivo puramente enfocado en TI y migrar hacia un marco sistémico de resiliencia directiva e institucional.

5.1. Pilares de Protección y Prevención Técnicas

- **Copias de Seguridad Inmutables:** Implementar la regla 3-2-1-1: 3 copias de datos, 2 medios diferentes, 1 copia fuera de sitio y 1 copia completamente fuera de línea/inmutable (WORM). Realizar pruebas periódicas de restauración real.
- **Arquitectura Zero Trust:** Adoptar un modelo donde nunca se confía y siempre se verifica. Implementar MFA (Autenticación Multi-Factor) obligatorio en todos los puntos de acceso, micro-segmentación de red y cifrado estricto de datos en reposo y en tránsito.

- **Gestión de Vulnerabilidades y Superficie de Exposición:** Cerrar inmediatamente las conexiones RDP directas a Internet. Implementar pasarelas VPN/ZTNA securizadas con MFA y aplicar un programa riguroso de gestión de parches para vulnerabilidades críticas.
- **Monitoreo Avanzado y EDR:** Desplegar soluciones EDR/XDR con capacidades de aislamiento automático de endpoints ante comportamientos anómalos (ej. ejecuciones masivas de cifrado o modificación de sombras de volumen).

5.2. Preparación Operativa, Legal y de Respuesta a Incidentes

- **Plan de Respuesta y Continuidad de Negocio:** Desarrollar y ejercitar mediante simulaciones de mesa (Tabletop Exercises) un plan integral de respuesta a incidentes que involucre al C-Suite, Legal, Comunicaciones y Operaciones.
- **Cumplimiento Regulatorio y Privacidad:** Establecer de forma anticipada los protocolos de notificación obligatoria a autoridades regulatorias de protección de datos personales para mitigar sanciones administrativas y legales.
- **Cultura de Ciberseguridad e Higiene Digital:** Implementar programas continuos de ciberhigiene que transformen al personal de un eslabón débil a un sensor activo en la detección de anomalías y correos sospechosos.
- **Servicios Forenses y Equipos Especializados:** Contar con acuerdos previos (Retainers) con firmas especializadas en análisis forense digital y respuesta a incidentes para actuar sin demoras burocráticas durante una crisis.

6. Conclusiones y Hoja de Ruta Ejecutiva

El ransomware ha evolucionado de un problema técnico de TI a un riesgo estratégico corporativo y de seguridad nacional. La resiliencia ante esta amenaza no se logra adquiriendo herramientas aisladas, sino construyendo una cultura organizacional orientada a la seguridad, la preparación operativa continua y la capacidad de absorber un impacto sin interrumpir la misión corporativa.

Reflexión Final para el Comité Ejecutivo

La pregunta para la alta gerencia ya no es SI la organización será objetivo de un ataque de ransomware, sino CUÁNDO ocurrirá y QUÉ TAN PREPARADA está la institución para responder, contener y recuperarse en tiempo récord sin ceder al Chantaje del adversario.