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

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Guía de Ransomware

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO DE CIBERSEGURIDAD

Análisis de Riesgos, Evaluación Estratégica y Protocolos de Mitigación del Ransomware Empresarial

Documento de Referencia: Guía INCIBE - Ransomware para Empresarios [cite: 1]-

1. Resumen Ejecutivo y Alcance Estratégico

El ransomware ha evolucionado de ser una mera plaga informática a consolidarse como la amenaza cibernética corporativa de mayor impacto operativo, financiero y reputacional para el tejido empresarial [cite: 1]. La sofisticación actual de los vectores de ataque, sumada a la superficie de exposición expandida por la transformación digital, el trabajo remoto y la integración de Internet de las Cosas (IoT), exige un enfoque de defensa en profundidad riguroso y estructurado [cite: 1].

El presente informe ofrece un desglose analítico y técnico derivado de la guía de ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE), complementado con lineamientos defensivos de nivel directivo para neutralizar la amenaza antes, durante y después de un eventual compromiso de seguridad [cite: 1].

> **PROPÓSITO DEL ANÁLISIS**
> El objetivo prioritario de este documento es convertir el conocimiento defensivo en resiliencia operativa. No se trata únicamente de evitar infecciones, sino de garantizar que ante cualquier eventualidad crítica, la continuidad del negocio esté formalmente asegurada sin la necesidad de ceder ante extorsiones criminales [cite: 1].

2. Taxonomía y Evolución Técnica del Ransomware

El ransomware es un código malicioso (malware) diseñado para impedir el acceso a los datos o sistemas informáticos, exigiendo el pago de un

rescate económico para su liberación [cite: 1]. Su evolución histórica refleja un salto cualitativo crítico: de simples bloqueadores de interfaz a algoritmos criptográficos asimétricos e híbridos de alta complejidad que imposibilitan el descifrado por fuerza bruta sin la clave privada [cite: 1].

2.1 Clasificación de Variantes y Niveles de Amenaza

- **Hoax Ransomware:** Simulación engañosa de cifrado que aplica técnicas de ingeniería social extremas para inducir al pago mediante amenazas de borrado inminente sin haber afectado realmente la estructura del sistema de archivos [cite: 1].
- **Scareware:** Falsas soluciones de seguridad en forma de alertas emergentes molestas que informan sobre supuestas infecciones víricas e inducen al usuario a descargar limpiadores fraudulentos que actúan como ejecutables maliciosos [cite: 1].
- **Bloqueadores de Pantalla:** Malware que impide el uso operativo del dispositivo bloqueando el entorno gráfico mediante ventanas a pantalla completa. Incluye variantes que suplantan a las Fuerzas y Cuerpos de Seguridad (como el denominado 'virus de la policía'), exigiendo multas inexistentes [cite: 1].
- **Ransomware de Cifrado (Crypto-Ransomware):** La vertiente más destructiva. Utiliza cifrado simétrico/asimétrico robusto sobre discos locales, unidades mapeadas, recursos compartidos en red y servicios cloud. Incluye la modalidad 'wiper', cuyo objetivo real es la destrucción irreversible de la información [cite: 1].
- **Doxware / Doble Extorsión:** Modalidad centrada en el 'doxing' o exfiltración previa de activos de información confidenciales o datos personales regulados (GDPR). El ciberdelincuente extorsiona a la organización no solo con la pérdida de los datos, sino con su divulgación pública [cite: 1].

2.2 El Ecosistema Monetario: Criptodivisas y Lavado de Fondos

Los ciberdelincuentes exigen el pago del rescate mediante criptodivisas (como Bitcoin) para garantizar el anonimato operativo [cite: 1]. La trazabilidad financiera se dificulta drásticamente mediante el uso de redes

anónimas (como Tor) y servicios de 'mixing' o 'tumbling' (mezcladores de criptoactivos), los cuales combinan fondos de múltiples transacciones para diluir el rastro policial [cite: 1]. Asimismo, la red criminal emplea intermediarios financieros denominados 'muleros' para la bancarización y blanqueo final del capital ilícito [cite: 1].

3. Vectores de Infección y Superficie de Ataque

Las organizaciones quedan expuestas a través de múltiples vectores de entrada, siendo el factor humano y la exposición técnica los focos de mayor vulnerabilidad [cite: 1]:

- **Ingeniería Social y Phishing:** Phishing masivo o dirigido (spear phishing), archivos adjuntos maliciosos con doble extensión (ej. factura.pdf.exe) y enlaces fraudulentos distribuidos por correo o mensajería [cite: 1].
- **Vulnerabilidades de Software:** Explotación automatizada de fallos de seguridad en software, sistemas operativos y navegadores mediante exploit kits en sitios web infectados (drive-by download) o inyección de anuncios maliciosos en portales legítimos (malvertising) [cite: 1].
- **Servicios y Puertos Expuestos:** Servicios RDP (Escritorio Remoto) expuestos directamente a Internet sin autenticación multifactor (MFA), puertos por defecto abiertos y credenciales corporativas comprometidas por fuerza bruta [cite: 1].
- **Infraestructura Crítica e IoT:** Servidores web desactualizados, sistemas de control industrial (SCADA/OT) y dispositivos IoT integrados a la red corporativa manteniendo contraseñas predeterminadas o embebidas en el código ('hard-coded') [cite: 1].

4. Estrategia Integral de Prevención y Mitigación

4.1 Factor Humano: Concienciación y Cultura de Seguridad

Más del 75% de las infecciones exitosas por ransomware involucran la manipulación humana mediante ingeniería social [cite: 1]. Resulta imperativo capacitar al personal para detectar la secuencia habitual de un

ataque: reconocimiento, establecimiento de confianza, manipulación (explotando la autoridad, urgencia o ego) y exfiltración [cite: 1].

- Desconfiar y descartar correos no solicitados o con lenguaje apremiante [cite: 1].
- Verificar la URL real de cualquier enlace utilizando expandidores de enlaces si el dominio está acortado [cite: 1].
- Habilitar la visibilidad de extensiones de archivos para identificar ejecutables enmascarados [cite: 1].
- Prohibir el almacenamiento de contraseñas corporativas en notas físicas (post-its) e implantar gestores de contraseñas autorizados [cite: 1].

4.2 Mínima Exposición y Segmentación de Red (DMZ)

Para mitigar el desplazamiento lateral dentro de la infraestructura corporativa, se debe segmentar la red interna mediante subredes y cortafuegos (Firewalls) de última generación (NGFW) o soluciones open source de alta eficiencia con capacidades IDS/IPS (Sistemas de Detección y Prevención de Intrusiones) [cite: 1].

Zona de Red	Servidores / Dispositivos	Medidas de Control Requeridas
DMZ (Desmilitarizada)	Servidores Web, Mail, Webmail, VPN, DNS	Monitoreo prioritario, aislamiento estricto de la LAN, actualización crítica inmediata [cite: 1].
Red Corporativa Interna	Estaciones de trabajo, bases de datos, ERP, Nóminas	Políticas de mínimos privilegios, restricción de tráfico entre VLANs, antivirus EDR [cite: 1].
Acceso Remoto / Movilidad	Portátiles corporativos, conexiones externas	Conexión obligatoria por VPN cifrada,

	DirectAccess o aislamiento en Sandbox [cite: 1].

4.3 Robustecimiento del Correo Electrónico

- **Filtrado Activo:** Despliegue estricto de filtros anti-spam corporativos en el servidor o proveedor de dominio [cite: 1].
- **Autenticación de Dominios:** Implementación obligatoria de los protocolos SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication) para evitar la suplantación de identidad corporativa [cite: 1].
- **Restricción de Ejecución:** Desactivación generalizada de la ejecución automáticas de macros en herramientas ofimáticas y bloqueo del formato HTML/JavaScript en cuentas públicas o de alta criticidad [cite: 1].
- **Sandboxing:** Uso de entornos de aislamiento (como Windows Sandbox o Cuckoo Sandbox) para la apertura y verificación de archivos o enlaces sospechosos [cite: 1].

4.4 Gestión de Privilegios y Copias de Seguridad (Regla 3-2-1)

El principio de mínimos privilegios exige la separación estricta entre cuentas de usuario estándar y cuentas con facultades administrativas, aplicando políticas de bloqueo automático ante intentos fallidos para prevenir ataques de fuerza bruta [cite: 1].

En materia de respaldos, la estrategia de respaldo debe basarse en la Regla 3-2-1 [cite: 1]:

- Mantener al menos TRES copias de seguridad actualizadas de la información [cite: 1].
- Guardar los respaldos en DOS soportes o medios diferentes (disco externo, almacenamiento local, nube) [cite: 1].
- Almacenar al menos UNA copia completamente desconectada (offline) o en una ubicación remota no sincronizada persistentemente,

previniendo que el ransomware cifre las copias alojadas en red o en la nube [cite: 1].
- Auditar y verificar periódicamente la integridad técnica y la capacidad de restauración de las copias guardadas [cite: 1].
- Cifrar los datos más sensibles almacenados en el backup para neutralizar amenazas de exfiltración o doxing [cite: 1].

5. Protocolo de Respuesta a Incidentes y Recuperación

Ante la confirmación de un incidente de ransomware, la organización debe ejecutar un Plan de Respuesta a Incidentes articulado en cuatro fases consecutivas [cite: 1]:

> **CICLO DE VIDA DE LA GESTIÓN DE INCIDENTES**
> Fase 1: Preparación (Estructura de gestión, documentación de red, contactos de emergencia y CERT).
> Fase 2: Detección y Análisis (Clasificación de la amenaza, alcance e identificación de vectores).
> Fase 3: Contención, Desinfección y Recuperación (Aislamiento, clonación forense, desinfección y restauración).
> Fase 4: Acciones Posteriores al Cierre (Registro documental, lecciones aprendidas e informe de mejora) [cite: 1].

5.1 Pasos Operativos de Recuperación de Activos

- **1. Aislamiento Físico y Lógico:** Desconectar inmediatamente el equipo o servidor afectado de la red cableada o inalámbrica. Desconectar unidades compartidas, discos extraíbles o servicios cloud para detener la propagación masiva [cite: 1].
- **2. Clonación Forense:** Realizar una copia bit a bit (clonación forense) del disco duro comprometido antes de realizar cualquier intervención. Esto preserva las evidencias legales y permite probar herramientas de descifrado futuras [cite: 1].

- **3. Rotación de Credenciales:** Modificar inmediatamente todas las credenciales de red, cuentas corporativas y servicios en la nube desde un equipo limpio [cite: 1].
- **4. Denuncia y Notificación:** Interponer la denuncia formal ante las autoridades competentes (Guardia Civil - GDT, Policía Nacional - BIT o Unidades Especializadas de Ciberdelincuencia) e informar al centro de respuesta estatal (INCIBE-CERT) [cite: 1].
- **5. Desinfección Profunda:** Ejecutar herramientas antimalware/antivirus actualizadas sobre el disco clonado y eliminar la persistencia del código malicioso antes de proceder a la restauración de archivos [cite: 1].
- **6. Descifrado o Restauración de Backup:** Utilizar plataformas internacionales como No More Ransom (www.nomoreransom.org) y la función Crypto-Sheriff para identificar la variante exacta de cifrado e investigar si existen claves públicas de descifrado [cite: 1]. Si no existen, restaurar desde copias de seguridad limpias/Shadow Copies en un soporte formateado e instalando el sistema operativo desde cero [cite: 1].

6. Posicionamiento Directivo sobre el Pago del Rescate

> **POLÍTICA CORPORATIVA DE ZERO PAYOUT**
> LA RECOMENDACIÓN INSTITUCIONAL Y TÉCNICA ES CATEGÓRICA: BAJO NINGUNA CIRCUNSTANCIA SE DEBE REALIZAR EL PAGO DEL RESCATE [cite: 1].

Las razones estratégicas y operativas que sustentan la negativa absoluta al pago se resumen a continuación [cite: 1]:

- **Sin Garantía de Recuperación:** No existe garantía alguna de que los criminales entreguen la clave de descifrado correcta o de que el proceso de desinfección no dañe definitivamente la integridad de la base de datos [cite: 1].

- **Re-victimización Garantizada:** Pagar valida la rentabilidad del modelo delictivo para la entidad atacada, marcando a la empresa como un objetivo altamente lucrativo para futuros ciberataques [cite: 1].
- **Incremento de Exigencias:** Es recurrente que tras un primer pago, las bandas extorsivas incrementen la cifra exigida solicitando cobros adicionales bajo la amenaza de divulgar la información exfiltrada [cite: 1].
- **Financiación del Cibercrimen:** El pago de rescates financia directamente la delincuencia organizada y la investigación de malware más destructivo a nivel internacional [cite: 1].

7. Recomendaciones de Auditoría y Compliance

Para validar la postura de seguridad de la organización frente a amenazas de ransomware, la Dirección de Ciberseguridad debe programar y requerir auditorías periódicas independientes que abarquen [cite: 1]:

- **Tests de Penetración (Pentesting):** Simulaciones de ciberataques externos e internos para identificar vías no autorizadas de acceso a activos críticos [cite: 1].
- **Auditorías de Red y Perímetro:** Escaneo perimetral de puertos abiertos, análisis de la electrónica de red (routers/switches) y revisión de configuraciones de cortafuegos [cite: 1].
- **Auditorías Web:** Identificación de fallos de seguridad, inyecciones de código y debilidades en servicios web e intranets corporativas [cite: 1].
- **Monitoreo SIEM y Análisis Forense:** Implantación de sistemas SIEM (Security Information and Event Management) para la correlación y monitoreo de eventos de seguridad en tiempo real, conservación de logs de auditoría y revisión de cibERP/Ciberseguros [cite: 1].