■ CONFIDENCIAL — MEDTECH DOMINICANA

OPERACIÓN SHADOWLOCK

Plan de Respuesta a Incidentes de Ciberseguridad

NIST SP 800-61 Rev. 2 · MedTech Dominicana · 2026

ACCEDE AL PROYECTO COMPLETO EN:

o-shadowlock.pages.dev

Haz clic o escribe la URL en tu navegador

PRESENTADO POR

Steven William Capellán

ID: 10163717

HIPAA Compliance | Ley 172-13 RD | NIST SP 800-61 | CSIRT | PUCMM 2026

Gestión de Incidentes · Sección 1910-5472 · PUCMM · Abril 2026

PONTIFICIA UNIVERSIDAD CATÓLICA MADRE Y MAESTRA

Centro de Tecnología y Educación Permanente – TEP PUCMM

FACULTAD:

Ciencias e Ingeniería

CARRERA:

Técnico Superior de Ciberseguridad

ASIGNATURA

Gestion de Incidentes

TEMA:

Operación Shadow Lock

PRESENTADO POR:

Steven W. Capellán - 10163717

WEB - Del Proyecto

PRESENTADO A:

Rolando del Rosario

FECHA DE ENTREGA:

07/Abr/2026

OPERACIÓN SHADOWLOCK

Plan de Respuesta a Incidentes de Ciberseguridad

Basado en NIST SP 800-61 Rev. 2

Organización: MedTech Dominicana
Rol del Responsable: Incident Response Manager
Clasificación: **CONFIDENCIAL**
Fecha: 26 de marzo de 2026

FASE	DESCRIPCIÓN
Fase 1	Preparación
Fase 2	Detección y Análisis
Fase 3	Contención, Erradicación y Recuperación
Fase 4	Actividad Post-Incidente

⚠ INCIDENTE ACTIVO: RANSOMWARE TIPO RYUK ⚠

RESUMEN EJECUTIVO

MedTech Dominicana, una clínica privada ubicada en la República Dominicana, fue víctima de un ataque de ransomware de tipo Ryuk. El ataque cifró múltiples servidores críticos, dejó inoperativo el sistema de citas médicas y los atacantes amenazaron con publicar historiales médicos confidenciales de pacientes.

Este incidente involucra una violación potencial del HIPAA (Health Insurance Portability and Accountability Act) y de la Ley 172-13 de la República Dominicana (Ley de Protección de Datos Personales), lo que eleva su criticidad al nivel más alto.

PARÁMETRO	DETALLE
Tipo de Ataque	Ransomware Ryuk (Categoría 1 - Prioridad ALTA)
Fecha/Hora Detección	26 de marzo de 2026 / 08:30 AM
Sistemas Afectados	Servidores de historiales médicos, sistema de citas, infraestructura de red
Regulaciones Violadas	HIPAA + Ley 172-13 (República Dominicana)
MTTD	2 horas
MTTR	48 horas
Costo Estimado	RD$ 2,500,000

FASE 1: PREPARACIÓN (NIST Sección 2)

La preparación es la base de toda respuesta efectiva. Esta fase define los recursos, equipos, políticas y herramientas necesarias antes de que ocurra un incidente.

1.1 Equipo CSIRT – Matriz RACI

La Matriz RACI define claramente las responsabilidades durante cada fase del incidente:

- R = Responsable: Ejecuta la tarea
- A = Accountable: Rinde cuentas del resultado
- C = Consulted: Brinda información o criterio
- I = Informed: Recibe información del estado

ROL / FASE	Detección	Contención	Erradicación	Recuperación	Post-Incidente
IR Manager	A	A	A	A	A
Analista SOC	R	R	C	I	C
Ing. de Sistemas	C	R	R	R	C
Asesor Legal	I	C	I	C	R
Dir. Médico	I	I	I	R	I
Comunicaciones	I	I	I	I	R
CISO	C	A	C	C	A

1.2 Política de Respuesta a Incidentes (IR Policy)

POLÍTICA OFICIAL DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

MedTech Dominicana | Versión 1.0 | Aprobada: 26/03/2026

1.2.1 Propósito y Alcance

Esta política establece el marco formal para la detección, reporte, manejo y recuperación de incidentes de seguridad informática en MedTech Dominicana, en cumplimiento con el NIST SP 800-61 Rev. 2, el HIPAA y la Ley 172-13 de la República Dominicana.

1.2.2 Definición de Incidente

Un incidente de seguridad es cualquier evento que amenace la confidencialidad, integridad o disponibilidad de los activos de información de MedTech Dominicana, especialmente los datos de pacientes.

1.2.3 Principios de la Política

1. Todo incidente debe ser reportado al IR Manager en un plazo máximo de 1 hora desde su detección.
2. Ningún empleado está autorizado a manejar un incidente de forma independiente sin notificar al CSIRT.
3. Se debe preservar la evidencia digital antes de cualquier acción correctiva.
4. La comunicación externa sobre incidentes es responsabilidad exclusiva del departamento de Comunicaciones y el Asesor Legal.
5. El cumplimiento con HIPAA y Ley 172-13 es obligatorio en toda respuesta.

1.2.4 Firmas de Aprobación

ROL	NOMBRE	FIRMA / FECHA
Gerente General	_____	_____ / 26-03-2026
CISO	_____	_____ / 26-03-2026
Director Médico	_____	_____ / 26-03-2026

1.3 Plan de Backups 3-2-1

La regla 3-2-1 garantiza la disponibilidad de datos ante cualquier evento destructivo:

REGLA	DESCRIPCIÓN	IMPLEMENTACIÓN EN MEDTECH
3 Copias	3 copias totales de datos	Original en producción + 2 backups independientes
2 Medios	En 2 tipos de medios distintos	NAS local cifrado + Nube (AWS S3 con cifrado AES-256)
1 Offsite	1 copia fuera del sitio	Backup diario automatizado a datacenter en Santo Domingo

- Frecuencia de backup: Diario (incremental) y semanal (completo)
- Pruebas de restauración: Mensualmente – verificar integridad y tiempo de recuperación
- Retención: 30 días para incrementales, 1 año para backups completos
- Cifrado: AES-256 en todos los medios de almacenamiento

1.4 Herramientas Instaladas y Verificadas

HERRAMIENTA	FUNCIÓN	ESTADO	RESPONSABLE
rsync v3.4.1	Backup 3-2-1 incremental de datos médicos con verificación de integridad MD5	☑ Ejecutado	Ing. Sistemas
osquery v5.21.0	Respuesta rápida y forense en endpoints	☑ Ejecutado	Analista SOC
nmap v7.98	Escaneo de red y detección de propagación lateral en segmento 192.168.0.0/24	☑ Ejecutado	Analista SOC
ClamAV v1.5.2	Bloqueo de tráfico malicioso	☑ Ejecutado	Ing. Sistemas
md5sum (GNU coreutils)	Detección y respuesta en endpoints	☑ Ejecutado	CISO

FASE 2: DETECCIÓN Y ANÁLISIS (NIST Secciones 3.1–3.2)

Esta fase cubre la identificación del incidente, su análisis técnico, clasificación y priorización según el impacto potencial sobre MedTech Dominicana.

2.1 Cronología del Incidente

HORA	SISTEMA	EVENTO
06:30 AM	Servidor Principal	Actividad inusual detectada: múltiples accesos a archivos en horas no laborables
07:15 AM	EDR	Alerta del EDR: proceso 'ryuk.exe' detectado en estación de trabajo Admin-01
07:45 AM	Red Interna	Propagación lateral detectada: 3 servidores adicionales comprometidos
08:30 AM	Sistema General	Archivos cifrados con extensión .ryuk. Nota de rescate encontrada en escritorios
08:30 AM	SOC	MTTD = 2 horas. Incidente escalado a CSIRT y declarado Categoría 1

2.2 Análisis Técnico – Detección con osquery (Output Real)

osquery v5.21.0 – Detección de Procesos por CPU (Output Real)

```
osquery> SELECT name, path, pid, user_time, system_time, uid FROM processes ORDER BY
user_time DESC LIMIT 10;
name=brave | path=/opt/brave-bin/brave | pid=61032 | user_time=6809540 | uid=1000
```

osquery v5.21.0 – Monitoreo de Conexiones de Red Activas (C2 Detection)

```
osquery> SELECT pid, local_address, local_port, remote_address, remote_port, state FROM
process_open_sockets WHERE remote_port != 0 LIMIT 10;
pid=2127 | local=192.168.0.110:41828 | remote=151.101.66.137:443 | state=ESTABLISHED
```

2.3 Clasificación del Incidente

CRITERIO	EVALUACIÓN
Categoría NIST	Categoría 1 – Malware/Ransomware
Prioridad	CRÍTICA – ALTA (impacto en vida humana por sistemas médicos afectados)
Confidencialidad	COMPROMETIDA – Riesgo de exfiltración de historiales médicos
Integridad	COMPROMETIDA – Archivos cifrados y potencialmente alterados
Disponibilidad	COMPROMETIDA – Sistemas de citas y registros fuera de servicio
Regulaciones	HIPAA (EE.UU.) + Ley 172-13 (República Dominicana)

FASE 3: CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN (NIST Sección 3.3)

3.1 Contención a Corto Plazo (Inmediata – 0-4 horas)

Objetivo: Detener la propagación del ransomware y limitar el impacto inmediato.

#	ACCIÓN	RESPONSABLE	ESTADO
1	Desconectar físicamente los servidores afectados de la red	Ing. Sistemas	☑ Ejecutado 08:45 AM
2	Activar firewall en todos los perfiles de red	Ing. Sistemas	☑ Ejecutado 08:50 AM
3	Bloquear puertos SMB (445) y RDP (3389) utilizados por Ryuk	Analista SOC	☑ Ejecutado 09:00 AM
4	Deshabilitar cuentas administrativas comprometidas	IR Manager	☑ Ejecutado 09:15 AM
5	Notificar a pacientes y autoridades regulatorias (HIPAA Breach Notification)	Asesor Legal	⏳ En proceso

nmap v7.98 – Escaneo de Red para Detectar Propagación Lateral (Output Real)

```
# Activar firewall en todos los perfiles
$ sudo nmap -sn 192.168.0.0/24 -oN ~/medtech/scan_red.txt
# Bloquear tráfico entrante del ransomware
Nmap scan report for 192.168.0.1 — Host is up (0.0026s) — MAC: 08:40:F3:63:26:A8
(Tenda/Router)
Nmap scan report for 192.168.0.110 — Host is up. | 256 IPs escaneadas | 2 hosts activos | Sin
propagación lateral
```

3.2 Contención a Largo Plazo (4-24 horas)

- Segmentar la red interna mediante VLANs para aislar áreas críticas (registros médicos, administración, citas)
- Implementar autenticación multifactor (MFA) en todas las cuentas administrativas
- Desplegar soluciones EDR actualizadas en todos los endpoints no comprometidos
- Establecer monitoreo 24/7 del tráfico de red con alertas en tiempo real

3.3 Erradicación (24-48 horas)

Objetivo: Eliminar completamente el ransomware y sus componentes del entorno.

Comandos de Erradicación

```
# Eliminar archivos cifrados y el malware
$ sudo freshclam && clamscan -r ~/medtech/ --infected --log=~/medtech/clamav_scan.txt
Known viruses: 3,627,814 | Scanned dirs: 12 | Scanned files: 14 | Infected files: 0 | ☑
Sistema limpio
```

- Análisis forense con osquery para identificar vector de entrada y procesos maliciosos activos
- Remoción de todas las claves de registro creadas por el malware

- Verificación de integridad de todos los sistemas mediante hash comparison
- Escaneo completo con herramientas antimalware actualizadas en todos los equipos

3.4 Recuperación – Golden Image (48-72 horas)

#	PASO DE RECUPERACIÓN	TIEMPO EST.	RESPONSABLE
1	Restaurar servidores desde backup offline (Golden Image)	4 horas	Ing. Sistemas
2	Probar restauración en entorno aislado (sandbox)	6 horas	Analista SOC
3	Verificar integridad de datos médicos restaurados	8 horas	Dir. Médico
4	Reconectar sistemas a la red con monitoreo intensivo	2 horas	Ing. Sistemas
5	Monitorear operación normal durante 72 horas continuas	72 horas	Analista SOC
6	Confirmar restauración completa y cierre del incidente	2 horas	IR Manager

FASE 4: ACTIVIDAD POST-INCIDENTE (NIST Sección 3.4)

Esta fase documenta las lecciones aprendidas, calcula métricas de desempeño e implementa mejoras para evitar futuros incidentes similares.

4.1 Métricas de Desempeño

MÉTRICA	VALOR REAL	OBJETIVO NIST	EVALUACIÓN
MTTD (Mean Time to Detect)	2 horas	< 4 horas	☑ CUMPLIDO
MTTR (Mean Time to Recover)	48 horas	< 72 horas	☑ CUMPLIDO
Tiempo de Contención	45 minutos	< 2 horas	☑ EXCELENTE
Sistemas Recuperados	100%	100%	☑ CUMPLIDO

4.2 Análisis de Costos del Incidente

CATEGORÍA DE COSTO	COSTO (RD$)	OBSERVACIONES
Tiempo de inactividad (48 h × ingresos perdidos)	RD$ 800,000	Sistema de citas caído
Honorarios legales (HIPAA + Ley 172-13)	RD$ 450,000	Notificaciones y asesoría
Recuperación técnica (horas extra equipo IT)	RD$ 350,000	72 horas de trabajo intensivo
Herramientas forenses y licencias adicionales	RD$ 200,000	osquery, nmap, ClamAV (open source)
Comunicación a pacientes afectados	RD$ 150,000	Cartas certificadas y call center
Mejoras de seguridad post-incidente	RD$ 550,000	MFA, EDR, segmentación de red
TOTAL ESTIMADO	**RD$ 2,500,000**	**Costo total del incidente**

4.3 Informe de Lecciones Aprendidas

Fortalezas Identificadas

- El equipo CSIRT respondió dentro de los tiempos objetivo establecidos por el NIST
- El sistema de backups 3-2-1 permitió la recuperación total de los datos médicos
- La política de IR facilitó la toma de decisiones rápidas y coordinadas

Áreas de Mejora

- Implementar monitoreo de comportamiento 24/7 para reducir el MTTD a menos de 1 hora
- Realizar simulacros trimestrales de ransomware con todo el personal clínico y administrativo
- Fortalecer la segmentación de red para evitar propagación lateral
- Establecer un canal de comunicación cifrado exclusivo para el CSIRT

Plan de Mejoras (30-60-90 días)

PLAZO	ACCIÓN	RESPONSABLE	PRIORIDAD
30 días	Implementar MFA en todos los sistemas críticos	CISO	CRÍTICA
30 días	Actualizar y probar todos los backups offline	Ing. Sistemas	ALTA
60 días	Segmentar red en VLANs por departamento	Ing. Sistemas	ALTA
60 días	Realizar tabletop exercise con todo el CSIRT	IR Manager	MEDIA
90 días	Capacitación en ciberseguridad para todo el personal	RRHH + CISO	MEDIA

TABLETOP EXERCISE – SIMULACRO (45 MINUTOS)

El ejercicio de mesa (Tabletop Exercise) simula el incidente Operación ShadowLock en un entorno controlado, permitiendo al equipo CSIRT practicar la toma de decisiones sin consecuencias reales.

Escenario 1: Detección (10 minutos)

SITUACIÓN: El SOC recibe una alerta del EDR a las 07:15 AM. El analista observa que el proceso 'ryuk.exe' está activo en la estación Admin-01 y hay tráfico inusual hacia IPs externas desconocidas.

Preguntas de Discusión

6. ¿Cómo determinas si esta alerta es un verdadero positivo o una falsa alarma?
7. ¿En qué momento decides escalar el incidente al CSIRT completo?
8. ¿Qué evidencia inicial debes preservar ANTES de tomar cualquier acción?
9. ¿A quién notificas primero según la Matriz RACI?

Escenario 2: Decisión de Contención (15 minutos)

SITUACIÓN: Se confirma que el ransomware se está propagando activamente. Tienes 2 opciones: (A) Aislar SOLO el servidor afectado manteniendo el resto de la red activa. (B) Desconectar TODA la red inmediatamente, incluyendo sistemas de urgencias médicas.

Preguntas de Discusión

10. ¿Cuál es el riesgo de cada opción para los pacientes en este momento?
11. ¿Cómo afecta cada decisión al cumplimiento del HIPAA y Ley 172-13?
12. ¿Cuándo sería aceptable cortar completamente internet en una clínica médica?
13. ¿Qué sistemas médicos críticos (p.ej. soporte vital) deben mantenerse activos a toda costa?

Escenario 3: Comunicación de Crisis (20 minutos)

SITUACIÓN: Los atacantes amenazan con publicar 5,000 historiales médicos en 24 horas si no se paga el rescate. Un periodista llama preguntando por el incidente. La Dirección de Salud Pública también solicita un informe.

Preguntas de Discusión

14. ¿Pagas el rescate? Argumenta tu posición con base en las mejores prácticas del NIST.
15. ¿Qué le dices al periodista? ¿Quién está autorizado para hablar con la prensa?
16. ¿Cómo notificas a los pacientes afectados según los plazos del HIPAA (72 horas) y Ley 172-13?
17. ¿Qué información incluyes en el informe a la Dirección de Salud Pública?