UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

CIBERSEGURIDAD EN EL IOMT: PROPUESTA DE ESTRATEGIAS DE PROTECCIÓN PARA LA INTEGRIDAD DE DISPOSITIVOS MÉDICOS CRÍTICOS

AUTOR:

EDGAR RAFAEL CHUVA GÓMEZ

DIRECTOR:

EDUARDO GUILLERMO PINOS VÉLEZ

CUENCA – ECUADOR
2025

Autor:

Edgar Rafael Chuva Gómez
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
echuvag@gmail.com

Dirigido por:

Eduardo Guillermo Pinos Vélez
Ingeniero Electrónico.
Magister en Gerencia y Liderazgo Educacional.
Doctor en Ingeniería
epinos@ups.edu.ec

DEDICATORIA

A mis padres, por su amor inmenso, sus sacrificios silenciosos y por enseñarme que los sueños no se alcanzan sin constancia. Cada paso en este camino lleva su nombre.

A mi familia, que con su paciencia y comprensión me dio el espacio para crecer, incluso en los días más difíciles.

A quienes creyeron en mí cuando ni yo mismo lo hacía. Gracias por sostenerme con sus palabras, su fe y su cariño.

Y a mí mismo, por no rendirme, por volver a intentarlo cada vez que caí y por haber llegado hasta aquí con el corazón lleno de propósito.

AGRADECIMIENTO

Agradezco con el corazón a la Universidad Politécnica Salesiana, por ser más que una institución académica: por ser el lugar donde descubrí mi vocación, forjé mi carácter y me preparé para servir desde el conocimiento.

A mi tutor, Eduardo Pinos, por su guía paciente, sus consejos certeros y su disposición generosa. Su acompañamiento marcó una diferencia profunda en este proyecto.

A mis profesores, por compartir su conocimiento con pasión y por ser faros en este proceso de aprendizaje.

A mi familia, por su amor incondicional. Gracias por esperarme despiertos, por alentarme en los días grises y por abrazarme sin preguntas cuando el cansancio pesaba más que las palabras.

A mis amigos y compañeros, por los mensajes de aliento, las conversaciones que sanan y por recordarme que no estoy solo en el camino.

Y a la vida, por enseñarme que las metas más grandes siempre requieren el valor de comenzar… y la valentía de continuar.

Ciberseguridad en IoMT: Propuesta de Protocolo Integral para la Protección de Dispositivos Médicos Críticos en Entornos Hospitalarios

Edgar Rafael Chuva Gómez[1] and Eduardo Guillermo Pinos Vélez [2]

[1] Universidad Politécnica Salesiana, Sede Cuenca, Ecuador
echuva@est.ups.edu.ec
epinos@ups.edu.ec

Abstract. The convergence of medical devices and networked systems has led to the emergence of the Internet of Medical Things (IoMT), a paradigm that significantly enhances clinical monitoring, diagnostics, and data-driven healthcare. However, the lack of built-in security mechanisms in many IoMT devices makes them vulnerable to cyberattacks, potentially endangering patient safety and data integrity. This paper presents an integrated cybersecurity protocol specifically designed for IoMT environments. The protocol is structured into three functional layers: prevention (including TLS 1.3 encryption, multi-factor authentication, and VLAN segmentation), detection (using open-source tools such as Snort and Wazuh), and automated response.

To validate the protocol, a simulation was conducted involving a Webmin 1.910 server as a vulnerable target, attacked from Kali Linux, with detection and monitoring handled by Snort and Wazuh. The results demonstrated a significant reduction in detection and response times compared to baseline scenarios. This work aligns with international regulations such as HIPAA and GDPR, as well as Ecuador's national data protection law, and proposes a technically feasible and scalable approach to secure critical medical infrastructures in developing healthcare systems.

Keywords: IoMT, cybersecurity, medical devices, intrusion detection, monitoring, data protection.

1 Introducción

El avance acelerado de las tecnologías de conectividad ha transformado el sector de la salud a través de la incorporación del Internet de las Cosas Médicas (IoMT), una arquitectura que permite integrar dispositivos clínicos a sistemas en red para recolectar y transmitir datos en tiempo real [1]. Esta conectividad ha mejorado la eficiencia en el monitoreo y tratamiento de pacientes, pero también ha expuesto nuevas superficies de ataque que comprometen tanto la información médica como la integridad operativa de los equipos [2].

Los dispositivos IoMT, diseñados mayoritariamente sin un enfoque de seguridad, presentan vulnerabilidades críticas como firmware desactualizado, falta de cifrado, contraseñas por defecto y ausencia de monitoreo interno [3]. Estas debilidades han sido aprovechadas por actores maliciosos para acceder a redes hospitalarias, comprometer historiales médicos e incluso alterar la funcionalidad de dispositivos vitales [4].

En Ecuador, aunque la Ley Orgánica de Protección de Datos Personales constituye un marco regulatorio reciente [5], aún no se han establecido directrices técnicas específicas para el IoMT. En este contexto, el presente trabajo propone un protocolo integral de ciberseguridad, estructurado en tres fases: prevención, detección y respuesta, e implementado mediante herramientas como Snort y Wazuh [6]. La propuesta se valida en un entorno simulado de laboratorio que replica escenarios de ataque real, con el objetivo de aportar una solución adaptable y técnica a las necesidades del sector salud.

2 Análisis de vulnerabilidades en dispositivos IoMT

2.1 Vulnerabilidades a nivel dispositivo y protocolo en IoMT

El ecosistema IoMT comprende dispositivos conectados como bombas de infusión, sensores portátiles, marcapasos, oxímetros y monitores de signos vitales [7]. Muchos de ellos no fueron concebidos con criterios de seguridad y, en consecuencia, exhiben fallas críticas: firmware desactualizado, credenciales por defecto, comunicaciones sin cifrar y ausencia de autenticación fuerte [8]. Estas debilidades habilitan vectores como el escaneo de puertos, ataques de fuerza bruta, ejecución remota de comandos o denegación de servicio [27].

En la *Figura 1* se comparan dos capturas: *(a)* un intercambio *HTTP sin cifrar*, donde son legibles las cabeceras *GET*, *Host* y *User-Agent*, exponiendo metadatos del dispositivo médico en tránsito hacia el servidor; y *(b)* tráfico bajo *TLS 1.3*, en el que solo se observan los mensajes de negociación *(ClientHello/ServerHello)* y los *"Encrypted Application Data"*, manteniéndose ocultas las cabeceras y el contenido de aplicación.

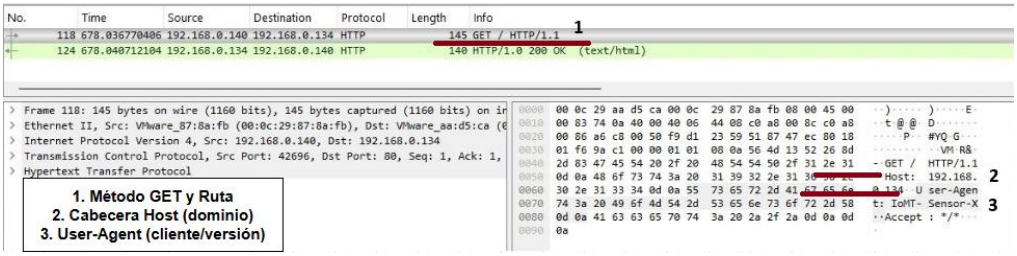

Fig. 1a. *HTTP* sin cifrar — cabeceras *GET*, *Host* y *User-Agent* visibles

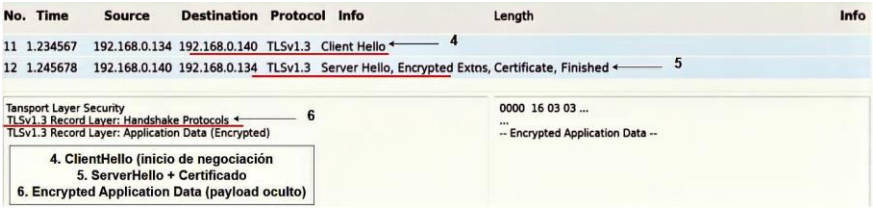

Fig. 1b. TLS 1.3 — solo se observan mensajes de negociación (*Client/ServerHello*) y los "*Encrypted Application Data*", ocultando cabeceras y contenido de aplicación.

2.2 Exposición y superficie de ataque en redes hospitalarias

En hospitales y clínicas, los dispositivos IoMT suelen operar en redes internas que comparten infraestructura con sistemas administrativos o estaciones de trabajo *sin segmentación adecuada* [10]. Este diseño plano amplía el *dominio de difusión* y favorece el *movimiento lateral*: si un atacante compromete un equipo no clínico, puede alcanzar dispositivos médicos críticos y servicios de soporte clínico (PACS/RIS, HIS/EMR) [9]. A ello se suman superficies de ataque frecuentes en entornos heredados *sistemas operativos sin soporte, cuentas por defecto, servicios expuestos* (p. ej., SMB/RDP), o *accesos de terceros* que incrementan la probabilidad de escalamiento y persistencia [6, 17, 18].

Además, la *persistencia de protocolos obsoletos* (*Telnet*, *HTTP*) y la *ausencia de monitoreo en tiempo real* dificultan detectar a tiempo accesos no autorizados o alteraciones en la funcionalidad del equipo médico, con impacto potencial en la seguridad del paciente [10]. Este contexto justifica una arquitectura *con segmentación por función y riesgo*, políticas de *mínimo privilegio* y *telemetría continua*: VLANs dedicadas a IoMT con *ACLs/Firewall* para tráfico Este-Oeste, *NAC* para control de acceso por perfil de dispositivo, *cifrado* (*TLS 1.3/SSH*) en gestión y datos, *deshabilitación de Telnet/HTTP*, y *detección/correlación* mediante *NIDS+SIEM* (p. ej., *Snort/Wazuh*). Más adelante se presenta la *topología segmentada propuesta*, que mitiga estos riesgos y normaliza el flujo detección, correlación y respuesta [21, 23, 30].

2.3 Clasificación y priorización de amenazas

Para orientar la mitigación, las debilidades identificadas se agruparon y priorizaron considerando tres criterios: *exposición* (ubicación en la red, autenticación y cifrado disponibles), *explotabilidad* (existencia de *exploits* públicos, complejidad del ataque, credenciales por defecto/servicios legados) y *criticidad clínica* (impacto sobre disponibilidad, integridad y seguridad del paciente). Se aplicó un esquema cualitativo *alto/medio/bajo*; en empates, se privilegia el *impacto clínico* [1, 6, 9]. La *Tabla I* resume las categorías resultantes y alinea, para cada una, *contramedidas de prevención/detección/respuesta* (p. ej., *segmentación* y *NAC*; *NIDS/SIEM* para correlación; aislamiento automático del activo), de acuerdo con prácticas recomendadas para IoMT.

Tabla I. Vulnerabilidades comunes en dispositivos IoMT y medidas de mitigación recomendadas [17, 18, 27].

Vulnerabilidad	Nivel de riesgo	Ejemplo de ataque	Mitigación recomendada
Firmware desactualizado	Alto	Explotación de vulnerabilidad conocida	Gestión de parches periódica
Credenciales por defecto	Alto	Fuerza bruta a interfaz Webmin	Políticas de contraseñas y autenticación MFA
Tráfico sin cifrado (HTTP/Telnet)	Alto	Intercepción de datos sensibles	Uso de TLS 1.3 y SSH
Red sin segmentación	Medio	Movimiento lateral entre nodos	Implementación de VLAN y firewall internos
Falta de monitoreo en tiempo real	Medio	Actividad no detectada del atacante	Integración con SIEM (Wazuh, Snort)

3 Análisis del protocolo de protección IoMT

3.1 Enfoque General Del Protocolo

El protocolo se organiza en tres fases complementarias—*prevención*, *detección* y *respuesta*— que habilitan un enfoque integral capaz de anticipar amenazas, identificarlas y neutralizarlas en tiempo real [11, 21]. En prevención, prioriza la segmentación por función y riesgo (*VLAN/ACL*), el control de acceso a la red basado en el perfil del dispositivo y el principio de mínimo privilegio, el endurecimiento e inventario con gestión de parches, y el cifrado de gestión y datos (*TLS 1.3/SSH*) [22, 25]. En detección, establece telemetría continua y normalización de registros, correlación de eventos en *SIEM* y firmas/reglas en *NIDS* para descubrir patrones anómalos o indicadores de compromiso en dispositivos IoMT [26, 28]. En respuesta, automatiza playbooks que incluyen el aislamiento dinámico del activo (cambio de *VLAN*), bloqueo temporal del tráfico (*firewall-drop*), revocación de credenciales y notificación coordinada a equipos biomédicos y de TI, siguiendo pasos de contención, erradicación y recuperación [29]. El diseño se apoya en herramientas de código abierto (p. ej., *Snort/Wazuh*) y en políticas reproducibles, con el objetivo de reducir *MTTD/MTTR* y sostener la operación clínica sin comprometer la seguridad del paciente [30].

3.2 Componentes técnicos del protocolo

Cada fase del protocolo incorpora controles específicos (véase *Tabla II*). En *prevención*, se aplican autenticación multifactor, cifrado en tránsito con *TLS 1.3* y desuso de Telnet/HTTP, políticas de *RBAC* y segmentación por *VLAN/ACL* con *NAC* para hacer cumplir el mínimo privilegio y la separación por riesgo [21, 22, 25, 26, 27]. En *detección*, se integran *Wazuh* (recolección/normalización de registros, reglas y correlación) y *Snort* (NIDS/IPS con firmas personalizadas) para el análisis en tiempo real de eventos del sistema y del tráfico de red [12, 28, 30]. En *respuesta*, se orquestan *playbooks* y *scripts* para el aislamiento dinámico del activo (cambio de VLAN, *firewall-drop*), el bloqueo de IP maliciosas, la revocación de credenciales y la notificación, garantizando además la generación y preservación de evidencias para auditoría forense [13, 27, 29].

Tabla II. Fases del protocolo propuesto y sus componentes técnicos [21, 22, 25, 26, 27, 28, 29, 30].

Fase	Medidas incluidas	Herramientas/Implementación
Prevención	- Autenticación multifactor (MFA) - Control de acceso RBAC - Cifrado TLS 1.3 - Segmentación de red (VLAN)	Configuración de switches, políticas de red, certificados digitales
Detección	- Monitoreo de tráfico - Análisis de logs en tiempo real - Correlación de eventos	Wazuh, Snort
Respuesta	- Bloqueo automático de IPs - Alerta al administrador - Registro de incidentes - Auditoría post-evento	Scripts Bash/Python, integración Wazuh-Slack/Email

3.3 Lineamientos de integración en entornos hospitalarios

Los lineamientos clave para la integración en entornos hospitalarios, basados en casos de éxito y estándares vigentes, permiten una implementación sin hardware propietario mediante el uso de herramientas libres y estándares abiertos que se adaptan fácilmente a infraestructuras existentes (como servidores x86, máquinas virtuales o contenedores) [12, 14, 21, 22].

De forma general, se recomienda:

- **(i)** Agrupar los dispositivos IoMT en *VLAN dedicadas* con *ACL/Firewall* para limitar el tránsito este–oeste [25, 27].
- **(ii)** Ubicar un *NIDS* (p. ej., Snort) en puntos estratégicos para visibilizar intentos de acceso o explotación [30].
- **(iii)** Centralizar *correlación, alertamiento* y registro en *Wazuh/SIEM*, con normalización de eventos y *umbrales de severidad* [28, 29].
- **(iv)** Habilitar *respuestas automatizadas* (aislamiento lógico por VLAN, bloqueo temporal de IP, deshabilitación de servicios inseguros, *playbooks* de *hardening*) [25, 29].
- **(v)** Reforzar superficies de gestión mediante *TLS/SSH y autenticación robusta* [21, 22].

La arquitectura de referencia resultante facilita la integración de dispositivos IoMT, servidores clínicos y estaciones de monitoreo sin interrumpir servicios y, al mismo tiempo, reduce el *movimiento lateral* y mejora la *detección temprana* de incidentes [25, 27, 30].

4 Validación técnica del protocolo

4.1 Simulación de intrusión a Webmin 1.910 (escenario ofensivo)

La validación se efectuó en un entorno virtual conformado por máquinas virtuales configuradas con el único fin de ejecutar la prueba; el servidor Webmin 1.910 fue replicado en VM y los ataques se realizaron como simulaciones sobre esas instancias. Desde una estación atacante con Kali Linux, un actor realizó escaneos de puertos y *fingerprinting* del servicio, identificó el puerto *10000/tcp* (consola de administración) y confirmó la ausencia de TLS. Posteriormente, ensayó credenciales débiles y, tras autenticarse, ejecutó el módulo de *Metasploit* correspondiente, con lo que obtuvo una sesión remota sobre el sistema. La simulación reproduce un patrón frecuente en IoMT —superficies de gestión expuestas, credenciales por defecto y cifrado inexistente— que facilita el movimiento lateral y el control del host [15, 19, 20].

Metodología de la simulación:

1. *Reconocimiento.* - Exploración dirigida del puerto de gestión (*-p 10000*) y servicio asociado (*Nmap*), verificando respuesta de un servicio administrativo en esa interfaz.
2. *Verificación de exposición.* - Acceso a la consola en claro (*HTTP*) y confirmación de Webmin 1.910.
3. *Autenticación débil.* - Ingreso con credenciales triviales para simular un caso realista de políticas de contraseñas insuficientes.
4. *Explotación autenticada.* - Configuración del módulo de Metasploit para Webmin y ejecución del payload (*reverse shell*), comprobando acceso remoto efectivo al servidor.

Resultados de la simulación. La combinación de gestión sin *TLS + credenciales débiles* permite al atacante interceptar o probar accesos con alta probabilidad de éxito y ejecutar comandos con privilegios [20]. La figura 2 resume el proceso: (A) el escaneo de Nmap identifica el puerto *10000/tcp* expuesto y (B) la explotación con Metasploit culmina en la apertura de una sesión remota.

Controles de mitigación recomendados:

- Cifrado en la administración (*TLS 1.3* o *túneles SSH*) y deshabilitar *HTTP*.
- Políticas de contraseñas robustas + bloqueo por intentos fallidos.
- Restricción de acceso a la consola (listas de control, solo desde VLAN/segmento de administración).
- Actualización de Webmin y hardening del sistema (mínimos servicios expuestos).
- Detección y correlación: reglas NIDS (p. ej., Snort) para tráfico al 10000/tcp y monitoreo centralizado en Wazuh/SIEM con alertas tempranas.

Fig. 2a. Escaneo dirigido con Nmap: confirmación de *10000/tcp* abierto (consola de administración Webmin) en el objetivo.

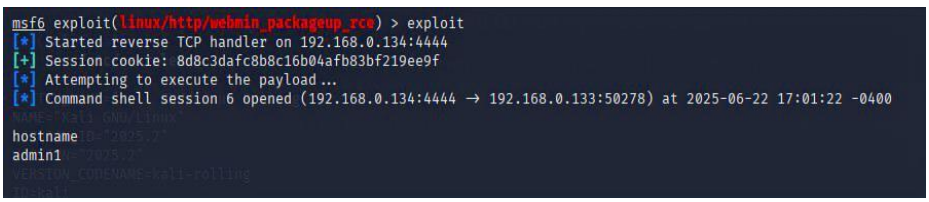

Fig. 2b. Explotación autenticada con Metasploit (*webmin_packageup_rce*): apertura de sesión remota por reverse TCP y evidencia de ejecución de comandos en el host.

4.2 Detección y monitoreo de intrusiones

Durante la fase de *detección*, se integraron un *NIDS* (Snort) y el *SIEM* (Wazuh) con el objetivo de identificar, en tiempo real, accesos indebidos a la consola de administración *Webmin (10000/tcp)* y eventos asociados al intento de explotación [16, 28]. Snort inspeccionó el tráfico en los puntos de control entre la VLAN de gestión y el segmento IoMT, mientras que Wazuh centralizó la recolección y normalización de

registros del servidor y de la red, aplicando reglas de *correlación* y *severidad* para priorizar el tratamiento del incidente [29, 30].

En la verificación inicial quedó evidenciada la *exposición del servicio 10000/tcp* y, cuando correspondió, el *acceso por HTTP sin TLS* (Fig. 3a–b). Con la vigilancia habilitada, *Snort* emitió alertas ante intentos de acceso o explotación a la consola (p. ej., *attempted-admin*, *web-application-attack*), mientras *Wazuh* correlacionó dichos eventos con los registros del host, *elevando la criticidad* cuando coexistieron múltiples indicios en una misma ventana temporal [28, 30]. La instrumentación implementada *proporcionó visibilidad temprana* y *posibilitó la priorización* del incidente antes de que se materializara un control sostenido del sistema [28, 29].

Fig. 3a. Exposición del servicio de administración en *10000/tcp* (Nmap; detección de *MiniServ/Webmin 1.910*)

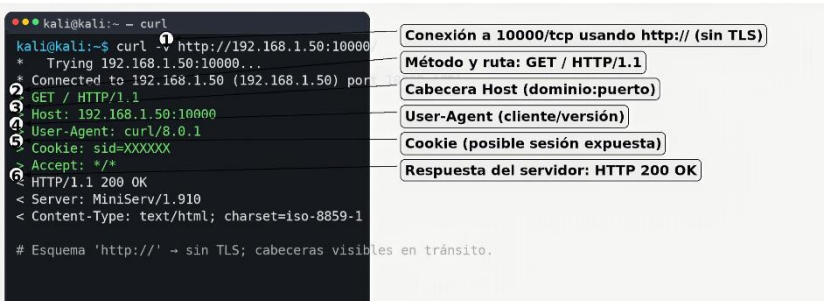

Fig. 3b. Acceso *HTTP sin TLS* a Webmin (*http://<IP>:10000*): cabeceras *GET, Host, User-Agent y Cookie* visibles

Con la vigilancia activada, el NIDS (Snort) generó alertas ante intentos de acceso al *10000/tcp* desde segmentos no autorizados y ante tráfico *HTTP* dirigido a la consola de Webmin. Dichos eventos fueron correlacionados en *Wazuh*, que elevó la severidad cuando coincidieron indicadores como *fallos de autenticación repetidos* y eventos *event.action=command_blocked*, priorizando el tratamiento del incidente (*Fig. 4a*) [28, 30].

Para validar la detección y orientar la respuesta, el equipo inspeccionó la consola del servidor afectado y confirmó el estado del sistema tras el intento. Esta acción respaldó la implementación de medidas de contención (*ACL/Firewall, aislamiento por VLAN*) y de remediación *(forzar TLS 1.3, deshabilitar HTTP, fortalecimiento de credenciales*) (Fig. 4b) [29].

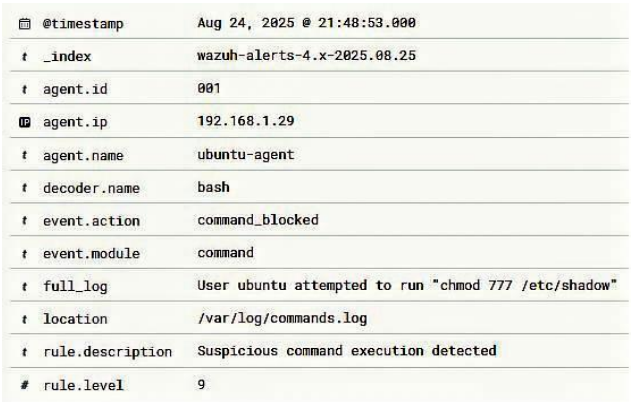

Fig. 4a. Registro en *Wazuh/SIEM* con evento *command_blocked (rule.level=9*) y metadatos del agente (ip, nombre, *decoder* bash, ubicación del log)

```
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen
 1000
    link/ether 00:0c:29:87:8a:fb brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.1/24 scope global ens37
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe87:8afb/64 scope link
       valid_lft forever preferred_lft forever
```

Fig. 4b. Consola del host afectado: salida de *ip addr* mostrando interfaces/estado de red posteriores al intento

4.3 Medidas preventivas aplicadas al entorno IoMT

En la fase final se aplicaron controles preventivos orientados a reducir la superficie de ataque y a incrementar la visibilidad del entorno [17, 26]. La red se segmentó mediante *VLAN dedicadas para IoMT* con *ACL/Firewall* que limitan el tráfico este–oeste y restringen la consola de administración exclusivamente a la *VLAN de gestión* [25, 27]. En paralelo, se endurecieron las superficies de administración: *deshabilitación de HTTP/Telnet*, adopción de *TLS 1.3/SSH, políticas de contraseñas robustas* con bloqueo por intentos fallidos y, cuando aplicó, *MFA* [21, 22, 26]. La *Figura 5* muestra la topología resultante, con el segmento IoMT aislado y los puntos de inspección y monitoreo (*Snort/Wazuh*).

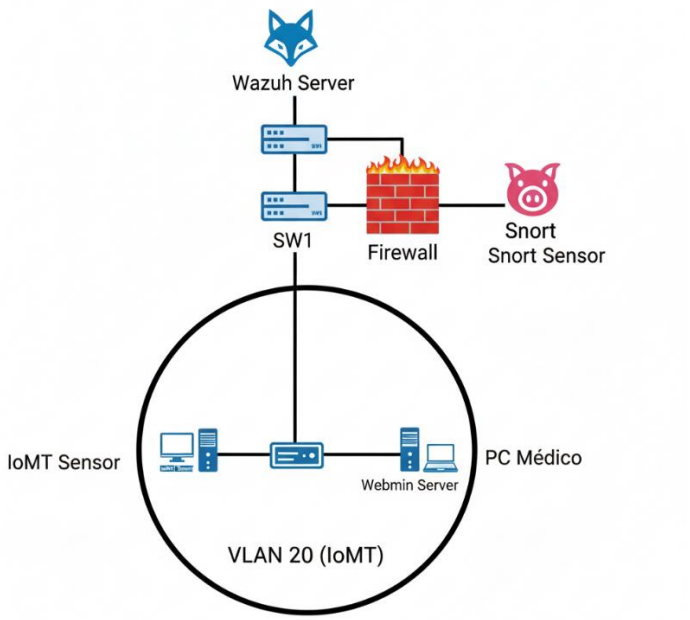

Fig. 5. Topología segmentada propuesta para entornos hospitalarios: *VLAN IoMT* aislada, *Firewall/ACLs* controlando el tránsito Este–Oeste, *IDS/IPS* (*Snort*) para inspección y *Wazuh/SIEM* para correlación y respuesta

El cifrado de comunicaciones se verificó por captura de red, confirmándose el tránsito como *Encrypted Application Data* bajo *TLS 1.3* (véase Figura 1b) [21, 22]. Adicionalmente, se reforzó la telemetría: reglas *NIDS* (Snort) para vigilar accesos al puerto de administración y correlación en *Wazuh/SIEM* con elevación de severidad ante coincidencia de intentos fallidos y *command_blocked* [28, 29, 30]. Finalmente, se habilitaron respuestas automatizadas para contención (aislamiento por VLAN, bloqueo de IP, deshabilitación temporal de servicios inseguros), cuya ejecución se ilustra en la *Figura 6* [25, 29].

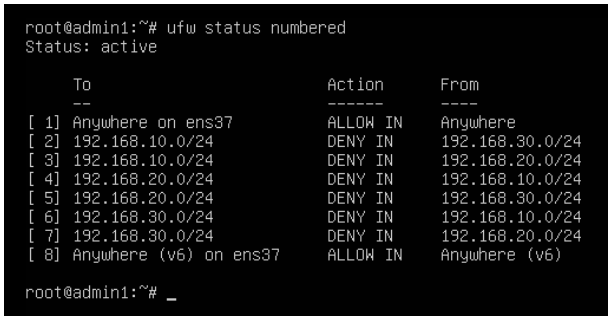

Fig. 6. Ejecución de respuesta automática ante alerta: disparo de script de contención desde la plataforma de monitoreo tras la correlación del evento

5 Conclusiones

El análisis realizado evidenció que los dispositivos IoMT presentan vulnerabilidades estructurales recurrentes, entre ellas el uso de credenciales por defecto, la ausencia de cifrado en las comunicaciones y la falta de segmentación lógica en las redes hospitalarias. Estas debilidades representan un riesgo crítico para la confidencialidad de los datos médicos y la seguridad operacional de los entornos clínicos, cumpliendo así con el primer objetivo específico.

Con base en dichos hallazgos, se diseñó un protocolo integral de ciberseguridad que articula medidas preventivas, mecanismos de detección de amenazas y estrategias de respuesta automatizada. El protocolo se basa en herramientas de código abierto como Wazuh y Snort, lo que lo convierte en una propuesta viable y escalable para instituciones de salud con limitaciones presupuestarias, en cumplimiento del segundo objetivo específico.

La validación práctica del protocolo se desarrolló mediante simulaciones de ataque y defensa sobre un servidor vulnerable con Webmin. Durante estas pruebas, se logró reducir el tiempo de detección y respuesta ante amenazas, mejorando sustancialmente la capacidad del sistema para mitigar ataques en tiempo real. Estas evidencias respaldan el tercer objetivo específico, orientado a establecer un sistema de monitoreo continuo.

Complementariamente, se evidenció que la segmentación de red mediante VLAN, el uso de cifrado TLS 1.3 y la automatización de respuestas ante incidentes permiten elevar significativamente el nivel de protección en infraestructuras clínicas modernas, especialmente aquellas que integran dispositivos IoMT conectados permanentemente.

En síntesis, el marco desarrollado cumple con el objetivo general de esta investigación, al ofrecer una solución integral que mejora la postura de ciberseguridad en entornos hospitalarios, protege la información sensible y salvaguarda la integridad de los dispositivos médicos conectados frente a amenazas cibernéticas emergentes. Sin embargo, aún persisten desafíos como la escalabilidad del monitoreo basado en reglas, la interoperabilidad de estándares entre fabricantes y la detección de amenazas avanzadas, los cuales constituyen oportunidades relevantes para futuras investigaciones [18].

Como línea de continuidad, se propone validar el protocolo a escala multisedes; profundizar la microsegmentación y el control de acceso (*NAC 802.1X/SDN*); extender el cifrado extremo a extremo (*TLS 1.3/mTLS*) a *DICOM/HL7/FHIR* [24]; y automatizar el inventario y la gestión de vulnerabilidades de IoMT (*SBOM*, *CVE*). Asimismo, conviene explorar detección basada en comportamiento y correlación avanzada en Wazuh (anomalías/ML), la orquestación de respuesta (*SOAR*) para aislamientos automáticos y *deception/honeypots*; complementado con ejercicios de resiliencia clínica (*purple-team*) y seguimiento de métricas *MTTD/MTTR*, cuidando la privacidad y la retención de logs [23].

Referencias

[1] A. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment," Computer Networks, vol. 144, pp. 190–204, 2019.

[2] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, and K. Fu, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in IEEE Symposium on Security and Privacy, 2008, pp. 129–142.
[3] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, 2016.
[4] B. P. Matt, "The cyber risks of the Internet of Medical Things," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 10–15, 2020.
[5] Asamblea Nacional del Ecuador, "Ley Orgánica de Protección de Datos Personales," Registro Oficial Suplemento 459, 2021.
[6] S. S. Chowdhury, M. S. Kaiser, and M. Akbar, "A survey on cybersecurity for IoT and IoMT: Issues, challenges, and research opportunities," in Proc. of 2020 IEEE International Conference on Computer and Information Technology (ICCIT), 2020, pp. 1–8.
[7] R. Zhang and L. Mi, "Cybersecurity for the internet of medical things: The challenge of regulating known unknowns," Journal of Internet Law, vol. 22, no. 2, pp. 12–19, 2018.
[8] A. Singh, R. Sandhu, and D. S. Rana, "Security challenges and cyber threat taxonomy in Internet of Medical Things (IoMT)," in Proc. of 2019 IEEE Int. Conf. on Data Science and Engineering (ICDSE), 2019, pp. 20–24.
[9] L. Tamersoy, E. Acar, B. Durak, and B. Barak, "Risk assessment and security for IoMT systems: A taxonomy and case studies," IEEE Access, vol. 8, pp. 103909–103927, 2020.
[10] J. Suo, K. Singh, and S. Chandrasekharan, "Cybersecurity challenges for IoMT: A systematic review," Journal of Healthcare Engineering, vol. 2018, pp. 1–12.
[11] A. Alhussein, M. S. Elhoseny, and K. Shankar, "A secure data sharing model using blockchain and cloud storage for IoMT," IEEE Access, vol. 8, pp. 192698–192710, 2020.
[12] J. Voas, "Cybersecurity for the internet of things," IEEE Computer, vol. 49, no. 10, pp. 61–64, 2016.
[13] J. R. Butts and S. Shenoi, *Critical Infrastructure Protection V*, Springer, 2011.
[14] H. Attarwala, "IoMT: A revolution in medical technology," IEEE Instrumentation & Measurement Magazine, vol. 23, no. 3, pp. 27–34, 2020.
[15] D. Kotz, C. A. Gunter, S. Kumar, and J. P. Weiner, "Privacy and security in mobile health: A research agenda," Computer, vol. 49, no. 6, pp. 22–30, 2016.
[16] L. G. Ko, B. S. Park, and H. J. Kang, "Security enhancement in IoMT through machine learning techniques," in Proc. of 2020 IEEE International Conference on Consumer Electronics (ICCE), 2020, pp. 1–4.
[17] T. W. Tay and S. J. Hsiao, "Cybersecurity in medical devices: An overview of risks and recommendations," Healthcare Technology Letters, vol. 7, no. 4, pp. 107–112, 2020.
[18] Y. Zhang, W. Liu, S. Xu, and H. Wang, "IoT security: Ongoing challenges and research opportunities," IEEE Transactions on Services Computing, vol. 13, no. 6, pp. 1072–1084, 2020.
[19] NVD, "CVE-2019-12840: Webmin through 1.910 'Package Updates' RCE (authenticated)." 2019. Accedido: 16-sep-2025.
[20] Tenable/Nessus, "Webmin ≤ 1.910 Remote Command Execution (Plugin ID 146488)." 2021. Accedido: 13-sep-2025.
[21] E. Rescorla, RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3, RFC Editor, 2018. Accedido: 13-sep-2025.
[22] Y. Sheffer et al., RFC 7525 (BCP 195): Recommendations for Secure Use of TLS and DTLS, RFC Editor, 2015. Accedido: 13-sep-2025.
[23] DICOM Standard, PS 3.15 – Security and System Management Profiles (Ed. 2025c), NEMA/MITA. Accedido: 13-sep-2025.
[24] HL7, FHIR Security (Communications Security, Authentication/OAuth), build.fhir.org (v6.0.0-ballot3). Accedido: 13-sep-2025.
[25] NIST, SP 800-207: Zero Trust Architecture, 2020. Accedido: 13-sep-2025.
[26] IEEE, IEEE Std 802.1X-2020: Port-Based Network Access Control, 2020. Accedido: 13-sep-2025.
[27] IEC, IEC 80001-1:2021 – Application of risk management for IT-networks incorporating medical devices, 2021. Accedido: 13-sep-2025.
[28] Wazuh Docs, Rules classification (levels 0–16), versión "current". Accedido: 16-sep-2025.
[29] Wazuh Docs, Active Response (firewall-drop / casos de uso), versión "current". Accedido: 16-sep-2025.
[30] Snort Project, Snort — Open Source IPS (overview / docs Snort 3), snort.org. Accedido: 16-sep-2025