FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS
UNIVERSIDAD CENTRAL DEL ECUADOR

INGENIO
2024, VOL 7(1), enero-JUNIO, pp. 118- 127

REVISTA INGENIO

Análisis de Vulnerabilidades en Equipos de TO de Grado Médico en el Hospital de SOLCA Núcleo de Quito

Vulnerability Analysis in Medical Grade OT Equipment at the SOLCA Nucleus Hospital in Quito

Gerardo Iván Cajamarca Méndez 1 | ID Instituto Superior Tecnológico Rumiñahui (Ecuador)
Mario Giovanny Ron Gavi 2 | ID Instituto Superior Tecnológico Rumiñahui (Ecuador)
María Gabriela Vera 3 | ID Instituto Superior Tecnológico Rumiñahui (Ecuador)
María Karina Alvarado Figueroa 4 | ID Instituto Superior Tecnológico Rumiñahui (Ecuador)
Bryan Alexander Cajamarca Albán 5 | ID Universidad Central del Ecuador (Ecuador)

HISTORIA DEL ARTÍCULO
Recepción: 13/10/2023
Recepción tras revisión: 13/11/2023
Aprobación: 4/12/2023
Publicación: 31/1/2024

PALABRAS CLAVE
Equipos OT, SOLCA, salud, Seguridad de la información, Tenable OT, vulnerabilidades, riesgo informático

RESUMEN
La importancia de la seguridad de la información que contienen los equipos médicos de un Sistema Hospitalario (SH) es primordial para el seguimiento del estado de salud del paciente. El SH se abastece de equipos cada vez más avanzados tecnológicamente por el alcance de los resultados, los mismos están conectados a la red del SH, si no hay un control adecuado en la administración pueden ser vulnerables ante ataques cibernéticos e impedir el normal funcionamiento de la red hospitalaria y comprometer el historial médico de un paciente, poniendo en riesgo su salud. Nace el interés médico, en poner bajo protección, los equipos OT (tecnología operativa), equipamiento que apoya los procesos industriales y críticos en tiempo real de un SH, para precautelar la información de un paciente. El Hospital Solca Quito, realizará un análisis de vulnerabilidades bajo la herramienta Tenable OT, obteniendo la identificación de los activos, los riesgos y acciones inmediatas, lo que permitirá trabajar de manera segura.

ARTICLE HISTORY
Received: 13/10/2023
Received after revision: 13/11/2023
Approved: 4/12/2023
Accepted: 31/1/2024

KEY WORDS
OT Equipment, SOLCA, health, information security, Tenable OT, Vulnerabilities, informatics risk

ABSTRACT
The importance of the information security contained in the medical equipment of a Hospital System (HS) is crucial for monitoring the patient's health status. The HS relies on increasingly technologically advanced equipment due to the scope of the results; these are connected to the HS network. Without proper control in administration, they can be vulnerable to cyberattacks, disrupting the normal functioning of the hospital network and compromising a patient's medical history, endangering their health. The medical interest arises in protecting the Operational Technology (OT) equipment, which supports real-time industrial and critical processes within an HS, in order to safeguard patient information. Hospital Solca Quito will conduct a vulnerability analysis using the Tenable OT tool, identifying assets, risks, and immediate actions, enabling working in a secure way.

1. INTRODUCCIÓN

En la era digital actual, la tecnología ha revolucionado la industria de la atención médica de manera impresionante. Desde la gestión de registros de pacientes hasta los dispositivos médicos conectados a Internet, los avances tecnológicos han mejorado la eficiencia y la calidad de la atención médica [1]. Sin embargo, esta interconexión también ha traído consigo un riesgo creciente: la vulnerabilidad de los datos y sistemas médicos ante amenazas cibernéticas. La información de salud es altamente sensible y privada. Incluye datos médicos confidenciales, historiales de tratamiento y diagnóstico, información de seguros y datos personales. Un ciberataque exitoso podría exponer estos datos a manos no autorizadas, lo que puede tener consecuencias devastadoras para la privacidad y la dignidad de los pacientes. La pérdida de confidencialidad en la atención médica puede llevar a la discriminación, el robo de identidad y la pérdida de confianza en los profesionales de la salud[2].

La interrupción de los servicios médicos debido a ataques cibernéticos puede tener consecuencias graves. Los sistemas hospitalarios, dispositivos médicos y registros electrónicos son vitales para la atención médica moderna. Un ataque exitoso que inmovilice estos sistemas podría poner en riesgo la vida de los pacientes y causar el caos en

https://doi.org/10.29166/ingenio.v7i1.5935
pISSN 2588-0829
eISSN 2697-3243

fing.revista.ingenio@uce.edu.ec

los entornos de atención médica [3].

Los dispositivos médicos, como marcapasos y bombas de insulina, ahora están conectados a la red para monitoreo y ajuste remoto, estos dispositivos son objetivos potenciales para ataques cibernéticos. Un acceso no autorizado a estos dispositivos podría causar daño físico real a los pacientes. La ciberseguridad adecuada es esencial para proteger la salud y la seguridad de los pacientes que dependen de estos dispositivos. Las regulaciones, como la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) en los Estados Unidos, establecen estándares estrictos para la protección de la información de salud. El incumplimiento de estas regulaciones puede resultar en multas significativas y daño a la reputación de las organizaciones de atención médica [4]. La ciberseguridad efectiva es esencial para cumplir con estas regulaciones y evitar consecuencias legales y financieras adversas.

La formación de profesionales de la salud y el personal administrativo en ciberseguridad es esencial, estos son el eslabón más débil en la cadena de seguridad. La capacitación adecuada puede ayudar a prevenir ataques de ingeniería social y mejorar la seguridad en general. Por ello, la ciberseguridad en entornos médicos no es un lujo; es una necesidad crítica. La integridad, confidencialidad y disponibilidad de la información médica son fundamentales para la atención de calidad y la protección de la privacidad del paciente[5]. La interrupción de los servicios médicos y el daño a dispositivos médicos conectados a Internet pueden tener consecuencias mortales. Es imperativo que las organizaciones de atención médica inviertan en ciberseguridad, implementen prácticas sólidas y fomenten la educación y la conciencia en este ámbito. La seguridad cibernética y la atención médica están inextricablemente entrelazadas en la sociedad moderna, y solo a través de una protección sólida se pueden garantizar los beneficios continuos de la tecnología en la atención médica.

En Ecuador el Hospital de SOLCA(Sociedad de Lucha contra el cáncer), es una entidad de salud que se dedica a controlar o mitigar las consecuencias de un tumor en el cuerpo humano y con esto dar una mejor calidad de vida al paciente; para este fin adquiere equipos OT médicos de avanzada tecnología, dispositivos que se alimentan de los datos que arroje el estado de salud de un paciente[6]. Varios son los procedimientos que se realizan para estabilizar la salud de un paciente con cáncer, y esto conlleva a que es una enfermedad costosa económicamente, de mucha paciencia y voluntad.

En la cama de un paciente puede haber varios equipos OT médicos emitiendo datos de monitorización continua, "Como resultado, este típico entorno sanitario moderno debe soportar decenas de miles de equipos OT que se conectan a la red" del Sistema Hospitalario (SH)[7]. Administrar la seguridad de un SH, es todo un reto pues no solo debe velar por la protección de los datos a nivel empresarial sino también asegurar los datos de los equipos OT de línea médica y sus redes.

Los equipos OT de línea médica (como un escáner de resonancia magnética) se deben al mantenimiento y funcionalidad del fabricante, y los equipos empresariales (como un computador de escritorio) al Departamento de informática del SH. Pese a estas diferencias, el SH debe acoplarse a los requisitos que solicite el dispositivo médico para su correcto funcionamiento y el Departamento de informática deberá implementar lo necesario para que estos equipos médicos trabajen en conjunto dentro de la red con su equipo empresarial.

La Seguridad informática, se especializa en proteger al Sistema conectado en red de los ataques cibernéticos abarcando dos conceptos la seguridad física y lógica de los dispositivos, ambas custodian los datos de accesos no autorizados hacia un sistema informático[8]. Hay que aceptar el hecho de que todo sistema de información es quebrantable, lo que indica que incluso un Hospital puede ser severamente atacado en su red, el mismo que dispone de varios equipos OT de línea médica de diferentes fabricantes y no todos contienen la seguridad apropiada para proteger la información que se almacena en su software, en ciertos casos se trabaja aún con equipos médicos ya obsoletos sin ningún tipo de seguridad que fácilmente pueden ser vulnerados [9].

Varios han sido los ataques cibernéticos a nivel mundial en distintos SH. Sin ir tan atrás en el tiempo, en el 2020 cuando apareció la infección por COVID-19, aprovechando el caos que esta enfermedad trajo a varios países, fue atacada España por un ransomware "Newalquer" que enviaba correos electrónicos al personal sanitario camuflado con asunto del COVID-19 para ingresar al SH, inmovilizarlo y por último pedir dinero a cambio de devolver la información.

Al inicio de la pandemia en República Checa, un ransomware inactivó los equipos OT de línea médica del Hospital Universitario, perjudicando al paciente y al personal médico en intervenciones quirúrgicas y demás situaciones que atentaban contra la salud. Algo parecido sucedió en Estados Unidos, que por medio de un ciberataque quisieron causar lentitud en la funcionalidad de los equipos informáticos al Departamento de Salud y Servicios Humanos, pero no lo lograron. De igual manera en el Reino Unido, un ransomware WannaCry en el 2017 produjo un ataque a varias instituciones sanitarias en las que se solicitaba un rescate económico por el acceso al SH, el personal médico se vio en la necesidad de apagar el sistema informático junto con los equipos OT médicos [9]. Ante estos ataques a nivel mundial, se realizó un proyecto de revisión del alcance de los ciberataques contra el SH, lo que sirvió para varias reuniones, acuerdos y soluciones por un equipo con diversas disciplinas de profesionales, de tantos encuentros suscitados, resulta el tema de ciberseguridad en el SH; esto sucedió en el año 2018 dentro del foro bianual de salud de Ginebra, teniendo como fin

asegurar el ciclo de vida del equipo, mediante la identificación de los activos en caso de riesgo, capacitación a los usuarios, localización de vulnerabilidades, restricciones de accesos y control de privilegios administrativos, presentación de una línea de defensa ante un ataque y un plan de continuidad después del incidente, para que la ciberseguridad logre su objetivo en el entorno sanitario tanto el personal fabricante como el personal del SH deben mantener una buena comunicación para acrecentar la resistencia ante un ataque cibernético. [10]

La investigación se enfoca en un análisis de las vulnerabilidades que podrían comprometer la seguridad el equipamiento médico del Hospital de SOLCA Núcleo de Quito, el cual se suma a precautelar los activos e implementar barreras de defensa ante las posibles vulnerabilidades existentes en los equipos OT de grado médico, para el fin se realizará un análisis con la ayuda de la aplicación TENABLE TO, esta herramienta se presta para la seguridad del Internet de las cosas mediante el escaneo a toda la red en la que se obtendrán las vulnerabilidades de los equipos OT, los accesos no autorizados a sus datos y los riesgos humanos a los que se enfrentan [11].

Materiales

El cuadrante de Gartner permite evaluar equipos de la Tecnología Operativa (OT). Es una metodología que se utiliza principalmente para evaluar proveedores y soluciones en diversas áreas de tecnología de la información (TI), pero no se utiliza de manera común para evaluar equipos de OT en sí.

La OT se relaciona principalmente con sistemas y equipos utilizados en el sector empresarial e incluso equipos médicos. Para llevar una gestión de control de seguridad en equipos OT de grado médico, se debe tener claro que la línea de seguridad es compleja porque se va a tratar con equipos de diferentes fabricantes a nivel industrial y cada uno de ellos ha implementado un tipo de seguridad de acorde a sus intereses y alcances, esta forma de operar conlleva a una alta demanda de vulnerabilidades y costos operativos, por esta razón se implementan nuevas herramientas que permiten dar un seguimiento de seguridad de la información y del estado del equipo OT de cualquier fabricante. A continuación, un cuadro comparativo entre ambos equipos [7].

Tabla 1

Diferencias entre equipos OT de línea médica y empresariales

Funcionamiento	Equipo Médico Ot	Equipo Empresarial
Inicio de Sesión en la red	Registro como dispositivo médico	Registrado como dispositivo empresarial
Número de serie	Es el mismo que el del fabricante del equipo médico	Es el mismo que el del fabricante del equipo empresarial
Credenciales de usuario	Es un médico autorizado capacitado	Personal empresarial autorizado
Control/Propiedad del dispositivo	Departamento de tecnología médica	Departamento de informática
Software y versión del Sistema Operativo	Consiste con los requisitos del fabricante	Atiende a lo que la empresa requiera y el Departamento de informática lo ejecuta.
Escaneos	Según las especificaciones del fabricante	Cambia si el departamento de TI realiza actualizaciones
Agente de Seguridad de TI	Proporcionado por el fabricante del equipo OT	Según la política del departamento de TI

Nota: [7]

Según la Tabla 1 se muestra que los equipos OT de línea médica (como un escáner de resonancia magnética) se deben al mantenimiento y funcionalidad del fabricante, y los equipos empresariales (como un computador de escritorio) al Departamento de informática del SH. Pese a estas diferencias, el SH debe acoplarse a los requisitos que solicite el dispositivo médico para su correcto funcionamiento y el Departamento de informática deberá implementar lo necesario para que estos equipos médicos trabajen en conjunto dentro de la red con su equipo empresarial.

Las herramientas para realizar los controles de seguridad a este tipo de equipos, se mantiene en continuas actualizaciones porque la tecnología crece a medida de las necesidades requeridas, con la finalidad de poder analizar los riesgos a los que los equipos se puedan enfrentar para minimizar o prevenir ataques [12].

Dentro de los Sistemas de Control Industrial(SCI) se encuentran los equipos OT de grado médico, esta definición abarca a todos los sistemas de gestión y herramientas que tengan relación con procesos industriales[12]. Este tipo de sistemas permite realizar una enumeración de todos los activos técnicos que estén conectados a la red, comprendiendo todos los equipos de hardware hasta licencias de software, incluyendo a los activos más importantes categorizados como activos

críticos por su facilidad de ser vulnerables ante ciberataques informáticos.

Las consecuencias de un ataque cibernético en un equipo OT puede llegar desde provocar la pérdida de los datos, robo de los derechos de propiedad intelectual, interrupción operativa de los equipos hasta causar daños irrecuperables en el sistema llevando a la organización a perder la confidencialidad, integridad y confianza de los clientes, para caer en la quiebra y cierre del negocio. La gerencia deberá tomar con grado de alta importancia el tema de valorar la seguridad informática de los equipos OT en la red, como medida de prevención o plan de continuidad ante un ataque informático. Para ello, en el mercado se dispone de varias herramientas que permiten llevar un control de la seguridad de equipos industriales desde el nivel informático.

Tabla 2
Herramientas existentes para la detección de activos OT y Análisis de vulnerabilidades

Herramienta	Fabricante	Característica	No brinda
Tenable OT	Tenable	Muestra todos los activos conectados a la red Facilita información de la vulnerabilidad basada en el riesgo	Clasificación de activos críticos
Axonius	Axonius	Identificación de activos sin administración	No muestra las vulnerabilidades
Scrutiny	Bayshore networks	Muestra las conexiones en la red y sus dispositivos	No muestra las vulnerabilidades
Claroty	Claroty	Detecta amenazas, presenta los activos críticos y presenta la gestión de los dispositivos.	No muestra la clasificación de los dispositivos en riesgo.
Nozomi network	Nozomi	Muestra los activos que están conectados a la red, notificaciones de cambios de hardware en la red y gestión de las vulnerabilidades	No muestra la clasificación de los activos en riesgo.
CyberX	CyberX	Presenta una topología de la red, los activos y la gestión de vulnerabilidades.	No muestra la clasificación de los activos en riesgo.
AT&T security	AT&T Business	Clasifica los activos críticos y las vulnerabilidades. Enlista todos los activos conectados a la red.	
Liu et al	Applied Risk		No clasifica los activos de riesgo
Shodan	Shodan	Muestra información de todos los activos en la red	No muestra la clasificación de los activos de riesgo ni vulnerabilidades.

Nota: [12]

En la investigación se utilizó la herramienta Tenable OT, la misma que fue implementada en la institución en modo licenciamiento, debido a la coyuntura actual del país en relación a la ley orgánica de protección de datos la misma que en su Art. 40 hace referencia al análisis de riego, amenazas y vulnerabilidades, que se deben realizan con la finalidad de precautelar los datos personales de los pacientes. Esta herramienta se comunica con los dispositivos sin comprometer el funcionamiento normal del dispositivo a manera de consulta, recopila la información de modo pasivo de manera que se pueda definir el idioma nativo del dispositivo y con esto recolectar datos de configuración, versiones de firmware, usuarios, vulnerabilidad, metadatos y otros problemas de seguridad [13] realizando seguimientos de cambios sean estos en la red o en el propio dispositivo, estos cambios son analizados y envía la notificación respectiva si se encuentra frente a un caso de inseguridad.

Tenable OT previene a las redes industriales de ataques cibernéticos, de agentes que comprometan la confidencialidad de la información y de errores humanos, identificando los activos y sus vulnerabilidades con el fin de solucionar estos accesos para garantizar la confiabilidad en el funcionamiento del equipo [14].

Figura 1
Entornos de OT

Nota: [14]

Principales Características:

- Visibilidad convergente: permite visualizar completamente de manera integral los componentes de OT e IT en cualquier plataforma de cómputo, usando las herramientas de Tenable como: SIEAM, SOAR, firewalls de próxima generación, firewalls basados en diodos, inventario de activos y gestión de cambios.
- Detección de amenazas: Mediante la metodología de detección múltiple, Tenable OT detecta cambios sospechosos en la red, aplica políticas de seguridad y emite alertas sobre ellas, las mismas que pueden originarse de fuentes externas o internas siendo ocasionadas por malwares o errores humanos. Tenable OT es capaza de reconocer incluso una amenaza de un equipo que no esté conectado a la red lo cual es útil para mitigar de manera ágil un respuesta inmediata, permitiendo a las organizaciones "detectar y mitigar los eventos de riesgos en los entornos de OT"[14]

- Control de gestión de activos: Se refiere a llevar un control de las versiones de firmware, sistema operativo, configuraciones, software, usuarios, número de series para todos los activos detectados en el inventario.
- Control de vulnerabilidades: Tenable OT, genera niveles de riesgo, puntuaciones de riesgo, sugerencias de mitigación a factores de riesgo con lo cual permite al personal debidamente autorizado a dar una solución rápido ante un ataque cibernético.
- Control de configuración: Mientras la organización se mantiene bajo las operaciones de Tenable OT, éste trabaja controlando cualquier cambio en la red sea por el personal operativo o algún malware de la misma red o en el mismo dispositivo llevando el registro respectivo, lo relevante de esta acción es que Tenable OT va guardando una copia de seguridad de los activos que tengan el estado Aceptable, por si se diera el caso de alguna anomalía, Tenable OT permite al usuario recuperar el último estado Aceptable del activo y continuar con el debido funcionamiento de los equipos. [15].

2. MÉTODO

Tenable OT puede proporcionar visibilidad completa de la infraestructura de TI y OT en un entorno médico, lo que incluye dispositivos médicos conectados, sistemas de control, redes y otros activos. Esta visibilidad es esencial para comprender la superficie de ataque y detectar posibles vulnerabilidades. Así como, es capaz de identificar y evaluar vulnerabilidades en una amplia gama de dispositivos y sistemas, incluidos los dispositivos médicos. Esto ayuda a los equipos de seguridad a identificar de manera proactiva las debilidades en estos antes de que puedan ser explotados por amenazas cibernéticas.

La plataforma Tenable OT clasifica y prioriza las vulnerabilidades según su gravedad y el impacto potencial en la seguridad del entorno. Esto permite a los profesionales de seguridad enfocar sus esfuerzos en abordar las vulnerabilidades más críticas y reducir el riesgo. Puede ayudar a las organizaciones de atención médica a demostrar el cumplimiento al identificar y abordar las vulnerabilidades que podrían poner en riesgo la privacidad y seguridad de los datos del paciente.

Además de la evaluación de vulnerabilidades, Tenable OT también puede detectar actividad sospechosa y amenazas en tiempo real en los sistemas médicos. Esto es crucial para identificar y responder rápidamente a posibles ataques cibernéticos. Proporcionando informes detallados que pueden ser útiles para las auditorías de seguridad y para comunicar los resultados a las partes interesadas en la organización de atención médica, incluyendo la alta dirección y las autoridades reguladoras.

De acuerdo con la realidad de la institución se determinó la factibilidad del uso de la herramienta de análisis de vulnerabilidades para equipos OT (Tenable OT), la misma que se ha implementado debido al despliegue de su esquema de seguridad en la actualidad.

Es de gran importancia recalcar la apertura de la institución en temas de seguridad de la información y la preocupación del aseguramiento de su infraestructura tecnológica que ha hecho posible que esta herramienta esté disponible para este trabajo ya que herramientas como esta, son de difícil acceso tanto por su costo como por su poca socialización en giros de negocio similares.

La metodología de investigación a utilizar para alcanzar los objetivos del presente proyecto es la mixta, ya que se va a realizar la exploración directa a través de la herramienta de análisis de vulnerabilidad planteada. La metodología cuantitativa se utilizará en la elaboración de análisis de riesgo con la finalidad de conocer: ¿Cuáles son las vulnerabilidades más comunes en los equipos OT analizados?, ¿Cuáles son los equipos y fabricantes con más riesgo? y ¿Cuáles son las vulnerabilidades más severas?

La investigación se desarrolló en las siguientes fases:

Primera Fase. Una vez estudiado el contexto de la herramienta Tenable OT, se determinó que el nivel de madurez de la misma en base a su posicionamiento en el mercado de ciberseguridad a nivel mundial, como líder en análisis de vulnerabilidades; así como la estructura de su documentación y organización permitió la aplicación del documento "Checklist-ICS-Cyber-Security-

Considerations_es-la", con la finalidad de establecer una línea base sobre las áreas y los equipos OT con los que se va a trabajar.

Segunda Fase. Al evaluar el documento propuesto en la primera fase se determinó el alcance en cuanto los dominios de los criterios a utilizar en el presente trabajo los cuales se detallan a continuación: Visibilidad a lo largo de la infraestructura de TO, Inventario de activos, Detección de amenazas, Evaluación de vulnerabilidades y gestión de riesgo y Escala de riesgo proporcionada por el fabricante.

Tabla 3
Niveles de Riesgo tecnológico en Hospital SOLCA Núcleo Quito

	Riesgo Bajo (>=1<=30): Se mantiene vigilado, aunque no necesite de medidas preventivas.
	Riesgo Medio (>=31<=60): Realizar un análisis, de ser posible implementar medidas preventivas para reducir el nivel de riesgo caso contrario se mantienen controlada las variables
	Riesgo Crítico(>=61<=100): Implementación de medidas de mitigación y prevención ante un ataque cibernético.

Tercera Fase.
Análisis de resultados: Una vez que se implementó la herramienta de análisis la misma que está compuesta por un equipo de core que realiza el procesamiento de la información que es enviada por el segundo componente un, sensor en modo sniffer, se pudo identificar los equipos agrupados de acuerdo a las sub redes asignadas por la institución, de esta manera se logró inventariar los equipos OT de acuerdo a su criticidad declarada por la herramienta en base a su ¨know how¨ basado en varios factores como marca, modelo, fabricante y tipo; a fin de dar respuesta a las interrogantes planteadas.

¿Cuáles son las vulnerabilidades más comunes en los equipos OT analizados?

En la Fig. 1 se enumera las vulnerabilidades más comunes, por ejemplo, que el host remoto está escuchando en el puerto UDP 137 o en el puerto TCP 445, y responde a solicitudes NetBIOS nbtscan o SMB, otra vulnerabilidad hace referencia al envió de una solicitud de búsqueda al mapeador de puertos (TCP 135 o epmapper PIPE) con lo cual fue posible enumerar la Computación Distribuida de servicios de entorno (DCE) que se ejecutan en el puerto remoto. Usando esta información es posible conectar y vincular a cada servicio enviando una solicitud por RPC al puerto remoto.

Figura 2
Vulnerabilidades más comunes


Most Common Vulnerabilities

Name	Severity	VPR	Affected assets
Windows NetBIOS / SMB Remote Host Informati...	Info		1
Traceroute Information	Info		1
DCE Services Enumeration	Info		1
Microsoft Windows SMB NativeLanManager Re...	Info		1
SSL Certificate Information	Info		1
Microsoft Windows SMB Service Detection	Info		1
Nessus SYN scanner	Info		1
OS Identification	Info		1
Nessus Scan Information	Info		1

¿Cuáles son los equipos y fabricantes con más riesgo?

Como se puede observar en la Fig. 3 los equipos que presentan mayor riesgo son el de gamma cámara de marca Siemens, la estación de comando de la resonancia magnética de marca Hewlett Packard y un ecógrafo de marca Avalue Technology. Inc. Al ser equipos llave en mano se debe realizar una reunión con el fabricante para determinar el nivel de riesgo aceptable.

Figura 3
Listado de equipos de acuerdo con el riesgo


Highest Risk Assets

Name	Type	Risk	IPs	MACs	Vendor
MEDNUC_GAMMAC_2	OT Workstat...	36	192.16...	4c:5...	Siemens
IMA_RESONANCIA	OT Device	36	192.16...	84:a...	Hewlett...
IMA_ECO8	OT Device	36	192.16...	00:0...	Avalue ...
MEDNUC_GAMMAC_1	OT Workstat...	35	192.16...	90:1...	Fujitsu ...
IMA_ECO9	OT Device	35	192.16...	00:0...	Avalue ...
IMA_ECO7	OT Device	35	192.16...	00:0...	Advant...
MEDNUC_GAMMAC_1_PROC	OT Workstat...	35	192.16...	40:a...	HP
IMA_RX2	OT Device	35	192.16...	90:1...	Fujitsu ...
CITOM201	OT Device	33	192.16...	f4:39...	HP
CITFLU_MICROS	OT Device	32	192.16...	00:2...	CARL Z...

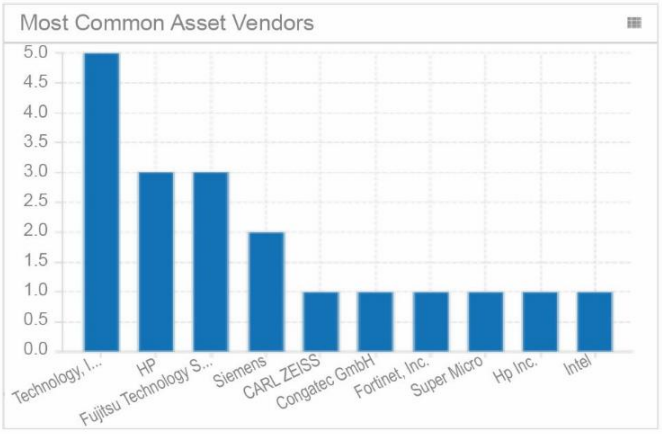
¿Cuáles son las vulnerabilidades más severas?

En la Fig. 4 se enumera las vulnerabilidades más severas, por ejemplo, la vulnerabilidad con severidad crítica indica que se puede ejecutar un código remotamente arbitrario, la vulnerabilidad baja indica que el host remoto permite conexiones SSL/TLS con uno o más Módulos del algoritmo Diffie-Hellman menores o iguales a 1024 bits, un atacante a través de criptoanálisis, puede recuperar el texto sin formato o violar potencialmente la integridad de las conexiones.

Figura 4
Vulnerabilidades Críticas

En la Fig. 5 y Fig. 6 (Anexo Fig.6) se muestra una visión general del equipamiento OT por fabricante y clasificado por el sistema operativo que utiliza.

Figura 5
Equipamiento Ot por fabricante



En la Fig. 7 (Anexo Fig.7) y Fig. 8(Anexo Fig.8) permite tener una visión holística de la distribución y comportamiento de los equipos OT en la infraestructura de networking del Hospital.

3. RESULTADOS Y DISCUSIÓN

En el ámbito hospitalario los equipos médicos especializados para procedimientos médicos generales y oncológicos son adquiridos a empresas que manejan sus soluciones con un formato "llave en mano" lo que implica que la gestión en su totalidad es por parte del proveedor en el manejo y soporte tanto operativo como tecnológico, lo cual implica que la institución hospitalaria pierda visibilidad de los mismo en su infraestructura, por eso la importancia de monitorear el ámbito de seguridad informática para verificar que los proveedores manejan estándares de seguridad mínimos para estos equipamientos; la herramienta utilizada provee una base de conocimiento propia para evaluar estas vulnerabilidades la misma que se está aprovechando para validar y minimizar el riesgo en la infraestructura del hospital[14]. En tal sentido, los resultados del análisis de vulnerabilidades en los equipos OT de la institución evidencia que existen 50 equipos de grado médico (OT) distribuidos principalmente en las áreas de Imagenología, Medicina nuclear, Radioterapia y áreas afines, mismos que soportan los procedimientos de análisis, diagnóstico y tratamiento oncológico en los pacientes, razón por la cual este equipamiento es crítico para el desempeño de las actividades médicas en el hospital por lo que su aseguramiento tecnológico es de vital importancia para reducir los riesgos y vulnerabilidades. Tomando en cuenta, que la mayoría de los dispositivos médicos utilizan tanto hardware como software para realizar operaciones críticas. Además, ya no están aislados y utilizan tecnologías de comunicación para proporcionar servicios sanitarios de calidad. Los dispositivos médicos en red han permitido mejorar las posibilidades de diagnóstico, tratamiento y enfermedades crónicas. La pronta proliferación en la interconectividad de los dispositivos médicos con otros sistemas relacionados ha mejorado profundamente la atención al paciente[16].

Los investigadores del mundo académico, la industria y anuncios públicos han informado con frecuencia de la presencia de vulnerabilidades de seguridad en el firmware de los dispositivos médicos conectados y sus causas subyacentes. El tema común es la ausencia de medidas de seguridad en el diseño de los sistemas electrónicos (software) que se integra en estos dispositivos, el software utilizado en los dispositivos médicos es de extrema importancia, ya que es responsable de funciones críticas[2]. Por otra parte, en el caso de los equipos médicos OT, la seguridad no se tuvo en cuenta al fabricar estos dispositivos y, por este motivo, utilizan protocolos inseguros[16]. Con relación a las vulnerabilidades encontradas se determinó que las mismas en su mayoría están categorizadas con un riesgo bajo el mismo que la institución los ha aceptado como política de seguridad, también se encontró 2 riesgos críticos relacionados a accesos remotos a los equipos mismos que fueron notificados a las empresas a cargo para su mitigación al ser soluciones llave en mano. Las vulnerabilidades presentes en el software de los dispositivos médicos son las principales responsables ciberataques en la sanidad[10].

En resumen, estos resultados subrayan la importancia de mantener estándares de seguridad óptimos para la seguridad de la información de la institución más aun tomando en cuenta la actualidad del país en cuanto a normativas que obligan a asegurar la información y datos personales de los pacientes. Se recomienda realizar auditorías continuas y programadas a fin de validar que las vulnerabilidades no rebasen el umbral de riesgo aceptado por el hospital. De acuerdo a la tabla Tabla 3, el umbral de riesgo aceptado por la institución es <=60 lo que corresponde a un nivel de riego medio y bajo.

De igual manera se debe complementar con análisis de seguridad a la red y accesos a sistemas críticos no médicos

y que tengan interoperabilidad con el equipamiento de grado médico (OT) a fin de garantizar la seguridad de la información a nivel general de la organización.

4. CONCLUSIONES

El análisis de las vulnerabilidades en equipos OT, permite tener una línea de vista del equipamiento médico en la institución que por años no se han podido analizar a profundidad a fin de determinar brechas de seguridad o corroborar el nivel de aseguramiento del proveedor dado que los mismos entregan estas soluciones como un esquema "llave en mano" que no pueden ser manipulados por el personal de TIC.

También se propone realizar en un futuro una comparativa de resultados de análisis de vulnerabilidades de equipos de grado médico (OT) en otras instituciones de salud a fin de determinar de manera macro el nivel de seguridad que los proveedores de estos equipamientos aplican.

De igual manera se logró determinar que esta herramienta ha sido de vital importancia para la administración, monitoreo y seguridad de esta área de infraestructura tecnológica de la organización.

A pesar de encontrar vulnerabilidades críticas puntuales en alguno de los equipos ha sido de gran valía determinar también que el riego se mantiene en medio (moderado) y mínimo a manera general en los equipos analizados.

La gestión de vulnerabilidades de estos equipos de grado médico (OT) aporta a la concientización de los administradores de sistemas y seguridad del hospital sobre la importancia de la seguridad ya que, los mismos son utilizados para manejo de información crítica de los pacientes al almacenar la información médica.

Las amenazas relacionadas con la confidencialidad incluyen situaciones en las que el adversario obtiene acceso no autorizado a información sensible. En las amenazas relacionadas con la integridad, el atacante manipula información sensible sin autorización. Sin embargo, los ataques relacionados con la disponibilidad incluyen casos en los que el adversario actúa para denegar servicios a usuarios legítimos.

Los ciberataques se dirigen a diferentes empresas, incluido el sector médico. Desde dispositivos médicos como marcapasos hasta instituciones médicas como hospitales y clínicas son objetivos vulnerables para los ciberdelincuentes. Las infracciones cibernéticas en el ámbito médico no sólo pueden poner en riesgo la vida de los pacientes, sino que también pueden provocar la fuga de datos sensibles y confidenciales. Debido a la naturaleza de los objetivos médicos y su importancia y sensibilidad, existe una gran necesidad de revisar e investigar las vulnerabilidades y debilidades actuales y pasadas dentro de los dispositivos y las instituciones médicas. Esta investigación tiene como objetivo investigar las vulnerabilidades recientes y actuales de las instituciones y dispositivos médicos y resaltar la importancia de las cuestiones de seguridad cibernética en esta área.

Se ha visionado como trabajo futuro incrementar el análisis de vulnerabilidades a equipos de grado médico (OT) que se los denomina móviles, en vista de que los mismos no mantienen una conexión permanente a la red de la organización y los mismos fueron catalogados como de menor riesgos por los coordinadores de las áreas analizadas.

REFERENCIAS

[1] S. F. Ahmed, M. S. Bin Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions," *Inf. Fusion*, p. 102060, Sep. 2023, doi: 10.1016/j.inffus.2023.102060.

[2] H. Verma, N. Chauhan, and L. K. Awasthi, "A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns," *Comput. Sci. Rev.*, vol. 50, p. 100591, Nov. 2023, doi: 10.1016/j.cosrev.2023.100591.

[3] S. A. Wagan, J. Koo, I. F. Siddiqui, M. Attique, D. R. Shin, and N. M. F. Qureshi, "Internet of medical things and trending converged technologies: A comprehensive review on real-time applications," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9228–9251, Nov. 2022, doi: 10.1016/j.jksuci.2022.09.005.

[4] P. O. Iyiewuare, I. D. Coulter, M. D. Whitley, and P. M. Herman, "Researching the Appropriateness of Care in the Complementary and Integrative Health Professions Part 2: What Every Researcher and Practitioner Should Know About the Health Insurance Portability and Accountability Act and Practice-based Research in the United States," *J. Manipulative Physiol. Ther.*, vol. 41, no. 9, pp. 807–813, Nov. 2018, doi: 10.1016/j.jmpt.2018.11.003.

[5] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, and R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," *Appl. Soft Comput.*, vol. 118, p. 108439, Mar. 2022, doi: 10.1016/j.asoc.2022.108439.

[6] A. Orozco, "*Sobrevida libre de enfermedad en pacientes con cáncer de recto localmente avanzado que recibieron quimio-radioterapia en Hospital SOLCA Quito"*, vol. 33, no. 1, pp.89, Quito, 2022.

[7] D. Citharthan, M. Varatharaj, and P. Rajan, "*Role of Cryptography and Its Challenges in Integrating Secured IoT Products"*, no. November, 2020. doi: 10.1201/9781003032441-3.

[8] J. F. Andrade, "Ciberseguridad y Salud," *INNDEV - Innov. Dev. Ciencias del Sur*, vol. 2, no. 1, pp. 1–11, 2023, [Online]. Available: https://www.itscs-cicc.com/ojs/index.php/inndev/article/download/47/17

[9] J. García and L. Herrero, "La ciberdefensa en los sistemas de información sanitarios militares," vol. 76, no. 3, pp. 140–142, 2020, doi: 10.4321/S1887-85712020000300001.

[10] S. T. Argaw *et al.*, "Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, pp. 1–10, 2020, doi: 10.1186/s12911-020-01161-7.

[11] B. C. Santamaría, "concepto de tres herramientas de gestión y análisis de vulnerabilidades," 2021.

[12] C. Liu, Y. Alrowaili, N. Saxena, and C. Konstantinou, "Cyber risks to critical smart grid assets of industrial control systems," *Energies*, vol. 14, no. 17, pp. 0–19, 2021, doi: 10.3390/en14175501.

[13] H. Pulkkinen, "SAFE SECURITY SCANNING OF A PRO- DUCTION STATE AUTOMATION Master of Science Thesis," December, 2022.

[14] H. D. E. Datos, "Tenable.ot™," 2023.

[15] E. L. D. D. E. La, "DE CIBERSEGURIDAD INDUSTRIAL," 2023.

[16] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019, doi: 10.1109/COMST.2019.2914094.

Anexo

Figura 6

Equipamiento OT por OS

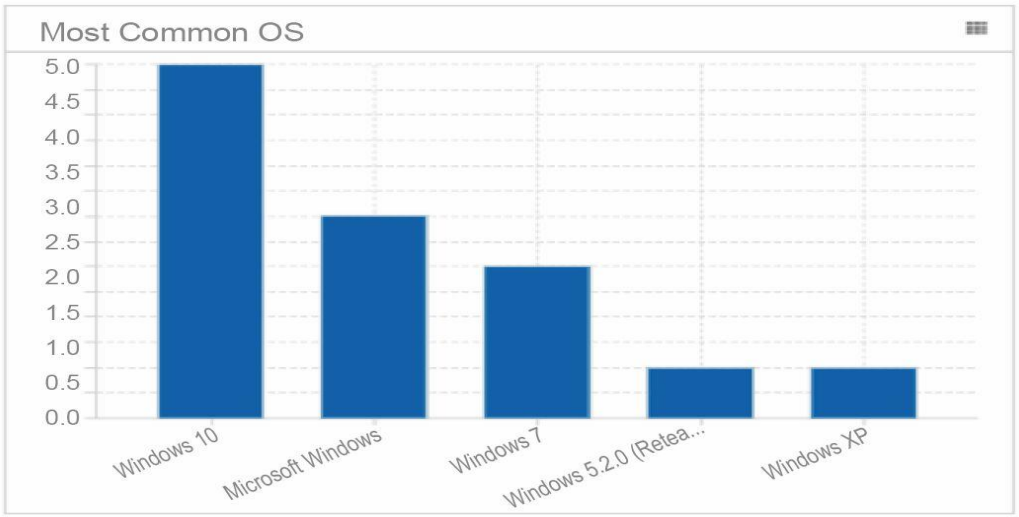


Figura 7

Mapa de red de equipos OT

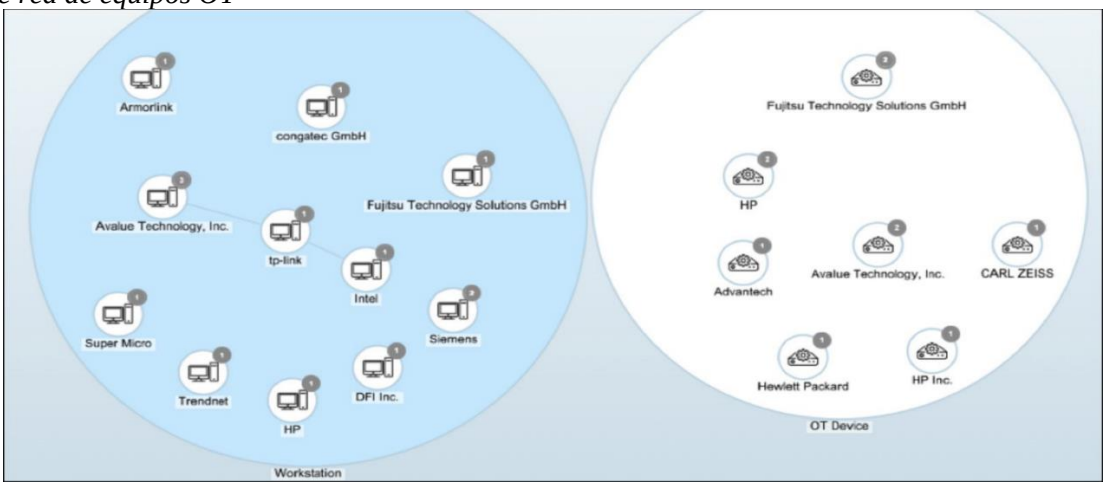


Figura 8

Tráfico de red de equipamiento OT