TLP:CLEAR

Guía de mitigación: sector de la atención médica y la salud pública (HPH)

Octubre de 2023
Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency)

Este documento está marcado como TLP:CLEAR. Los destinatarios pueden compartir esta información sin restricciones. La información está sujeta a normas estándar de derechos de autor. Para obtener más información sobre el protocolo de semáforo (TLP, por sus siglas en inglés), consulte http://www.cisa.gov/tlp.

Índice

Introducción

Esta Guía de mitigación de la Agencia de Ciberseguridad y Seguridad de la Infraestructura (CISA, por sus siglas en inglés) ofrece recomendaciones y prácticas recomendadas para combatir las amenazas cibernéticas generalizadas que afectan al sector de la atención médica y la salud pública (HPH, por sus siglas en inglés). Las vulnerabilidades identificadas en las organizaciones del sector de la HPH presentan oportunidades para mitigar los riesgos antes de que se produzcan intrusiones. Las vulnerabilidades no mitigadas aumentan la probabilidad de que los agentes de amenazas empleen con éxito tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) maliciosos contra organizaciones de HPH.

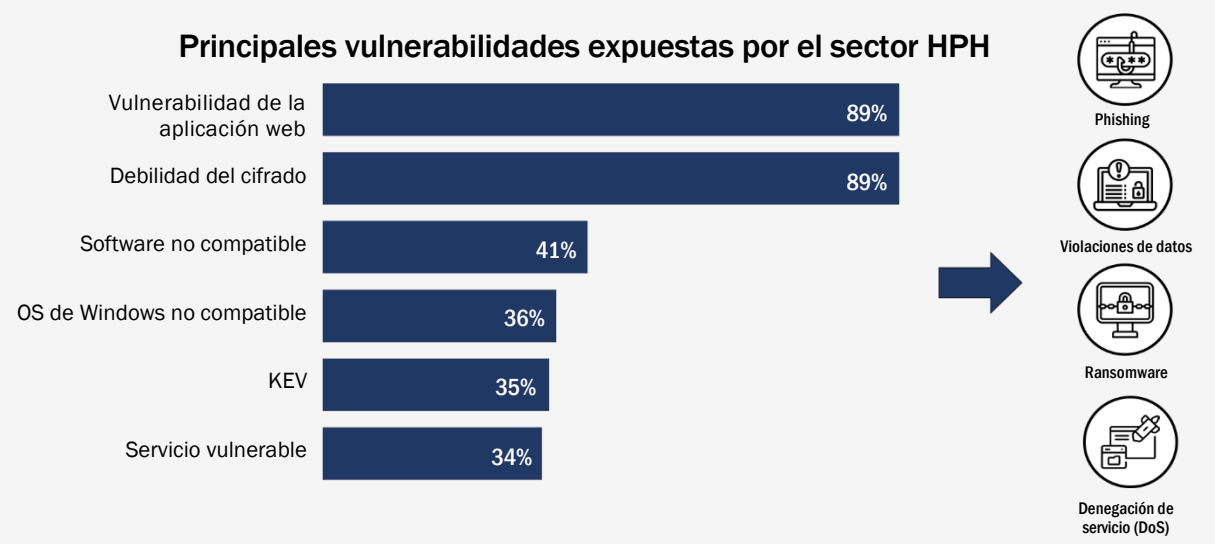

Figura 1: Principales vulnerabilidades y amenazas para el sector HPH

Como se indica en el ***Resumen de riesgos cibernéticos: calendario del sector de la atención médica y la salud pública (HPH) para el año 2022***[1] y la figura 1, la CISA identificó vulnerabilidades comunes y configuraciones inseguras en todo el sector de la HPH, como las siguientes:

- Vulnerabilidad de la aplicación web
- Debilidad del cifrado
- Software no compatible
- Sistema operativo (OS, por sus siglas en inglés) de Windows no compatible
- Vulnerabilidades explotadas conocidas (KEV, por sus siglas en inglés)
- Servicios vulnerables.[2]

La exposición de estas vulnerabilidades puede generar actividades cibernéticas perjudiciales, como ransomware, violaciones de datos o denegación de servicio. Cada uno de estos puede comprometer la disponibilidad, confidencialidad e integridad de los sistemas, funciones y datos críticos de HPH.

Esta guía de mitigación de vulnerabilidades mapea los Objetivos de desempeño de ciberseguridad intersectoriales (CPG, por sus siglas en inglés) de la CISA con la publicación conjunta del Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) y el Consejo de Coordinación del Sector Sanitario (HSCC, por sus siglas en inglés): 405(d) Prácticas de ciberseguridad de la industria sanitaria (HICP): gestión de amenazas y protección de los pacientes, que se detalla en la guía de la Tabla de correlación de HICP de CPG. Esta guía de mitigación evalúa las vulnerabilidades más comunes expuestas en el sector de la HPH y proporciona recomendaciones personalizadas y prácticas recomendadas para organizaciones de HPH de todos los tamaños. Además de los CPG, las HICPy la Guía de implementación del marco de ciberseguridad del sector de la HPH, la CISA recomienda que los fabricantes de productos de tecnología de HPH tomen medidas en línea con los Principios y enfoques de la CISA para la Seguridad desde el diseño y de manera predeterminada con el fin de reducir la carga de la ciberseguridad en sus clientes.

[1] El *Resumen de riesgos cibernéticos: calendario del sector de la atención médica y la salud pública (HPH) para el año 2022* es un informe TLP:GREEN; los destinatarios autorizados pueden comunicarse con su asesor regional de ciberseguridad o con csd_vm_insights_intake@cisa.dhs.gov para obtener acceso.

[2] Consulte la tabla 3 de la sección *Estrategia de mitigación 1: gestión de activos y seguridad* a continuación para obtener más información sobre los servicios vulnerables.

Nota de datos

El Resumen de riesgos cibernéticos de la HPH y esta Guía de mitigación evalúan y analizan datos de vulnerabilidad de activos accesibles a Internet de entidades del sector de la HPH inscritas en los servicios de escaneo de vulnerabilidades (VS, por sus siglas en inglés) y escaneo de aplicaciones web (WAS, por sus siglas en inglés) de higiene cibernética (CyHy, por sus siglas en inglés) de la CISA. Para contextualizar las tendencias de vulnerabilidad y ayudar a las entidades de HPH a comprender mejor las amenazas y los riesgos para su sector, esta guía incorpora el catálogo de KEV de la CISA, información de código abierto, fuentes de inteligencia de amenazas comerciales y el MITRE ATT&CK® (Tácticas, técnicas y conocimientos comunes de los adversarios).

Además, esta guía proporciona orientación sobre mitigación recomendada con medidas de mitigación de referencia asignadas a los CPG de la CISA. Utilizando fuentes similares, esta guía proporciona orientación y apoyo adicionales a las entidades de HPH al aprovechar y ampliar los datos presentados en el Resumen de riesgos cibernéticos para el sector de la HPH.[1] La tabla 1 muestra cada una de las fuentes y los marcos utilizados en este documento.

Tabla 1: Fuentes y marcos.[3]

Fuente	Dueño	Descripción
Escaneo de vulnerabilidades (VS) de higiene cibernética (CyHy)	CISA	VS de CyHy evalúa la presencia en la red externa mediante la ejecución de escaneos continuos sin credenciales de IPv4 estáticos públicos conectados a Internet en busca de servicios accesibles y vulnerabilidades mediante NMAP y Tenable Nessus.
Escaneo de aplicaciones web (WAS)	CISA	WAS es un "escaneo de Internet como servicio" que evalúa la "salud" de las aplicaciones web de acceso público mediante la búsqueda de vulnerabilidades conocidas y configuraciones débiles.
Objetivos de desempeño intersectoriales en materia de ciberseguridad (CPG) Versión 1.0.1	CISA	Los CPG son un subconjunto priorizado de prácticas de ciberseguridad de IT y OT que los propietarios y operadores de infraestructura crítica pueden implementar para reducir de forma significativa la probabilidad y el impacto de los riesgos conocidos y las técnicas de los adversarios.
Prácticas de ciberseguridad en la industria sanitaria (HICP)	HHS/HSCC	La publicación de HICP proporciona un punto de partida con diez prácticas de mitigación para implementar prácticas básicas de ciberseguridad en las organizaciones de atención médica.
Tabla de correlación de HICP de CPG	HHS/HSCC	Mapeo diseñado para ser utilizado como una vía para conectar los CPG de la CISA con la publicación de HICP 405(d) del HHS.
Marco MITRE ATT&CK Versión 13.0	MITRE	El marco MITRE ATT&CK es una guía para clasificar y describir ciberataques e intrusiones.
Catálogo de vulnerabilidades explotadas conocidas (KEV)	CISA	El catálogo de KEV es un conjunto priorizado de vulnerabilidades que han sido explotadas activamente.

[3] Algunas descripciones se toman directamente de los sitios fuente.

Estrategia de mitigación 1: gestión de activos y seguridad

Debido al alto valor de la información médica protegida (PHI, por sus siglas en inglés) y la importancia crítica de los servicios centrados en el paciente, los agentes de amenazas buscan continuamente nuevas formas de explotar las vulnerabilidades dentro del sector de la HPH. Las organizaciones que no han implementado o mantenido una política de gestión de activos corren el riesgo de exponer vulnerabilidades o servicios que podrían ser explotados por agentes de amenazas para obtener acceso no autorizado, robar datos confidenciales, interrumpir servicios críticos o implementar ransomware, causando un daño significativo a los pacientes y a la reputación de la organización.

Esta sección aborda diferentes conceptos de gestión y seguridad de activos, incluidos el inventario, la adquisición y el desmantelamiento de activos y la segmentación de la red, en relación con los activos de hardware, software y datos.

Área de enfoque 1: inventario de activos

Como estrategia de mitigación inicial y prioritaria, la CISA recomienda implementar y mantener un inventario de activos para su entorno. Saber qué activos hay en la red de su organización es fundamental para la ciberseguridad: “no se puede proteger lo que no se puede ver”. Los profesionales de ciberseguridad dentro del sector de la HPH deben identificar y comprender todas las relaciones o interdependencias, la funcionalidad de cada activo, lo que expone y qué software se está ejecutando para asegurarse de que cada organización proteja la PHI electrónica (ePHI) y permita el cumplimiento de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA, por sus siglas en inglés). Las organizaciones pueden completar inventarios de activos utilizando escaneos activos, procesos pasivos o una combinación de ambas técnicas. La recopilación de los atributos de inventario de activos enumerados en la figura 2 aclarará la red para que pueda administrar el inventario.

Vulnerabilidades y amenazas abordadas

- KEV
- Servicios vulnerables
- Software y OS obsoletos y sin soporte
- Ataques de ransomware
- Pérdida o robo de equipo o datos
- Ataques contra dispositivos médicos conectados a la red

Técnicas MITRE ATT&CK asociadas

- T1021 Servicios remotos
- T1046 Descubrimiento de servicios de red
- T1133 Servicios remotos externos
- T1190 Explotación de aplicaciones públicas
- T1199 Relación de confianza
- T1210 Explotación del servicios remotos
- T1219 Software de acceso remoto
- T1482 Descubrimiento de confianza del dominio
- T1563 Secuestro de sesión de servicio remoto
- T1557 Ataque de "adversario en el medio"
- T1571 Puerto no estándar
- T1610 Contenedor de implementación

CPG de la CISA y HICP del HHS relevantes

- Inventario de activos: CPG 1.A | HICP 5.M.A
- Segmentación de red: CPG 2.F | HICP 6.M.A
- Capacitación en ciberseguridad de OT: CPG 2.J | HICP 10.S.C
- Datos confidenciales seguros: CPG 2.L | HICP 1.M.A
- Proceso de aprobación de hardware y software: CPG 2.Q | HICP 2.L.D
- Prohibir la conexión de dispositivos no autorizados: CPG 2.V | HICP 2.S.A
- Sin servicios explotables en Internet: CPG 2.W | HICP 3.S.A
- Limitar las conexiones OT a la Internet pública: CPG 2.X | HICP 6.S.A

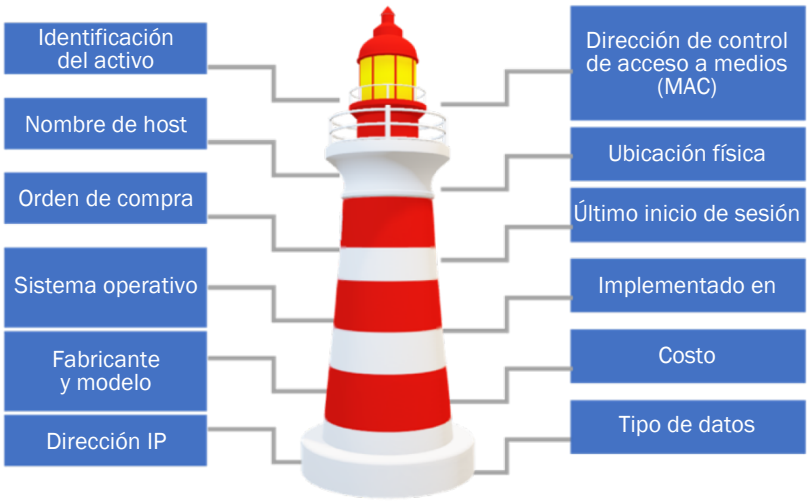

Figura 2: Atributos del inventario de activos

- Las herramientas de descubrimiento activo, incluidas las herramientas de monitoreo de red con funcionalidad de descubrimiento automatizado, escanean la red con una variedad de diferentes tipos de paquetes para identificar todos los activos conectados. El descubrimiento activo de activos suele ser más confiable que el pasivo; sin embargo, puede provocar congestión en la red o interrumpir dispositivos sensibles. Las técnicas activas de descubrimiento de activos también podrían afectar de forma negativa a los dispositivos médicos más antiguos debido a su memoria y unidad central de procesamiento (CPU, por sus siglas en inglés) limitadas.
- Las técnicas pasivas de descubrimiento incluyen la revisión de registros de conmutadores, enrutadores, directorios activos y otros lugares para identificar activos de red. Aunque estas técnicas se consideran menos perjudiciales para la red, tienden a pasar por alto activos que no han generado ninguna actividad durante el período de revisión.
- El descubrimiento híbrido utiliza técnicas activas y pasivas, según corresponda, en toda la red. El descubrimiento híbrido depende de una sólida comprensión de la estructura de la red organizativa para conformar el diseño y la implementación.

La CISA recomienda encargar a personal designado dentro de la organización la tarea de mantener el inventario actualizando mediante el rastreo, la inclusión y la eliminación de activos, sobre todo durante las etapas de adquisición o desmantelamiento. La CISA anima a las entidades de HPH a codificar la adquisición y el desmantelamiento de activos y tecnología en un procedimiento operativo estándar (SOP, por sus siglas en inglés), asignando roles y responsabilidades para cada función.

La tecnología obsoleta o los activos de IT que ya no se utilizan deben almacenarse de forma segura (p. ej., casilleros, cajas, salas) o retirarse de servicio de acuerdo con las políticas y los procedimientos de la organización. Si bien el desmantelamiento de activos puede parecer una tarea libre de estrés, la CISA anima a las organizaciones a trabajar con proveedores externos especializados en la destrucción o borrado seguro.[4] Asegúrese de obtener un recibo de destrucción y eliminación del proveedor para evitar el abuso o mal uso de los datos de los activos desmantelados.

[4] Ilascu, Ionut. "Hackers Can Breach Networks Using Data on Resold Corporate Routers." BleepingComputer. 23 de abril de 2023. https://www.bleepingcomputer.com/news/security/hackers-can-breach-networks-using-data-on-resold-corporate-routers/.

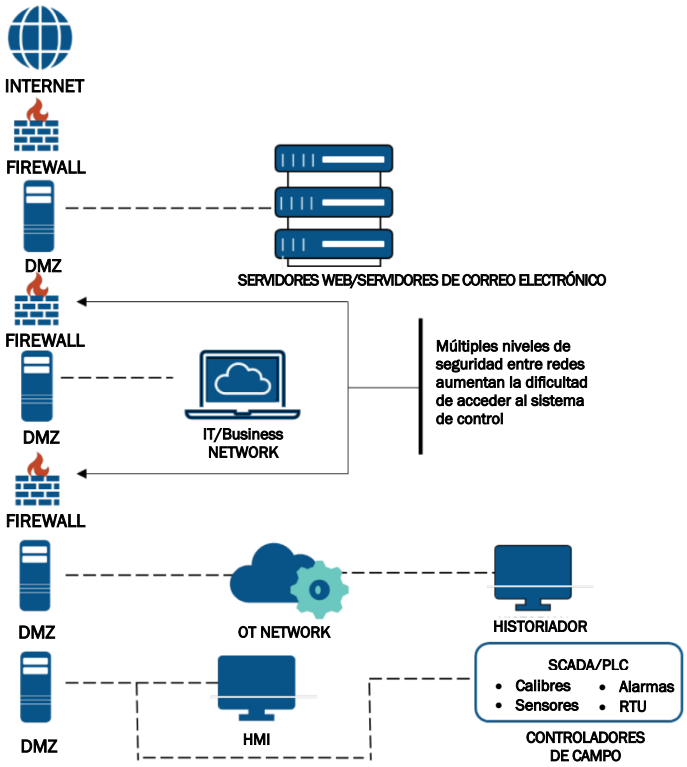

Figura 3: Segmentación de red

Área de enfoque 2: cómo proteger los activos

Al crear el inventario de activos, la CISA recomienda implementar la segmentación de red para aislar los dispositivos de IT y OT en diferentes segmentos.[5] La segmentación de red divide una red en partes más pequeñas, lo que permite el control sobre la comunicación de red entre segmentos. Un componente importante de la seguridad de la red es controlar qué activos pueden acceder a redes OT, qué activos pueden acceder a Internet desde una red interna y qué activos deben almacenarse en su propio compartimento.

Como se ve en la figura 3, las zonas desmilitarizadas (DMZ, por sus siglas en inglés) y los firewalls protegen la red contra el acceso no autorizado, con firewalls capaces de bloquear el tráfico de direcciones de red, aplicaciones o puertos mientras permiten el paso de los datos necesarios. Se deben utilizar políticas y controles para supervisar y regular el acceso al sistema y el movimiento del tráfico entre zonas.

En caso de una violación o vulneración, los segmentos de red adecuadamente protegidos pueden evitar que los agentes de amenazas se muevan lateralmente a través de su entorno. Un inventario de activos bien mantenido ayuda a detallar cómo los administradores de red dividen los recursos en segmentos según un conjunto de consideraciones, incluido lo crítico que sea el activo para las funciones comerciales, la sensibilidad de los datos que atraviesan el activo y los requisitos de acceso a Internet al activo. La tabla 2 muestra los controles de segmentación de la red.

[5] Instituto Nacional de Estándares y Tecnología (NIST). "Special Publication 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security." NIST. Mayo de 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Tabla 2: Controles de segmentación de la red

	Control de la segmentación de red	Descripción
☑	**Establecer y mantener una arquitectura de red**	Proporciona una vista detallada de los activos y la arquitectura de la red.
☑	**Configurar firewalls y listas de control de acceso (ACL)**	Aprueba o rechaza las comunicaciones entre segmentos según las reglas del administrador de red.
☑	**Recopilar y analizar registros de tráfico**	Determinar la estrategia de monitoreo dependiendo de los recursos disponibles para inspeccionar la comunicación entre segmentos.

Si bien los avances tecnológicos en dispositivos médicos reducen la carga laboral y la exposición a errores humanos, los dispositivos conectados a la red introducen nuevas vulnerabilidades de ciberseguridad que pueden traer mayores riesgos y afectar de forma negativa a la atención al paciente. Es posible que los dispositivos de IT tradicionales, como conmutadores, enrutadores y servidores, no hayan sido diseñados teniendo en cuenta la seguridad; sin embargo, dichos dispositivos pueden integrarse y administrarse mediante la mayoría de las herramientas de seguridad, si se configuran correctamente.

Las tecnologías utilizadas en entornos de atención médica a menudo comparten los mismos principios de diseño y podrían exponer servicios vulnerables que los agentes de amenazas podrían aprovechar en cualquier punto de la cadena de ataque cibernético. En noviembre de 2022, la Oficina Federal de Investigaciones (FBI, por sus siglas en inglés), la CISA y el Departamento de Salud y Servicios Humanos (HHS, por sus siglas en inglés) publicaron un aviso de ciberseguridad (CSA, por sus siglas en inglés) que indica que el grupo de ransomware Hive obtiene acceso inicial a las redes de las víctimas mediante el Protocolo de escritorio remoto (RDP, por sus siglas en inglés), redes privadas virtuales (VPN, por sus siglas en inglés) y otros protocolos de conexión de red remota.[6] La tabla 3 enumera los servicios vulnerables y explotables y su puerto común asociado.

Tabla 3: Servicios vulnerables y explotables

Categoría	Servicios (puertos comunes)
Acceso remoto	RDP (3389), Telnet (23)
Transferir archivos/compartir archivos	FTP (20, 21), SMB (445)
Comunicaciones entre procesos	RPC (135), NetBIOS (137, 138), SNMP (161, 162)
Autenticación y autorización	Kerberos (88, 464), LDAP (389)
Base de datos	SQL (1433)

[6] Agencia de Ciberseguridad y Seguridad de la Infraestructura. "#StopRansomware: Hive Ransomware". Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency) 17 de noviembre de 2022. https://www.cisa.gov/sites/default/files/publications/aa22-321a_joint_csa_stopransomware_hive.pdf

La CISA recomienda que las entidades de HPH implementen las medidas de mitigación enumeradas en la tabla 4 en toda su infraestructura para limitar la exposición.

Tabla 4: Medidas de mitigación de la seguridad de los activos

	Categoría de mitigación	Medida de mitigación recomendada
☑	**Exposición de puertos y servicios**	• Minimizar la exposición de la red únicamente a aquellos servicios que requieren las necesidades de la organización. • Deshabilitar los puertos no utilizados o innecesarios en los conmutadores, mediante la función de seguridad del puerto del conmutador. • Proteger la exposición de servicios vulnerables según las necesidades comerciales al exigir acceso con autenticación multifactor (MFA, por sus siglas en inglés) resistente al phishing. • Mantener versiones actualizadas de los servicios expuestos y eliminar versiones obsoletas y sin soporte.
☑	**Monitoreo de redes y seguridad**	• Implementar la segmentación de red para separar y restringir las comunicaciones entre los puntos finales expuestos públicamente y la red interna. • Asegurarse de que los sistemas de detección de intrusiones (IDS, por sus siglas en inglés) basados en firmas tengan sus conjuntos de firmas actualizados de forma periódica.
☑	**Seguridad de la base de datos**	• Revocar la función “ejecutar” en funciones generosas del servidor de lenguaje de consulta estructurado (SQL, por sus siglas en inglés). • Asegurarse de que las declaraciones no validadas no estén incluidas dentro de sus declaraciones “permitidas”. • Definir el código SQL con declaraciones preparadas para diferenciar entre el código y la entrada del usuario. • Asegurarse de que se completen los acuerdos de notificación actualizados con proveedores externos.

Recursos

- Póster de prescripción 405(d): gestión de activos
- Publicación especial 1800-5B del NIST: Gestión de activos de IT
- Publicación especial del NIST 800-82 rev. 2: Guía de seguridad de los sistemas de control industrial (SCI)
- Video sobre los conceptos ICS de SANS: Cómo crear una red OT segura
- Publicación especial del NIST 800-41 rev. 1: Directrices sobre firewalls y políticas de firewalls
- HHS Guía de implementación del marco de ciberseguridad del sector de la HPH
- CISA Directiva operativa vinculante 23-01: Mejora de la visibilidad de activos y detección de vulnerabilidades en redes federales

Estrategia de mitigación n.º 2: gestión de identidad y seguridad de dispositivos

A medida que el sector de la HPH continúa transfiriendo más de sus activos y sistemas en línea, la CISA recomienda que las entidades aseguren sus dispositivos y cuentas digitales y administren su acceso en línea para proteger los datos confidenciales y la PHI contra riesgos.

Varias áreas clave analizadas en esta sección incluyen seguridad del correo electrónico y prevención de phishing, administración y monitoreo de acceso, políticas de contraseñas y prácticas de protección de datos.

Área de enfoque 1: seguridad del correo electrónico y prevención de phishing

Ante la amenaza constante de correos electrónicos de phishing y ataques de vulneración de correo electrónico empresarial (BEC, por sus siglas en inglés), es esencial que las organizaciones configuren y protejan adecuadamente sus sistemas de correo electrónico. Además, para seguir cumpliendo con la normativa, las organizaciones deben aplicar las medidas de seguridad de correo electrónico adecuadas para cumplir con los requisitos de la regla de seguridad de la HIPAA, que protege la ePHI.

Las organizaciones deben asegurarse de que haya instalado software moderno contra programas malignos y de que las firmas se actualizan automáticamente cuando sea posible. Para obtener orientación adicional, consulte la Guía para mejorar la seguridad web y del correo electrónico de la CISA.

Para optimizar la seguridad y la protección del correo electrónico, la CISA recomienda implementar todos los controles de seguridad del correo electrónico indicados en la tabla 5. Estos controles de protección también son recomendados por los servicios de correo electrónico de software como servicio (SaaS, por sus siglas en inglés), como Microsoft O365 y Google Workspace. El blog de Seguridad de correo electrónico de Office 365de HIPPA Journal y el repositorio del centro de ayuda Ayude a prevenir la suplantación de identidad, el phishing y el spam de Google Workspace ofrecen orientación detallada sobre protección de correo electrónico.

Vulnerabilidades y amenazas abordadas

- Vulnerabilidad de la aplicación web
- Intentos de phishing
- Ataques de ransomware
- Ingeniería social
- Violaciones de datos

Técnicas MITRE ATT&CK asociadas

- T1098 Manipulación de cuentas
- T1078 Cuentas válidas
- T1566 Phishing
- T1110 Fuerza bruta
- T1557 Ataque de “adversario en el medio”
- T1565 Manipulación de datos
- T1003 Volcado de credenciales de OS

CPG de la CISA y HICP del HHS relevantes

- Cambiar contraseñas predeterminadas: CPG 2.A | HICP 9.M.B
- Seguridad mínima de la contraseña: CPG 2.B | HICP 3.M.C
- Credenciales únicas: CPG 2.C | HICP 3.M.C
- Revocación de credenciales para empleados salientes: CPG 2.D | HICP 3.S.A
- Separación de cuentas de usuario y privilegiadas: CPG 2.E | HICP 2.S.A
- Detección de intentos de inicio de sesión fallidos (automatizados): CPG 2.G | HICP 2.M.B
- Autenticación multifactor (MFA) resistente al phishing: CPG 2.H | HICP 2.M.A
- Capacitación básica en ciberseguridad: CPG 2.I | HICP 10.S.C
- Cifrado fuerte y ágil: CPG 2.K | HICP 2.S.A y 1.M.B
- Datos confidenciales seguros: CPG 2.L | HICP 1.M.A
- Seguridad del correo electrónico: CPG 2.M | HICP 1.M.A
- Recopilación de registros: CPG 2.T | HICP 2.L.B
- Almacenamiento seguro de registros: CPG 2.U | HICP 6.L.A

Tabla 5: Controles de protección del correo electrónico

	Control de correo electrónico	Descripción
☑	**Habilitar StartTLS**	Comando utilizado para actualizar una conexión no cifrada existente a una cifrada.
☑	**Implementar el marco de políticas de remitente (SPF) y el correo identificado DomainKeys (DKIM)**	Permite que un dominio de envío coloque una "marca de agua" en sus correos electrónicos, lo que hace que los correos electrónicos no autorizados sean fáciles de detectar.
☑	**Establecer la autenticación de mensajes basada en dominios, informes y conformidad (DMARC) en "rechazar"**	Garantiza que los mensajes no autenticados sean rechazados en el servidor de correo, incluso antes de la entrega.

Las organizaciones deben establecer y mantener un programa de capacitación en ciberseguridad para su fuerza laboral que cubra conceptos básicos de ciberseguridad, como concientización sobre phishing, riesgos del correo electrónico comercial, seguridad operativa básica y seguridad de contraseñas. Como mínimo, la capacitación debe realizarse anualmente y los nuevos empleados deben recibir capacitación inicial en ciberseguridad dentro de los primeros 10 días posteriores a su incorporación.

Los empleados deben tener especial cuidado al enviar y recibir correos electrónicos que contengan PII o PHI, y deben verificar dos veces que la dirección de correo electrónico del destinatario previsto sea correcta.

La tabla 6 muestra lo que los empleados deben reconocer como ejemplos de técnicas e indicadores de phishing.

Tabla 6: Ejemplos de técnicas de phishing e indicadores

	Indicador	Descripción
	**Compruebe si hay hipervínculos incrustados o falsificados**	Valide que la URL del enlace coincida con el texto del propio enlace. Para hacerlo, pase el cursor sobre el enlace para ver la URL del sitio web al que desea acceder. Tenga siempre cuidado al hacer clic en un enlace externo, ya que no todos los enlaces externos le dirigirán a un sitio web de confianza.
	**Busque direcciones de envío sospechosas**	Verifique los correos electrónicos recibidos para ver si las direcciones de envío contienen información falsificada o errores ortográficos. Puede comprobarlo colocando el cursor sobre el nombre del remitente. Las direcciones legítimas deben coincidir con lo que figura en el campo "De:".
	**Tenga cuidado con los mensajes "urgentes"**	Si el mensaje de correo electrónico requiere una acción inmediata, especialmente si incluye una solicitud para acceder a su correo electrónico o a cualquier otra cuenta, no abra el correo electrónico ni realice ninguna acción sin verificar que sea legítimo.
	**Tenga cuidado con los mensajes que parecen "demasiado buenos para ser verdad"**	Si recibe un mensaje inesperado sobre ganar dinero o tarjetas de regalo, no abra el correo electrónico ni realice ninguna acción sin verificar que sea legítimo.
	**Tenga cuidado con los errores ortográficos, gramaticales o de diseño**	Revise los correos electrónicos recibidos para detectar errores ortográficos, gramaticales o de diseño. Es inusual ver errores como estos en un correo electrónico legítimo.

Para obtener información adicional y orientación sobre phishing, consulte la Infografía sobre phishing de la CISA.

Área de enfoque 2: gestión de acceso

Así como el personal puede usar una placa con su nombre para identificarse en el entorno de trabajo físico, las prácticas de gestión de acceso a la ciberseguridad son esenciales para garantizar que todos los usuarios estén correctamente identificados y autenticados en el espacio digital. Para la gestión básica del acceso, las organizaciones deben implementar lo siguiente:

- **Implemente la MFA, preferiblemente resistente al phishing.** La MFA es un enfoque en capas para proteger cuentas y dispositivos en línea. Requiere una combinación de dos o más autenticadores para verificar la identidad de un usuario antes de que el servicio le otorgue acceso, con el factor adicional de algo que usted tiene, algo que usted es o algo que usted sabe. La MFA resistente al phishing completa el mismo proceso, pero quita a las "personas" de la operación para ayudar a frustrar las estafas de ingeniería social y los ataques de phishing dirigidos que podrían haber tenido éxito con una MFA tradicional. Las dos formas principales de MFA resistente a la suplantación de identidad son la autenticación FIDO/Web Authentication (WebAuthn) y la autenticación basada en infraestructura de clave pública (PKI, por sus siglas en inglés). Priorice el uso de MFA resistente a la suplantación de identidad en las cuentas con mayor riesgo, como las cuentas administrativas privilegiadas de activos clave. Para obtener información adicional sobre la MFA resistente al phishing, consulte la Guía de implementación de MFA resistente al phishing de la CISA.
- **Mantenga cuentas únicas y separadas para cada usuario de la organización.** Los usuarios no deben compartir contraseñas. Cada usuario debe crear una contraseña de cuenta que sea diferente a la de su cuenta personal. Evite el uso de cuentas compartidas o genéricas, siempre que sea posible.
- **Finalice el acceso tan pronto como un usuario abandone la organización.** Si un usuario cambia de función dentro de la organización, es importante finalizar el acceso a su puesto anterior antes de emitir nuevas credenciales.
- **Restrinja el uso de cuentas con privilegios elevados.** Las organizaciones deben asignar a los administradores del sistema dos cuentas: una con privilegios elevados y otra para funciones rutinarias de la oficina (como navegación web o correo electrónico comercial). Asegúrese de realizar una revisión periódica de todos los accesos y cuentas privilegiados.

Área de enfoque 3: políticas de contraseñas

La creación de credenciales y contraseñas sólidas y únicas es vital para la seguridad de las cuentas y los dispositivos. Los agentes de amenazas han aprovechado credenciales débiles y compartidas para obtener acceso inicial a la red y llevar a cabo diversos ataques. Las organizaciones deben procurar implementar lo siguiente:

- **Cambiar todas las contraseñas predeterminadas.** Antes de colocar cualquier hardware, software o firmware en la red, cambie de inmediato las contraseñas predeterminadas proporcionadas por el proveedor.
- **La longitud de la contraseña debe ser de un mínimo de 15 caracteres.** Para que los agentes de amenazas tengan más dificultades para adivinar o descifrar las contraseñas, las organizaciones deberían exigir una longitud mínima de contraseña de 15 o más caracteres cuando sea técnicamente posible. Para obtener más orientación sobre cómo crear contraseñas seguras, consulte la guía Creación de una contraseña de la CISA.

Área de enfoque 4: protección de datos y prevención de pérdidas

Con los requisitos de la HIPAA para proteger la información de salud del paciente, cualquier violación de datos o seguridad que resulte en la vulneración, la pérdida o la divulgación de datos confidenciales, incluyendo PII y PHI, puede tener impactos importantes para su organización. Para evitar interrupciones en la seguridad del paciente y la prestación de atención, es esencial que todas las entidades de HPH implementen buenas políticas de protección de datos que garanticen la seguridad de la información confidencial. Para la protección de datos y la prevención de pérdidas, las organizaciones deben implementar lo siguiente:

- **Asegúrese de almacenar y gestionar el acceso de forma adecuada a toda la información confidencial, incluidas las credenciales.** Los datos confidenciales, como las credenciales, no deben ordenarse en texto sin formato y solo deben acceder a ellos usuarios autenticados y autorizados. Considere soluciones de administración de cuentas privilegiadas, como un administrador de credenciales y contraseñas, para garantizar que todas las credenciales se almacenen de forma segura.

- **Mantenga protocolos y algoritmos de cifrado fuertes y actualizados.** Las organizaciones deben asegurarse de que se utilicen protocolos de cifrado configurados de forma correcta y actualizados, como la seguridad de la capa de transporte (TLS, por sus siglas en inglés), para proteger los datos, tanto en reposo como en tránsito. Las organizaciones también deberían planificar la identificación de cualquier uso de algoritmos de cifrado débiles u obsoletos y actualizarlos con algoritmos lo bastante fuertes.

La tabla 7 muestra prácticas recomendadas de cifrado adicionales.

Tabla 7: Prácticas recomendadas de cifrado

	Práctica de cifrado	Descripción
☑	**Algoritmo clave**	Dependiendo del caso de uso y la sensibilidad de los datos, se debe seleccionar un algoritmo simétrico, como el Estándar de cifrado avanzado (AES, por sus siglas en inglés), o un algoritmo asimétrico, como RSA o el Algoritmo de firma digital de curva elíptica (ECDSA, por sus siglas en inglés). Los algoritmos simétricos utilizan la misma clave para cifrar y descifrar los datos, mientras que los algoritmos de cifrado asimétrico utilizan dos claves diferentes.
☑	**Tamaño de la clave**	El NIST recomienda 256 bits para claves AES y 2048 o 4096 bits para claves RSA. En cuanto al tamaño de la clave, cuanto mayor sea la clave, más segura será y durante más tiempo brindará protección. Sin embargo, dado que las claves más grandes también pueden generar problemas de rendimiento, la elección del tamaño debe hacerse con cuidado según el caso de uso.
☑	**Agilidad criptográfica**	Los algoritmos de cifrado tienden a debilitarse con el tiempo. Es importante que su organización esté preparada para cambiar los algoritmos o el tamaño de la clave. Sea consciente de la amenaza de la computación cuántica y esté preparado para cambiar a algoritmos poscuánticos si o cuando sea necesario.
☑	**Rotación de claves**	Utilizar la misma clave durante un largo período de tiempo aumenta las posibilidades de que la clave se vea comprometida. Es una buena práctica actualizar (o rotar) las claves de cifrado de forma periódica.
☑	**Retirar la clave**	Cuando una clave ya no es necesaria, se debe retirar. El retiro implica eliminar de forma permanente la clave para garantizar que no haya más riesgos y reducir la cantidad de claves activas que se administran.
☑	**Almacenamiento seguro de claves**	El NIST recomienda utilizar un módulo de seguridad de hardware (HSM, por sus siglas en inglés) para almacenar claves de cifrado, ya que proporcionan una fuerte protección física y lógica.
☑	**Control del acceso**	Las claves de cifrado no deberían estar disponibles para todos los usuarios en todo momento. Solo los usuarios autorizados y autenticados deben tener permitido acceder, administrar y utilizar las claves de cifrado.

Área de enfoque 5: registros de dispositivos y soluciones de monitoreo

Para proteger los dispositivos y evitar que los agentes de amenazas se muevan lateralmente a través de la red de su organización, considere implementar una solución de detección y respuesta de puntos finales (EDR, por sus siglas en inglés). Una EDR es una solución de seguridad de puntos finales que monitorea continuamente los dispositivos de los usuarios finales para detectar comportamientos sospechosos, brindar información contextual y responder con sugerencias de solución.

Al seleccionar una solución de EDR, asegúrese de que incorpore análisis de comportamiento de usuarios y entidades (UEBA, por sus siglas en inglés) y supervise de cerca los registros de acceso para detectar desviaciones fuera del comportamiento normal. Los intentos de inicio de sesión fallidos o automatizados deben registrarse. Almacene los registros en un sistema central, como una herramienta de manejo de eventos e información de seguridad (SIEM) o una base de datos central. Solo deben acceder y modificar los registros los usuarios autorizados y autenticados y deben almacenarse de forma segura durante el tiempo recomendado por las pautas regulatorias o de riesgo.

Recursos

- CISA Autenticación multifactor
- CISA Infografía sobre phishing
- NIST SP 800-63-3 Pautas de identidad digital
- H-ISAC Introducción y sistemas de protección de correo electrónico, ciberseguridad para la capacitación del médico
- H-ISAC Protección de datos y prevención de pérdidas, ciberseguridad para la capacitación del médico
- HHS Volumen técnico 1: Prácticas de ciberseguridad para pequeñas organizaciones de atención médica
- HHS Volumen técnico 2: Prácticas de ciberseguridad para organizaciones de atención médica medianas y grandes
- HHS Guía de implementación del marco de ciberseguridad del sector de la HPH

Estrategia de mitigación n.º 3: gestión de vulnerabilidades, parches y configuración

Área de enfoque 1: gestión de vulnerabilidades y parches

La gestión de vulnerabilidades es el proceso continuo de identificar, evaluar, notificar, gestionar y corregir las vulnerabilidades cibernéticas en el software y los sistemas. El proceso implica escanear de forma proactiva dispositivos y sistemas en busca de vulnerabilidades o fallas tecnológicas que los agentes de amenazas podrían explotar. La gestión de parches, que a menudo se utiliza indistintamente con la gestión de vulnerabilidades, es un componente vital de toda solución de gestión de vulnerabilidades. Implica aplicar actualizaciones a servidores, aplicaciones y software para abordar fallas de seguridad. La gestión de vulnerabilidades y parches son componentes clave en la planificación y determinación de la implementación adecuada de controles y la gestión de riesgos.

Como la gestión de vulnerabilidades es un proceso continuo y evolutivo, a menudo es un ciclo de varios pasos, como se muestra en la figura 4.

Vulnerabilidades y amenazas abordadas

- KEV
- Ataques de ransomware
- Violaciones de datos

Técnicas MITRE ATT&CK asociadas

- T1190 Explotación de aplicaciones públicas
- T1210 Explotación del servicios remotos
- T1212 Explotación para acceso a credenciales

CPG de la CISA y HICP del HHS relevantes

- Mitigación de vulnerabilidades conocidas: CPG 1.E | HICP 7.M.D and 2.S.A
- Configuraciones de dispositivos de documentos: CPG 2.O | HICP 10.S.B
- Detección de amenazas y TTP relevantes : CPG 3.A | HICP 2.L.B

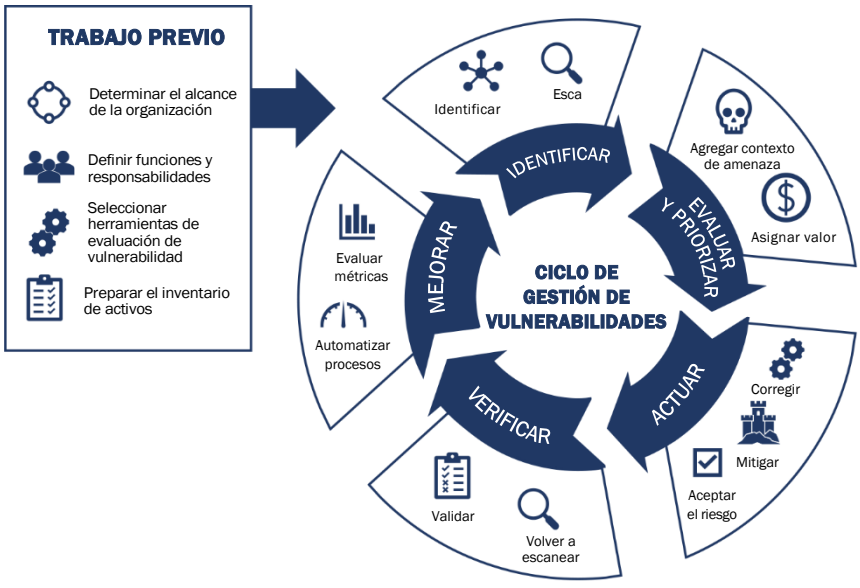

Figura 4: Ciclo de vida de la gestión de vulnerabilidades
(adaptado del Marco de orientación sobre gestión de vulnerabilidades de Gartner)

Paso 1. Identificar. El primer paso y el más importante en cualquier proceso de gestión de vulnerabilidades es identificar todas las vulnerabilidades que puedan existir en el entorno de la organización. Para ayudar a descubrir las vulnerabilidades, siga estos pasos:

- **Un Inventario de activos.** Un inventario de activos debe enumerar todos los activos empresariales de su organización, como dispositivos, sistemas operativos, software y servicios que se evaluarán para detectar vulnerabilidades.

- **Un escáner de vulnerabilidad.** Un escáner de vulnerabilidades realiza escaneos con credenciales y sin credenciales de sistemas accesibles a la red para identificar puertos abiertos y servicios que se ejecutan en esos sistemas escaneados y buscar vulnerabilidades conocidas cuando está configurado correctamente. La CISA ofrece escaneo de vulnerabilidades gratuito a través de Servicios de Higiene Cibernética (CyHy, por sus siglas en inglés) para activos conectados a Internet. Las entidades de HPH deben utilizar un escáner de vulnerabilidades configurado con complementos actualizados para realizar exploraciones continuas de los activos de la red interna.

Paso 2. Evaluar y priorizar. Una vez que se identifiquen las vulnerabilidades en su entorno, evalúelas y priorícelas para abordar adecuadamente los riesgos planteados de acuerdo con la estrategia de riesgos de su organización. Para ayudar con la priorización, es esencial lo siguiente:

- **Asigne los activos a funciones críticas para el negocio.** Para la corrección de vulnerabilidades, priorice los activos que son más críticos para las operaciones en curso o que, si resultan afectados, podrían impactar en la continuidad del negocio, la seguridad de la PII o PHI confidencial, la reputación o la posición financiera de su organización.
- **Utilice información de inteligencia sobre amenazas.** Para la corrección, priorice las vulnerabilidades que los agentes de amenazas explotan de forma activa. Para ayudar, aproveche el catálogo de KEV de la CISA y otras fuentes de inteligencia sobre amenazas.
- **Aproveche las metodologías de priorización, calificaciones y puntuaciones.** El Sistema de puntuación de vulnerabilidades comunes (CVSS, por sus siglas en inglés) evalúa la gravedad técnica de las vulnerabilidades. El Sistema de puntuación de predicción de exploits (EPSS) mide la probabilidad de explotación y puede ayudar a decidir qué vulnerabilidades priorizar. La metodología de categorización de vulnerabilidades específica de las partes interesadas (SSVC, por sus siglas en inglés) de la CISA aprovecha los árboles de decisiones para priorizar las vulnerabilidades relevantes en cuatro decisiones: Supervisar, Supervisar*, Asistir y Actuar en función del estado de explotación, del impacto técnico, de la prevalencia de la misión y de los impactos en la seguridad y el bienestar público.

Paso 3. Actuar. Una vez que se ha evaluado una vulnerabilidad y se la considera un riesgo, es necesario tratarla. A la hora de determinar estrategias de tratamiento específicas, lo mejor es que el equipo de seguridad de la organización, los propietarios y los administradores del sistema se reúnan y determinen el enfoque de solución adecuado. Hay tres acciones que las organizaciones pueden tomar ante una vulnerabilidad identificada:

- **Corrección.** La corrección implica reparar o aplicar un parche por completo a una vulnerabilidad para que los agentes de amenazas no puedan explotarla. Es la opción de tratamiento ideal que las organizaciones deben procurar alcanzar.
- **Medida de mitigación.** La medida de mitigación reduce la probabilidad o el impacto de una vulnerabilidad que está siendo explotada. Esto puede ser necesario cuando aún no hay disponible una solución o parche adecuado para una vulnerabilidad identificada. Lo ideal sería utilizar la medida de mitigación para ganar tiempo para que una organización pueda eventualmente corregir una vulnerabilidad.
- **Aceptación.** La aceptación implica no realizar ninguna acción para solucionar o minimizar la probabilidad o el impacto de una vulnerabilidad que está siendo explotada. Esto generalmente se justifica cuando una vulnerabilidad se considera de bajo riesgo o el costo o riesgo inherente a repararla es mucho mayor que el costo o el resultado en que incurriría una organización si la vulnerabilidad fuera explotada.

Para ayudar con la priorización y el tratamiento de vulnerabilidades, utilice la Guía de categorización de vulnerabilidades específicas de las partes interesadas (SSVC) y la Calculadora SSVC de la CISA.

Paso 4. Verificar. Una vez que se considera que la corrección se ha completado, es aconsejable ejecutar otro análisis de vulnerabilidad para garantizar que haya sido efectivamente corregida o mitigada.

Paso 5. Mejorar. Para mejorar y refinar el proceso de gestión de vulnerabilidades, continúe realizando evaluaciones de vulnerabilidades periódicas y evalúe los resultados para realizar los ajustes necesarios para mejorar la velocidad y la eficiencia de su programa.

Para aprovechar al máximo el programa de gestión de vulnerabilidades de su organización, se recomienda escanear todo el software, los dispositivos y los sistemas, al menos, una vez al mes. Las organizaciones deben evaluar de forma continua la exposición a las vulnerabilidades, mantener una documentación sólida de todos los análisis de vulnerabilidades e implementar parches producidos por la comunidad de proveedores.

Área de enfoque 2: gestión de la configuración y los cambios

Además de las soluciones establecidas de gestión de vulnerabilidades y parches, las entidades de HPH deberían implementar la gestión de configuración de seguridad (SecCM, por sus siglas en inglés) para identificar y abordar configuraciones erróneas en las configuraciones predeterminadas del sistema. Este proceso implica identificar, controlar, contabilizar y auditar los cambios realizados en las referencias preestablecidas, con el objetivo de ir más allá del diseño original de un sistema hacia una versión reforzada y operativamente sólida. Al igual que la gestión de vulnerabilidades, la gestión de configuración y cambios (CCM, por sus siglas en inglés) sigue varios pasos cíclicos:

Paso 1. Identificar los elementos de configuración. Al aprovechar el inventario de activos, este paso implica identificar los elementos de configuración (p. ej., hardware, software o firmware) dentro del entorno de la organización que requieren administración. Mantenga la documentación de los atributos básicos, como marca/modelo, número de serie, sistema operativo, ubicación y propietario.

Paso 2. Establecer referencias seguras. Como las configuraciones predeterminadas del proveedor rara vez son seguras y suelen ser el blanco de amenazas, es esencial que las entidades tengan referencias de configuración seguras preestablecidas. Los proveedores pueden ayudar al proporcionar configuraciones seguras de forma predeterminada, garantizando así que su producto sea seguro desde el primer momento. Las organizaciones pueden aprovechar los puntos de referencia de instituciones confiables, como el CIS o el NIST (ver Recursos a continuación), para desarrollar sus referencias, que deben incluir las tareas mínimas para lo siguiente:

- Deshabilitar servicios y puertos innecesarios.
- Instalar los últimos parches del sistema y de seguridad.

Cambiar el nombre de las cuentas del sistema predeterminadas.

- Cambiar las contraseñas y credenciales predeterminados.
- Configurar MFA cuando sea posible y apropiado.
- Habilitar configuraciones de seguridad, como firewalls internos y actualizaciones automáticas.

Paso 3. Implementar y auditar los cambios. Una vez que una organización identifica configuraciones y establece referencias, puede aplicar cambios a los sistemas. Considere utilizar herramientas automatizadas para aplicar las configuraciones cuando sea posible; la automatización reduce el riesgo de aplicar configuraciones erróneas y proporciona un registro de auditoría de todos los cambios para evitar acciones no autorizadas.

Paso 4. Evaluar y corregir. La gestión de la configuración es un proceso cíclico; es importante garantizar que los cambios se evalúen y solucionen continuamente. Las entidades deben consultar su estrategia de gestión de vulnerabilidades y ejecutar evaluaciones para verificar que los cambios esperados fueron exitosos o corregir si no lo fueron.

Recursos

- Guía de recursos suplementaria de la revisión de resiliencia cibernética de la CISA volumen 4 Gestión de vulnerabilidades
- Guía de recursos suplementaria de la revisión de resiliencia cibernética de la CISA volumen 3 Gestión de la configuración y el cambio
- NIST Guía para la planificación de la gestión de parches empresariales: mantenimiento preventivo para tecnología
- HHS Guía de implementación del marco de ciberseguridad del sector de la HPH
- H-ISAC Capacitación en video sobre gestión de vulnerabilidades y ciberseguridad para médicos
- Póster de prescripción 405d: gestión de vulnerabilidades

Hacia un futuro más seguro: seguridad desde el diseño

Dado que los sistemas conectados a Internet están conectados a sistemas y funciones de salud críticos, es fundamental que los fabricantes de productos tecnológicos utilizados por entidades de HPH empleen prácticas seguras desde el diseño. Con ese fin, la CISA fue coautora y publicó Cambiar el equilibrio del riesgo de la ciberseguridad: principios y enfoques para un software seguro desde el diseño, que insta a los fabricantes de tecnología a renovar sus programas de diseño y desarrollo para ofrecer productos que tengan seguridad incorporada y cuya configuración predeterminada sea segura.

Históricamente, los fabricantes y proveedores de tecnología han recurrido a la corrección puntual de las vulnerabilidades encontradas después de la implementación de los productos, y esto ha obligado a los clientes a aplicar parches por su cuenta. La CISA y sus socios buscan cambiar el equilibrio en el desarrollo de productos hacia (1) la seguridad desde el diseño, donde la seguridad de los clientes es un requisito comercial central, no solo una característica técnica, y (2) la seguridad predeterminada, para que la seguridad del producto esté lista para usar, sin necesidad de cambios de configuración y con funciones de seguridad disponibles sin costo adicional. Visite el sitio web Seguridad desde el diseño de la CISA para obtener orientación e información actualizadas.

La CISA recomienda que los fabricantes de productos de HPH tomen medidas para construir sus productos de manera segura desde el diseño, y que las entidades de HPH prioricen la importancia de comprar productos seguros desde el diseño. Para lograr esto, las organizaciones deberían hacer lo siguiente:

- **Desarrollar y establecer criterios de compra que enfaticen la importancia de prácticas de seguridad desde el diseño.** Los criterios de ciberseguridad deberían incorporarse en las posibles adquisiciones a través de solicitudes de información (RFI, por sus siglas en inglés) a los proveedores.
    - Para cumplir con los criterios de seguridad desde el diseño, la CISA recomienda que las entidades de HPH busquen fabricantes que sigan principios de seguridad desde el diseño. Los ejemplos incluyen fabricantes que publican artefactos de acuerdo con la guía de seguridad desde el diseño de la CISA, como publicar una hoja de ruta de seguridad desde el diseño y de memoria, proporcionar una lista de materiales de software (SBOM, por sus siglas en inglés), publicar una política de divulgación de vulnerabilidades y documentar los pasos tomados de acuerdo con el Marco de desarrollo de software seguro (SSDF, por sus siglas en inglés) de NIST y los CPG de la CISA.
    - Para configuraciones seguras de manera predeterminada, las entidades de HPH deben buscar productos que eliminen las contraseñas predeterminadas, proporcionen inicio de sesión único (SSO, por sus siglas en inglés) sin costo adicional, incluyan registros de auditoría de seguridad sin costo adicional e integren las configuraciones más seguras en el producto de manera predeterminada.
- **Establecer políticas y procedimientos que requieran que las adquisiciones de tecnología (incluidos los dispositivos médicos) se sometan a evaluaciones de seguridad.** La implementación de la evaluación de ciberseguridad brinda a su organización la oportunidad de comprender, evaluar y mitigar los riesgos cibernéticos antes de implementar la tecnología. Con la evaluación, las entidades de HPH deben insistir en recibir una Declaración de divulgación del fabricante (MDS, por sus siglas en inglés), que incluye respuestas a preguntas como las siguientes:
    - ¿Este dispositivo puede mostrar, transmitir o mantener datos privados (incluida PHI/PII electrónica)?
    - ¿El dispositivo médico puede crear un registro de auditoría?
    - ¿Es posible asignar a los usuarios diferentes niveles de privilegios dentro de una aplicación según sus "funciones" (p. ej., invitados, usuarios regulares, usuarios avanzados, administradores)?
- **Forjar relaciones de asociación estratégica con proveedores clave de IT.** Reforzar la importancia de las prácticas seguras desde el diseño tanto en los contratos formales o acuerdos con proveedores como en los aspectos informales. Las organizaciones deben esperar transparencia de sus proveedores de tecnología.
    - Al establecer contratos formales, las entidades de HPH deben exigir acuerdos de nivel de servicio (SLA, por sus siglas en inglés) y contratos con vendedores o proveedores de servicios que optan por ofertas más seguras, como MFA resistente al phishing, el principio de mínimo privilegio para cuentas administrativas, derechos de auditoría y la divulgación y notificación de vulnerabilidades de seguridad confirmadas dentro de un marco de tiempo conformado por el riesgo.
- **Colaborar con pares de la industria.** Cultivar relaciones de trabajo con socios de la industria para comprender los productos y servicios que mejor incorporan los principios de seguridad desde el diseño.
- **Al aprovechar los sistemas en la nube, asegurarse de comprender las responsabilidades de seguridad del proveedor.** Las organizaciones deben priorizar a los proveedores de nube que sean transparentes sobre su postura de seguridad. Consulte el Proyecto de Aplicaciones Empresariales Seguras en la Nube (SCuBA) de la CISA para obtener orientación sobre seguridad y configuración en la nube.

Guía de corrección de vulnerabilidades del sector de la HPH

Al implementar las estrategias de mitigación mencionadas en las secciones anteriores, la CISA anima a las entidades del sector de la HPH a rastrear y priorizar sus vulnerabilidades en función de su arquitectura de red interna y su postura de riesgo.

En la tabla 8 y la tabla 9 se muestran las pautas de corrección y los controles de compensación de las vulnerabilidades priorizadas identificadas en todo el sector, con base en el análisis de vulnerabilidades, la alta probabilidad de explotación, la máxima prevalencia dentro del sector y las categorizaciones de calificación de riesgo comercial.

Tabla 8: Vulnerabilidades priorizadas del sector de la HPH

CVE	Proveedor	Nombre de la vulnerabilidad
CVE-2021-44228	Apache	Vulnerabilidad de ejecución remota de código Log4j2 en Apache
CVE-2019-11043	PHP	Vulnerabilidad de desbordamiento de búfer en el administrador de procesos FastCGI (FPM) de PHP
CVE-2012-1823	PHP	Vulnerabilidad de parámetros de cadena de consulta PHP-CGI
CVE-2021-34473	Microsoft	Vulnerabilidad de ejecución de código remoto de Microsoft Exchange Server
CVE-2017-12617	Apache	Vulnerabilidad de ejecución remota de código Apache Tomcat

Tabla 9: Guía de mitigación y corrección de vulnerabilidades priorizadas

Corrección	Controles de compensación
CVE-2021-44228	
Actualizar a Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) y 2.3.2 (Java 2).	• Deshabilite la biblioteca Log4j. Deshabilitar el software mediante la biblioteca Log4j es una medida eficaz que favorece el tiempo de inactividad controlado frente a los problemas causados por agentes de amenazas. Sin embargo, esta opción podría causar impactos operativos y limitar la visibilidad de otros problemas. • Deshabilite las búsquedas de la interfaz de nombres y directorios de Java (JNDI, por sus siglas en inglés) o deshabilite las bases de código remotas. Esta opción, aunque efectiva, puede implicar trabajo del desarrollador y podría afectar la funcionalidad. • Desconecte las pilas afectadas. Las pilas de soluciones que no están conectadas a las redes de agencias plantean un riesgo de ataque considerablemente menor. Considere desconectar temporalmente la pila de las redes de la agencia. • Cree una red de área local virtual (VLAN, por sus siglas en inglés) de "red vulnerable" para aislar y segmentar la pila de soluciones del resto de la red empresarial. • Implemente un firewall de aplicaciones web (WAF, por sus siglas en inglés) configurado correctamente delante de la pila de soluciones. • Consulte la página web de Orientación sobre vulnerabilidades de Log4j de Apache de la CISA y el repositorio de GitHub para obtener futuras actualizaciones y orientación.
CVE-2019-11043	
Actualice a la versión 7.3.11 de PHP o posterior.	• Como Nginx está asociado con esta vulnerabilidad, debe configurarse para verificar los scripts y archivos existentes incluyendo el directorio `try_files` o usando una declaración if, como `if (-f $uri)`. Tenga en cuenta que esta medidas de mitigación solo funciona si Nginx y PHP-FRM comparten el mismo `docroot` en el mismo host. • Aplique parches y actualice PHP a su última versión con regularidad y deshabilite en consecuencia los complementos o componentes innecesarios u obsoletos.

Corrección	Controles de compensación
	• Habilite los controles de seguridad integrados de PHP y utilice la Hoja de referencia de configuración de PHP del Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP, por sus siglas en inglés). • Implemente controles de validación y saneamiento en todas las entradas o datos generados por el usuario. • Considere usar la aleatoriedad en la disposición del espacio de direcciones (ASLR, por sus siglas en inglés). Esta técnica aumenta la dificultad de realizar un ataque de desbordamiento de búfer. La ASLR asigna de forma aleatoria las direcciones de programas y funciones en la memoria de un sistema a diferentes regiones de datos, lo que dificulta que un agente de amenazas navegue a través de funciones sensibles en la memoria.
CVE-2012-1823	
Actualice a la versión 5.3.12 / 5.4.2 de PHP o posterior.	• Utilice una regla de `mod_rewrite` para indicarle al servidor web que no procese solicitudes con cadenas de consulta que comiencen con un "`-`" y que no contengan un "`=`". • Aplique parches y actualice PHP de forma periódica a su última versión y desactive los complementos o componentes innecesarios u obsoletos. • Habilite los controles de seguridad integrados de PHP y utilice la Hoja de referencia de configuración de PHP del Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP).
CVE-2021-34473	
Aplique las actualizaciones y parches de seguridad más recientes emitidos por el proveedor.	• Para verificar la versión actual de Microsoft Exchange que se ejecuta dentro de una organización, consulte la documentación de Microsoft relacionada con las compilaciones y versiones de Exchange Server. • Implemente una solución de monitoreo de integridad de archivos (FIM, por sus siglas en inglés) configurada correctamente para monitorear y prevenir la creación de archivos. Las soluciones de FIM monitorean de cerca tanto la configuración como el contenido de archivos confidenciales y activan alertas cuando detectan acceso, copias, descargas y modificaciones no autorizadas. • Implemente una solución EDR configurada correctamente para monitorear los registros de acceso y ayudar a detectar cualquier desviación del comportamiento normal. Asegúrese de que los registros se almacenen de forma segura y que solo usuarios autorizados y autenticados puedan acceder a ellos o modificarlos. • Asegúrese de que la MFA esté implementada para todos los accesos externos, como Outlook Web Access. • Deshabilite el acceso remoto a PowerShell para usuarios no administrativos de la organización.
CVE-2017-12617	
Actualice a la versión 9.0.1 o posterior de Apache Tomcat.	• Si es un nuevo usuario de Apache Tomcat, se recomienda suscribirse a la lista de correo de Apache Tomcat para recibir información sobre nuevas versiones y vulnerabilidades de seguridad. • El parámetro `readonly` `init-param` debe establecerse en verdadero para evitar que un agente de amenazas cargue archivos. • Considere bloquear las solicitudes `PUT` y `DELTE` en el servidor frontend (p. ej., en el WAF).

Conclusión

Esta guía apoya a las entidades de HPH con la formulación de recomendaciones basadas en TTP maliciosos pertinentes y datos de exposición a vulnerabilidades. Como se destaca en esta guía, las entidades del sector de la HPH deben estar atentas a sus prácticas de mitigación de vulnerabilidad para prevenir y minimizar el riesgo de amenazas cibernéticas. Una vez que una organización evalúa y considera que una vulnerabilidad es un riesgo, debe tratarla.

La CISA recomienda que las entidades de HPH implementen esta guía para reducir de forma significativa su riesgo en la ciberseguridad. También anima encarecidamente a las entidades de HPH a utilizar la información de inteligencia sobre amenazas mencionada en el informe Resumen de riesgos cibernéticos[1] para abordar y corregir con eficacia su exposición a vulnerabilidades y proteger a sus organizaciones de lo siguiente:

- Ataques potenciales de ransomware
- Violaciones de datos
- Pérdida o robo de equipo o datos
- Ataques contra dispositivos médicos conectados a la red

La CISA también recomienda que las entidades de HPH sigan las estrategias de mitigación y recomendaciones abordadas en esta guía para mejorar la postura de ciberseguridad organizativa.

Para ayudar aún más a sus organizaciones, la CISA anima a las entidades de HPH a registrarse para el análisis de vulnerabilidades gratuito de la CISA e invita a las entidades del sector de la HPH a buscar asesoramiento y asistencia adicionales de la CISA a través de vulnerability@cisa.dhs.gov.

Los comentarios sobre este producto son fundamentales para la mejora continua de la CISA. Si tiene comentarios específicos sobre su experiencia con este producto, envíe sus comentarios a la CISA completando la Encuesta de productos de la CISA.

Apéndice 1: Glosario de términos cibernéticos

Activo
Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar sus objetivos comerciales.

Compromiso del correo electrónico empresarial (BEC)
Una estafa sofisticada que tiene como objetivo organizaciones y personas mediante el uso de ingeniería social o intrusión informática para comprometer cuentas de correo electrónico legítimas y realizar transferencias de fondos no autorizadas u obtener información de identificación personal.

Riesgo de ciberseguridad
Un efecto de la incertidumbre sobre o dentro de la información y la tecnología. Los riesgos de ciberseguridad se relacionan con la pérdida de confidencialidad, integridad o disponibilidad de la información, los datos o los sistemas de información (o control) y reflejan las posibles repercusiones negativas en las operaciones de la organización (es decir, la misión, las funciones, la imagen o la reputación), los activos, las personas, otras organizaciones y la nación.

Tecnología de la Información (IT)
Cualquier equipo o sistema interconectado o subsistema de equipos que procesa, transmite, recibe o intercambia datos o información.

Autenticación multifactor (MFA)
La autenticación multifactor es un enfoque en capas para proteger datos y aplicaciones donde un sistema requiere que un usuario presente una combinación de dos o más credenciales para verificar su identidad para iniciar sesión.

Tecnología operativa (OT)
Sistemas o dispositivos programables que interactúan con el entorno físico (o gestionan dispositivos que interactúan con el entorno físico).

Gestión de correcciones
El proceso de distribuir y aplicar actualizaciones de seguridad al software y a los sistemas operativos.

Phishing
Una forma digital de ingeniería social para engañar a las personas y conseguir que proporcionen información confidencial.

Gestión de configuración de seguridad (SecCM)
La gestión y el control de las configuraciones de un sistema de información para permitir la seguridad y facilitar la gestión del riesgo.

Tácticas, técnicas y procedimientos (TTP)
El comportamiento de un agente. Una táctica es la descripción de más alto nivel de este comportamiento, mientras que las técnicas dan una descripción más detallada del comportamiento en el contexto de una táctica, y los procedimientos, una descripción de nivel aún más bajo, altamente detallada en el contexto de una técnica.

Vulnerabilidad
Una debilidad característica o específica que hace que una organización o un activo (como la información o un sistema de información) quede expuesto a la explotación por una amenaza determinada o sea susceptible a un peligro determinado.

Gestión de vulnerabilidades
El proceso mediante el cual las organizaciones identifican, analizan y gestionan las vulnerabilidades en el entorno operativo de un servicio crítico.

Apéndice 2: Acrónimos y abreviaturas

ACL: lista de control de acceso
AES: estándar de cifrado avanzado
API: interfaz de programación de aplicaciones
ASLR: aleatoriedad en la disposición del espacio de direcciones
ATT&CK: tácticas, técnicas y conocimiento común del adversario
BEC: compromiso del correo electrónico empresarial
CCM: gestión de la configuración y los cambios
CISA: Agencia de Ciberseguridad y Seguridad de la Infraestructura
CPG: objetivos de desempeño de ciberseguridad
CPU: unidad central de procesamiento
CRS: Resumen de riesgos cibernéticos
CSA: aviso sobre ciberseguridad
CVSS: Sistema común de puntuación de vulnerabilidades
CyHy: higiene cibernética
CY: año calendario
EDR: detección y respuesta en puntos finales
ePHI: información médica protegida electrónica
EPSS: Sistema de puntuación de predicción de exploits
ECDSA: algoritmo de firma digital de curva elíptica
FBI: Oficina Federal de Investigaciones
FIM: monitoreo de integridad de archivos
FTP: protocolo de transferencia de archivos
HHS: Departamento de Salud y Servicios Humanos
H-ISAC: Centro de análisis e intercambio de información sanitaria
HIPAA: Ley de Portabilidad y Responsabilidad del Seguro Médico
HPH: atención médica y salud pública
HSM: módulo de seguridad de hardware
IDS: sistema de detección de intrusiones
IT: tecnología de la información
JNDI: interfaz de nombres y directorios de Java
KEV: vulnerabilidades explotadas conocidas
LDAP: Protocolo ligero de acceso a directorios
MFA: autenticación multifactor
MDS: declaración de divulgación del fabricante
NetBIOS: sistema básico de entrada/salida en red
NIST: Instituto Nacional de Estándares y Tecnología
OS: sistema operativo
OT: tecnología operativa
OWASP: Open Web Application Security Project
PHI: información médica protegida
PII: información de identificación personal
PKI: infraestructura de clave pública
RDP: protocolo de escritorio remoto
RFI: solicitud de información
RPC: llamada a procedimiento remoto
SBOM: lista de materiales de software
SecCM: gestión de configuración de seguridad
SIEM: gestión de eventos e información de seguridad
SMB: bloque de mensajes del servidor
SMS: servicio de mensajes cortos/mensajería corta
SNMP: protocolo simple de administración de redes
SOP: procedimiento operativo estándar
SPF: marco de políticas para remitentes
SQL: lenguaje de consulta estructurado
SSO: inicio de sesión único
SSVC: categorización de vulnerabilidades específica de las partes interesadas
TCP: protocolo de control de transmisión
Telnet: red de teletipo
TLS: seguridad de la capa de transporte
TTP: tácticas, técnicas y procedimientos
UEBA: análisis del comportamiento de usuarios y entidades
VLAN: red de área local virtual
VPN: red privada virtual
VS: escaneo de vulnerabilidades
WAF: firewall de aplicaciones web
WAS: escaneo de aplicaciones web
WebAuthn: autenticación web