NULLWIRE SECURITY

PROPUESTA PARA MERIDIAN HEALTH SYSTEMS

Propuesta de Prueba de Penetración de Portal

Una evaluación de equipo rojo de alcance completo del portal de pacientes, respaldada por un contrato de retención para respuesta a brechas — diseñada para infraestructura regulada por HIPAA.

2026

CONTENIDO

DE UN VISTAZO

PROPUESTA

PRO-2026-0771

PARA APROBACIÓN

PREPARADO PARA

EXAMPLE DOCUMENT · WAXTABLE.COM

Meridian Health Systems — Renata Cole, Directora de Seguridad de la Información

PREPARADO POR
Nullwire Security, Seattle

EMITIDO
22 de enero de 2026

VÁLIDO HASTA
6 de marzo de 2026

ENCARGO
Evaluación de Seguridad y Servicio de Retención

DE UN VISTAZO

EL PROYECTO EN CINCO CIFRAS

WAXTABLE.COM · EXAMPLE DOCUMENT

Renata Cole, Director de seguridad de la información

WAXTABLE.COM · EXAMPLE DOCUMENT

01

LA OPORTUNIDAD

El portal de pacientes de Meridian Health Systems gestiona hoy resultados de laboratorio, facturación y mensajería para 340 000 pacientes, y nunca ha sido sometido a una evaluación externa de red team. Este es el plan para ponerlo a prueba como corresponde y estar preparados si algo llega a filtrarse.

RESUMEN EJECUTIVO

El portal de pacientes de Meridian Health Systems ha pasado de ser un programador de citas a convertirse en el canal principal para resultados de laboratorio, facturación y mensajería segura en toda su red hospitalaria. Se ha escaneado internamente en busca de vulnerabilidades conocidas cada trimestre, pero nunca ha enfrentado a un adversario externo que encadene pequeñas debilidades de la manera en que lo haría un atacante real, y la brecha de salud promedio todavía tarda más de 200 días en detectarse.

Nullwire Security propone un compromiso de ocho semanas que combina una prueba de penetración de alcance completo — externa, interna e ingeniería social — con un contrato de retención permanente para respuesta a brechas, de modo que Meridian sea evaluado antes de un incidente y esté listo para responder durante uno. Las siguientes secciones exponen el enfoque, el alcance, el cronograma y la inversión.

WAXTABLE.COM · EXAMPLE DOCUMENT

EL DESAFÍO

Los escaneos internos de vulnerabilidades detectan CVEs conocidos, pero pasan por alto exploits encadenados, integraciones de terceros mal configuradas y los puntos débiles humanos que una campaña de phishing atacaría. La API de resultados de laboratorio de Meridian y la conexión con el proveedor de facturación nunca han sido evaluadas de forma independiente.

A nivel operativo, la detección y respuesta nunca se han ensayado frente a un escenario real. Si ocurriera una brecha, el plan de respuesta a incidentes registrado no ha sido probado, y el equipo no sabe cuánto tiempo tomaría realmente la contención.

NUESTRO ENFOQUE

Ejecutamos el compromiso como lo haría un adversario real: reconocimiento y explotación externos, movimiento lateral desde un endpoint comprometido simulado, y una campaña de ingeniería social contra la mesa de ayuda, junto con una revisión dedicada de las dos integraciones de terceros que manejan datos de pacientes.

Los hallazgos se mapean directamente a la Regla de Seguridad de HIPAA y se entregan con una reprueba de remediación, de modo que nada se marca como cerrado hasta que se verifica que fue corregido. El contrato de retención para respuesta a brechas mantiene luego al mismo equipo disponible, de modo que el próximo incidente sea ensayado, no improvisado.

01
Más de 140
PRUEBAS DE PENETRACIÓN COMPLETADAS

02
<4 hrs
TIEMPO MEDIO DE ACTIVACIÓN DE RESPUESTA ANTE BRECHAS

03
8 semanas
DEL ALCANCE AL INFORME FINAL

SITUACIÓN

REGISTROS, COBERTURAS Y GARANTÍAS

CREDENCIAL	ENTIDAD EMISORA	REFERENCIA	ALCANCE	ESTADO
Entidad registrada	Registro de sociedades, Estados Unidos	Nullwire Security LLC	Nombre comercial e identidad jurídica	Activo
Registro fiscal	Autoridad fiscal, Estados Unidos	EIN 91-4820376	Todos los trabajos facturados	Activo
Seguro de responsabilidad civil profesional	Aseguradora comercial	Disponible a solicitud	Evaluación de Seguridad y Servicio de Retención	Se renueva anualmente
Seguro de responsabilidad civil general	Aseguradora comercial	Disponible a solicitud	Trabajos en sitio y en las instalaciones del cliente	Se renueva anualmente

WAXTABLE.COM · EXAMPLE DOCUMENT

Afiliación a un organismo profesional	Asociación sectorial, Estados Unidos	Disponible a solicitud	Código de conducta y procedimiento de reclamaciones	Al corriente

Los certificados y anexos de pólizas se entregan a solicitud y se reemiten a Meridian Health Systems a solicitud en cualquier momento durante el encargo.

Nullwire encontró un exploit encadenado que nuestro equipo interno había pasado por alto durante dos años, y nos tuvo contenidos en una hora cuando pusimos a prueba el retainer en un caso real.

OWEN MARSH

WAXTABLE.COM · EXAMPLE DOCUMENT

02

ALCANCE DEL TRABAJO

Un encargo de ocho semanas que combina una prueba de penetración de alcance completo con un servicio de retención permanente de respuesta ante brechas, para que Meridian Health Systems esté evaluado antes de un incidente y preparado para responder durante uno.

01
PRUEBA DE PENETRACIÓN EXTERNA

Activos expuestos a internet, el portal de pacientes y sus API públicas, evaluados hasta la explotación.

02
MOVIMIENTO INTERNO Y LATERAL

Un escenario simulado de endpoint comprometido, evaluando hasta dónde podría desplazarse un atacante una vez dentro.

03
INGENIERÍA SOCIAL

Una simulación de phishing y una campaña de pretexting de mesa de ayuda dirigida al personal.

04
REVISIÓN DE INTEGRACIONES DE TERCEROS

Evaluación de seguridad de las conexiones API con los proveedores de resultados de laboratorio y facturación.

05
RETAINER DE RESPUESTA ANTE BRECHAS

Respuesta a incidentes disponible bajo demanda y un manual de respuesta ensayado y listo para ejecutarse.

06
INFORMES DE CUMPLIMIENTO

Hallazgos vinculados directamente con la Regla de Seguridad de HIPAA para auditoría e informes a la junta directiva.

ENTREGABLES

[01] PRUEBAS

INFORME DE PRUEBA DE PENETRACIÓN DE ALCANCE COMPLETO

Hallazgos externos, internos y de movimiento lateral, con detalle de prueba de concepto y calificaciones de gravedad.

[02] PRUEBAS

EVALUACIÓN DE INGENIERÍA SOCIAL

Resultados de phishing y pretextos de mesa de ayuda, con recomendaciones de concientización dirigidas al personal.

[03] RESPUESTA

MANUAL DE RESPUESTA ANTE BRECHAS

Un plan de respuesta ante incidentes ensayado, con roles definidos, vías de escalamiento y la línea de guardia de Nullwire.

[04] CUMPLIMIENTO

INFORME DE HALLAZGOS VINCULADO A HIPAA

Cada hallazgo vinculado a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA, listo para auditoría.

[05] HABILITACIÓN

REPRUEBA DE REMEDIACIÓN Y APROBACIÓN FINAL

Una reprueba de seguimiento que verifica que cada hallazgo esté cerrado, con aprobación por escrito.

FUERA DEL ALCANCE

- Pruebas de penetración física de instalaciones más allá de los dos centros de datos nombrados
- Auditoría de código fuente de aplicaciones de proveedores externos
- Monitoreo continuo del SOC 24/7 más allá de la ventana de guardia del servicio de retención
- Presentación regulatoria y asesoría legal de notificación de brechas

WAXTABLE.COM · EXAMPLE DOCUMENT



[01] ▸ SEMANAS 1–2 · ALCANCE Y RECONOCIMIENTO

Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque.

[02] ▸ SEMANAS 3–5 · PRUEBAS ACTIVAS

Pruebas externas, internas y de ingeniería social contra el alcance acordado.

[03] ▸ SEMANA 6 · HALLAZGOS Y MAPEO HIPAA

Consolidación de hallazgos y mapeo a las salvaguardas relevantes de la Regla de Seguridad de HIPAA.

[04] ▸ SEMANA 7 · APOYO A LA REMEDIACIÓN

Apoyo guiado en la remediación para el equipo de ingeniería antes de la reprueba.

WAXTABLE.COM · EXAMPLE DOCUMENT

03

INVERSIÓN Y CONDICIONES

Las cuentas de prueba y una carta firmada de reglas de participación se entregan antes de que comience la prueba; un responsable está facultado para autorizar cambios de alcance en cada etapa; y las pruebas se limitan al portal de pacientes y sus dos integraciones de terceros designadas. Los cambios a esto modifican el cronograma y el costo, lo cual acordaríamos por escrito antes de proceder. La tarifa se mantiene para contrataciones que comiencen en o antes del 6 de marzo de 2026.

FLUJO DE TRABAJO	SEMANAS	TARIFA	IMPORTE
Alcance y reconocimiento Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque	2	$9,500 / wk	$19,000
Prueba de penetración externa Evaluación del portal de pacientes y la API expuestos a internet	2	$14,000 / wk	$28,000
Pruebas internas y de ingeniería social Escenario simulado de endpoint comprometido y ejercicio de phishing	1	$16,000 / wk	$16,000
Revisión de integraciones de terceros Evaluación de seguridad de la API de resultados de laboratorio y del proveedor de facturación	1	$12,000 / wk	$12,000
Informes y apoyo a la remediación Informe de hallazgos, mapeo HIPAA y guía de remediación	1	$10,000 / wk	$10,000
Reprueba y configuración de retención Reprueba de verificación de correcciones y entrega del manual de respuesta ante brechas	1	$9,000 / wk	$9,000
Total del proyecto			**$94,000**

WAXTABLE.COM · EXAMPLE DOCUMENT

HONORARIOS DEL PROYECTO	$94,000
IMPUESTO SOBRE VENTAS (WA — SERVICIOS PROFESIONALES EXENTOS)	$0
TOTAL	$94,000

TOTAL ADEUDADO **$94,000**

Todos los montos están en USD. Facturado en tres hitos: 40% en la firma, 30% al inicio de la construcción, 30% en la entrega. La tarifa se mantiene para contrataciones que comiencen en o antes del 6 de marzo de 2026.

01
EVALUACIÓN
$94,000

- Compromiso completo de ocho semanas
- Pruebas externas, internas y de ingeniería social
- Informe de hallazgos vinculado a HIPAA
- Dos semanas de soporte de remediación

02
EVALUACIÓN + RETAINER
$6,500/mo

- Todo lo incluido en Evaluación
- Línea directa de respuesta ante brechas 24/7
- Reescaneo mensual de vulnerabilidades
- SLA de respuesta prioritaria a incidentes (<4 hrs)

03
DEFENSA CONTINUA
$13,000/mo

- Todo lo incluido en Retainer
- Ejercicios trimestrales de equipo rojo
- Monitoreo continuo de la superficie de ataque externa
- Tiempo integrado de ingeniería de seguridad

OPCIONES

QUÉ MODALIDAD TE CONVIENE

	EVALUACIÓN	EVALUACIÓN + RETAINER	DEFENSA CONTINUA
Precio	$94,000	$6,500/mo	$13,000/mo
Alcance principal	Compromiso completo de ocho semanas	Todo lo incluido en Evaluación	Todo lo incluido en Retainer
Qué incluye	Pruebas externas, internas y de ingeniería social	Línea directa de respuesta ante brechas 24/7	Ejercicios trimestrales de equipo rojo
Entrega	Informe de hallazgos vinculado a HIPAA	Reescaneo mensual de vulnerabilidades	Monitoreo continuo de la superficie de ataque externa
Servicio posterior	Dos semanas de soporte de remediación	SLA de respuesta prioritaria a incidentes (<4 hrs)	Tiempo integrado de ingeniería de seguridad

Los precios están en USD y no incluyen el impuesto sobre las ventas (wa — servicios profesionales exentos). Las opciones se pueden combinar o escalonar; la recomendación para Meridian Health Systems se destaca en la sección de precios.

CALENDARIO DE PAGOS

CUÁNDO VENCE CADA CUOTA

N.º	HITO	DESENCADENANTE	PARTE	IMPORTE
01	Semanas 1–2 · Alcance y reconocimiento	16 de febrero de 2026	40%	$37,600
02	Semanas 3–5 · Pruebas activas	Al inicio de la entrega	30%	$28,200
03	Semana 6 · Hallazgos y mapeo HIPAA	En la aceptación del hito	30%	$28,200
Total (sin impuestos)			**100%**	**$94,000**

Las cuotas se facturan conforme a los hitos anteriores y son pagaderas dentro de los 30 días siguientes a cada factura. Todos los importes están expresados en USD y no incluyen impuesto sobre ventas (wa — servicios profesionales exentos).

SUPUESTOS DE LOS QUE DEPENDE ESTA ESTIMACIÓN

Se proporcionan cuentas de prueba y una carta firmada de reglas de compromiso antes de que comiencen las pruebas; un representante está facultado para autorizar cambios de alcance en cada etapa; y las pruebas se limitan al portal de pacientes y sus dos integraciones de terceros designadas. Los cambios a esto modifican el cronograma y el costo, lo cual acordaríamos por escrito antes de proceder. La tarifa se mantiene para compromisos que inicien el 6 de marzo de 2026 o antes.

Al firmar a continuación se acepta el alcance, el cronograma y la inversión establecidos en esta propuesta, y se autoriza el inicio del trabajo.

POR MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRECTORA DE SEGURIDAD DE LA INFORMACIÓN

Fecha

POR NULLWIRE SECURITY

NULLWIRE SECURITY

FIRMANTE AUTORIZADO

Fecha

WAXTABLE.COM · EXAMPLE DOCUMENT

PRÓXIMOS PASOS

LISTOS CUANDO USTED LO ESTÉ

La aceptación de esta propuesta da inicio al trabajo el 16 de febrero de 2026. La tarifa se mantiene para los proyectos confirmados antes del 6 de marzo de 2026.

Apruebe esta propuesta y podremos reservar el inicio del alcance para la semana del 16 de febrero. Responda a este documento o escriba a contact@nullwiresecurity.com.

Nullwire Security
contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com · Seattle, WA 98109

WAXTABLE.COM · EXAMPLE DOCUMENT