NULLWIRE SECURITY

PREPARADO PARA MERIDIAN HEALTH SYSTEMS

Alcance de trabajo

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

SOW

SOW-2026-0771

BORRADOR

ESTADO

Borrador — para revisión

DE UN VISTAZO

ALCANCE, CRONOGRAMA Y HONORARIOS

01
FLUJO DE TRABAJO

Evaluación de Seguridad y Servicio de Retención

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.

02
INICIO

16 de febrero de 2026

Con la contrafirma

03
DURACIÓN

12 meses

Por fases según el calendario siguiente

04
HONORARIOS

$94,000

$94,000, más impuesto sobre ventas (wa — servicios profesionales exentos)

05
ACEPTADO POR

Renata Cole

Directora de Seguridad de la Información

01

RESUMEN Y OBJETIVOS

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.

CONTEXTO Y METAS

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.

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

[01]

PRUEBAS DE NIVEL ADVERSARIO

Pruebas externas, internas y de ingeniería social ejecutadas de la forma en que un atacante real las encadenaría.

[02]

INFORMES MAPEADOS A HIPAA

Cada hallazgo mapeado a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA, listo para auditoría e informes a la junta.

[03]

RESPUESTA PERMANENTE

Un manual de respuesta a brechas ensayado y una retención de guardia permanente, para que el próximo incidente esté ensayado, no improvisado.

ESPECIFICACIÓN

ESPECIFICACIÓN DEL FLUJO DE TRABAJO

REF.	ÍTEM	ESPECIFICACIÓN	ESFUERZO	PLAZO	PRECIO UNITARIO
SPC-01	Alcance y reconocimiento	Reglas de compromiso, enumeración de activos y mapeo de la superficie de ataque	2	2 sem.	$9,500 / wk
SPC-02	Prueba de penetración externa	Evaluación del portal de pacientes y la API expuestos a internet	2	2 sem.	$14,000 / wk
SPC-03	Pruebas internas y de ingeniería social	Escenario simulado de endpoint comprometido y ejercicio de phishing	1	1 sem.	$16,000 / wk
SPC-04	Revisión de integraciones de terceros	Evaluación de seguridad de la API de resultados de laboratorio y del proveedor de facturación	1	1 sem.	$12,000 / wk
SPC-05	Informes y apoyo a la remediación	Informe de hallazgos, mapeo HIPAA y guía de remediación	1	1 sem.	$10,000 / wk

Las especificaciones quedan fijadas en el momento de la aceptación; cualquier cambio se gestiona mediante el procedimiento de control de cambios establecido en este documento.

[01] SEMANAS 1–2 · ALCANCE Y RECONOCIMIENTO

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

[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.

[05] ▸ SEMANA 8 · REPRUEBA Y ACTIVACIÓN DEL RETAINER

Reprueba de verificación de correcciones y traspaso del manual de respuesta ante brechas.

CRITERIOS DE ACEPTACIÓN

REF.	REQUISITO	PRIORIDAD
R-01	Las pruebas externas e internas deben incluir el portal de pacientes y sus dos integraciones de terceros nombradas	OBLIGATORIO
R-02	Cuentas de prueba y una carta firmada de reglas de compromiso proporcionadas antes de iniciar las pruebas	OBLIGATORIO
R-03	Todos los hallazgos asignados a la salvaguarda correspondiente de la Regla de Seguridad de HIPAA	OBLIGATORIO
R-04	Hallazgos críticos y altos vueltos a probar y verificados como cerrados antes de la aprobación final	OBLIGATORIO
R-05	Campaña de ingeniería social limitada a la mesa de ayuda y departamentos nombrados	OBLIGATORIO

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
Subtotal de honorarios			**$94,000**

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

TOTAL $94,000

Todos los importes están en USD y no incluyen los impuestos aplicables. Los honorarios se facturan en tres hitos: 40% a la firma, 30% al inicio de la construcción, 30% en la puesta en marcha.

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).

La contrafirma a continuación acepta el alcance, el cronograma, los criterios de aceptación y los honorarios establecidos en este Alcance de Trabajo y autoriza el inicio de los trabajos en la fecha de inicio indicada.

POR MERIDIAN HEALTH SYSTEMS

RENATA COLE

DIRECTORA DE SEGURIDAD DE LA INFORMACIÓN

Fecha

POR NULLWIRE SECURITY

NULLWIRE SECURITY

FIRMANTE AUTORIZADO

Fecha

NULLWIRE SECURITY

500 Yale Ave N, Seattle, WA 98109,
Estados Unidos

contact@nullwiresecurity.com · +1 206 555 0189 · nullwiresecurity.com

Nullwire Security LLC · EIN 91-4820376