Términos de referencia

Consultoría en materia de Seguridad informática perimetral y de software

Descripción General: Consultoría en materia de Seguridad informática, para la revisión y optimización de las plataformas tecnológicas, la red, aplicativos y páginas Web de Amnistía Internacional, Sección Mexicana, A.C. **Período de servicios**: 3 meses. **Dirección de correo electrónico de contacto**: consultoria.seguridad@amnistia.org.mx

I. Descripción del proyecto.

La seguridad informática es, sin lugar a dudas, un componente técnico que siempre debe ser contemplado en todos los proyectos de desarrollo Web, debido a las múltiples amenazas existentes de forma permanente en la Internet y a la necesidad de proteger los datos de una organización como Amnistía Internacional, Sección Mexicana, A.C.

Los objetivos principales de este proyecto son los siguientes:

- Análisis y revisión, en materia de seguridad informática, de sistemas, aplicaciones y plataformas Web, que incluyan el *Front End* y el *Back End*, así como todo lo relacionado con la seguridad de las bases de datos de Amnistía Internacional México.
- Diseñar y ejecutar pruebas de vulnerabilidad de las plataformas, sistemas Web y sus bases de datos integradas.
- Acompañar la implementación (a nivel de código PHP) de las mejoras y ajustes de seguridad de las plataformas y sistemas Web.
- Optimizar la seguridad física de la red informática de Amnistía Internacional México mediante dispositivo físico o firewall (a cargo de la consultora).

II. Descripción de la consultoría

Titulo	Consultoría en materia de Seguridad informática, para la revisión y optimización de las plataformas tecnológicas, red, aplicativos y páginas Web de Amnistía Internacional, Sección Mexicana, A.C.

Proyecto	Seguridad Informática Web.
Localidad	Remoto y presencial, con disponibilidad para reuniones virtuales y presenciales.
Tipo de contrato	Servicios profesionales y técnicos por tiempo definido.
Duración del proyecto	3 meses
Monto	$176,724.00 MXN +IVA 16%
Supervisión	Jefatura de Tecnologías de Información y Comunicación.
Relaciones Internas	Subdirección de Soporte, Jefatura de Comunicación y Campañas, Especialista en desarrollo de software, Coordinador de crecimiento digital y Responsable de Comunicación Digital.
Relaciones Externas	N/A
Objetivo principal de la consultoría	Brindar los servicios a la oficina de Amnistía Internacional, Sección Mexicana, A.C., a través de la Jefatura de Tecnologías de Información y Comunicación, para el mejoramiento y optimización de la seguridad Web de las plataformas y sistemas de la organización.
Perfil requerido	Especialista(s) en: • Ataques DDoS • SQL Injection • Cross Site Scripting (XSS) • Configuración de firewall físico y VPNs Asimismo en el uso de herramientas para realizar pruebas de seguridad a plataformas Web. Conocimientos profundos en el estándar ISO IEC 27001/27002. Recomendable una certificación en este estándar.
Habilidades	Análisis de entornos y plataformas Web para detectar vulnerabilidades, diseño y ejecución de pruebas de seguridad DDoS, SQL Injection y XSS. Reportes, acompañamiento en la programación de los ajustes de seguridad con código PHP, SQL y en la optimización de la seguridad en la Web y la prevención de eventuales ataques futuros.
Objetivos específicos de la consultoría	• Integrar y configurar firewall físico a la red (proporcionado por la consultora), conforme a las necesidades de la organización. • Realizar pruebas al firewall y documentar la configuración final. • Realizar un inventario de aplicativos, plataformas y páginas Web que se revisarán.

	• Diseñar y ejecutar pruebas iniciales de vulnerabilidad de aplicativos, bases de datos, plataformas y páginas Web. • Análisis de resultados. • Crear un plan de trabajo para que se realicen las correcciones a las eventuales vulnerabilidades que resulten de las pruebas. • Acompañar y apoyar el equipo de Tecnologías de Información y Comunicación para realizar los ajustes que resulten de las pruebas de seguridad. • Realizar una segunda aplicación de pruebas de vulnerabilidad de aplicativos, sistemas y plataformas Web. • Presentación de resultados. • Liberación de aplicativos, sistemas y plataformas Web.

III. Entregables

A continuación se detallan los documentos que deberán generarse a lo largo de la consultoría:

1. Metodología de trabajo.

   Debe incluir:
   a. Cronograma de trabajo general donde se incluya la integración y configuración del firewall así como todas las plataformas y sitios Web de la organización.
   b. Diseño de instrumentos de pruebas de vulnerabilidad de las plataformas Web, tipificando el tipo de prueba y su objetivo.

2. Ejecución de pruebas de vulnerabilidad a las plataformas y sitios Web.

   Debe incluir:
   a. Cronograma de ejecución de pruebas.
   b. Documentar cada vulnerabilidad encontrada, indicando la plataforma o aplicación afectada, el tipo de vulnerabilidad, el nivel de criticidad y su solución.

3. Cronograma de ajustes de cada vulnerabilidad encontrada

Debe incluir:

a. Cronograma de implementación de las correcciones de cada vulnerabilidad.
b. Revisión y pruebas de las correcciones implementadas.

4. Entrega de resultados

Debe incluir:

a. Reporte final donde se indique el estatus final de cada vulnerabilidad encontrada.
b. Sugerencias
c. Conclusiones

IV. Calendario de entregables

Cronograma	**Fecha de entrega**
Inicio del proyecto	1 de noviembre de 2023
Metodología de trabajo	9 de noviembre de 2023
Instalación, configuración y entrega de firewall	10 al 17 de noviembre de 2023
Ejecución de pruebas de vulnerabilidad a plataformas y sitios Web	18 de noviembre al 3 de diciembre de 2023
Entrega de resultados	4 de diciembre de 2023
Cronograma de correcciones de cada vulnerabilidad encontrada	4 de diciembre de 2023
Acompañamiento al equipo de Tecnologías de Información y Comunicación en la implementación de las correcciones de las vulnerabilidades encontradas	5 al 20 de diciembre de 2023 y del 8 al 19 de enero de 2024
Revisión de ajustes a las correcciones de las vulnerabilidades encontradas	16 al 20 de diciembre de 2023 y del 8 al 22 de enero de 2024
Ajustes finales	23 al 30 de enero de 2024
Liberación de todas las plataformas Web	31 de enero de 2024

V. Requisitos de elegibilidad

Las propuestas se seleccionaran con base en los siguientes criterios y a partir de una suma simple la propuesta ganadora será la que tenga el puntaje mayor: **Criterios**	**Puntaje**
Metodología de trabajo	20
Experiencia de la consultoría	30

CV del equipo de trabajo	15
Propuesta económica	20
Organización del equipo de trabajo	15

VI. Acuerdos institucionales

La consultoría tendrá acceso a toda la documentación e información requerida referente al proyecto, durante el tiempo determinado de duración del contrato.

El equipo de la consultoría deberá cubrir cualquier costo que surja con su metodología de trabajo.

VII. Montos y forma de pago

Los honorarios incluyen todos los gastos que puedan surgir para la consultora.

Los pagos se realizarán en pesos mexicanos, previa entrega de comprobante fiscal.

VIII. Presentación de propuestas

Las y los interesados deben enviar los siguientes documentos:
- Currículum Vitae o Credenciales de la empresa. Si se trata de personas morales, adjuntar también CV del equipo de trabajo.
- Propuesta técnica que detalle: Metodología y equipo de trabajo con responsabilidades correspondientes.
- Cotización.

Las propuestas deben enviarse al correo consultoria.seguridad@amnistia.org.mx a más tardar el 12 de octubre de 2023.