



ANEXO CONVOCATORIA

12/2018

RENGLONES

| Renglón | Especificación Técnica | Imagen |
|---------|--|--------|
| | <p>Web Application Firewall (WAF)</p> <p><i>Solución del tipo WAF (Web Application Firewall) virtualizada o modelo appliance para proteger los sitios Web expuestos hacia internet de la Universidad. Deberá cumplir mínimamente con las siguientes características:</i></p> <ul style="list-style-type: none">• Protección contra ataques sofisticados.• Análisis de comportamiento.• Estadísticas de uso y algoritmos de prevención de ataques.• Posibilidad de escalar la solución.• Protección contra ataques del tipo DDoS.• Protección contra amenazas.• Protección basadas en OWASP Top Ten y CWE SANS.• Identificación de amenazas del día cero (0 day).• Posibilidad de agregar nuevas firmas.• Protección ante ataques de Fuerza Bruta.<ul style="list-style-type: none">• Prevenir y controlar la ejecución remota de código (RCE).<ul style="list-style-type: none">• Analizar el tráfico para evitar crear falsos positivos.• Habilidad para proteger aplicaciones y APIs.<ul style="list-style-type: none">• Posibilidad de verificar posibles vulnerabilidades.• Brindar información sobre posibles vulnerabilidades.• Contar con un panel de administración o | |



| Renglón | Especificación Técnica | Imagen |
|---------|---|--------|
| | <p>dashboard para ver en tiempo real los ataques.</p> <ul style="list-style-type: none">• Integración con sistemas de Bug Trackers.• Integración y/o envío de emails con alarmas o sistemas de monitoreo.• Disponibilidad para hacer uso de API.• La solución no deberá estar sujeta a algún tipo de lenguaje de programación utilizado. <p><i>Otras consideraciones:</i></p> <ul style="list-style-type: none">• Soporte en español 7 x 24.• Partner local.• Capacitaciones sobre el uso de la solución.• Manuales y Documentación disponible. <h2>S o l u c i ó n E s c á n e r d e Vulnerabilidades para Aplicaciones Web</h2> <p><i>Solución del tipo Cloud (nube) para realizar escaneo de vulnerabilidades en aplicaciones Web expuesta en Internet, alcance 10 hosts/dominios. La solución debe contar con las siguientes características:</i></p> <ul style="list-style-type: none">• Interfaz intuitiva y simple.• Integración con SDLC y sistemas de Desarrollo Continuo.<ul style="list-style-type: none">• Soporte para HTML5, Aplicaciones 2.0, JavaScript, Node.js., entre otras tecnologías nuevas.• Compatibilidad con CVSS, OWASP Top Ten.<ul style="list-style-type: none">• Reportes basados en OWASP Top Ten, Técnicos y Gerenciales.• Informar sobre los diferentes niveles de riesgo.<ul style="list-style-type: none">• Identificación de CVEs en productos vulnerables.<ul style="list-style-type: none">• Debe ser capaz de identificar y explotar vulnerabilidades del tipo XSS, SQL Injection, entre otras.• Identificación de vulnerabilidades complejas | |



| Renglón | Especificación Técnica | Imagen |
|---------|--|--------|
| | <p>como Out-of-Band SQL Injection, Server-side Request Forgery (SSRF), Blind Cross-site Scripting.</p> <ul style="list-style-type: none">• Soporte para múltiples tipos de autenticación, Basic Authentication, Basadas en Form, NTLM, Digest, Kerberos.• Colaboración de Equipos.• Organización de Websites dentro de Grupos.• Utilizar diferentes niveles de visualización y privilegios.• Configuración de diferentes roles, pudiendo escanear diferentes tipos de vulnerabilidades.• Administración y remediación de vulnerabilidades.• Abrir y asignar tickets con diferentes estados de las vulnerabilidades.• Panel de Administración con detalle de métricas y niveles de riesgo de las vulnerabilidades halladas.• El panel debe ser capaz de mostrar una visión general e individual para cada sitio Web escaneado. <p><i>Otras consideraciones:</i></p> <ul style="list-style-type: none">• Soporte en español 7 x 24.• Partner local.• Capacitaciones sobre el uso de la solución.• Manuales y Documentación disponible. <p>Buenas Prácticas de Seguridad para Windows & *NIX</p> <p><i>Se solicita guías de buenas prácticas para diferentes sistemas operativos basados en Windows y *NIX. Las mismas deberán indicar las configuraciones necesarias para asegurar los sistemas, realizando un fortalecimiento o Hardening alineados al Best Practices for Security Fundamentals de Windows y los Security Benchmarks de CIS (Center for Internet Security). Ambas políticas deben</i></p> | |



| Renglón | Especificación Técnica | Imagen |
|---------|---|--------|
| | <p><i>contemplar:</i></p> <ul style="list-style-type: none">• Configuración de Servicios Básicos.• Seguridad para usuarios.• Bloqueo y política de contraseñas.• Configuración de Logs.• Permisos y accesos remotos.• Administración de Registros.• Mejores prácticas para IIS/Apache.• Cifrado y comunicaciones seguras.• Administración segura. <p><i>Se esperan 2 documentos, siendo 1 para Windows y otro para *NIX, el sistema operativo será definido en conjunto.</i></p> <h2>Servicio de Desarrollo y Operaciones</h2> <p><i>Se deberá proveer de servicios Desarrollo y Operaciones para la creación de un departamento de orquestación y automatización de servicios, que incluya los siguientes ítems:</i></p> <ul style="list-style-type: none">• Plan de acción para aplicaciones• Selección de aplicaciones• Con enfoque a producir resultados en el corto plazo a bajo riesgo.• Relevamiento de arquitectura de aplicaciones• Lenguajes• Frameworks• Middleware• Protocolos• Componentes• Integraciones• Relevamiento de flujo de desarrollo actual• Flujo de trabajo de desarrolladores• Herramientas que se utilizan• Manejo de builds para cada ambiente• Administración de dependencias entre | |



| Renglón | Especificación Técnica | Imagen |
|---------|---|--------|
| | <p>proyectos</p> <ul style="list-style-type: none">• Librerías externas• Pruebas de ejecución• Distribución y despliegue de aplicaciones en los diferentes ambientes• Administración y configuración de aplicaciones• Definición de un nuevo flujo de desarrollo• Controles de fuentes• Builds automatizados• Mismo equipamiento para todos los ambientes• Pruebas unitarias• Disponibilidad de ambientes para integración continua• Generación de reportes con métricas de los fuentes• Generación y publicación de equipos en un repositorio centralizado• Accesibilidad del equipo de desarrollo y operaciones• Ejecución de definiciones para aplicaciones ya instaladas• Despliegue de versiones específicas de aplicaciones en ambientes no productivos• Aprovisionamiento y orquestación• Configuración y despliegue de los equipos de las aplicaciones en los contenedores• Independencia de infraestructura disponible• Ejecución, documentación y transferencia de conocimiento• Ejecución de proceso definido para la aplicación seleccionada• Documentación de procesos y herramientas utilizadas• Transferencia de conocimiento <p><i>Plan de acción para infraestructura:</i></p> <ul style="list-style-type: none">• Selección de infraestructura• Relevamiento de arquitectura• Relevamiento de flujo y implementación• Definición del nuevo flujo de implementación• Definición del mecanismo de aprovisionamiento• Ejecución de definiciones para infraestructura | |



| Renglón | Especificación Técnica | Imagen |
|---------|---|--------|
| actual | <p><i>Definición de roles y organigrama para el nuevo departamento:</i></p> <ul style="list-style-type: none">• Director de proyecto• Equipo de desarrollo• Equipo de operaciones• Usuarios claves | |

Firma del Responsable de Contrataciones