CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA

CSTISA Gestión de Vulnerabilidades

Empresa: -
Revisión: Febrero 5, 2026
Realizada por: Angel Chaljub

1- INTRODUCCION

Hoy en día, la infraestructura tecnológica no es solo un soporte, sino el motor real de la competitividad y la confianza empresarial. Sin embargo, ante ataques cibernéticos cada vez más astutos, cualquier debilidad técnica deja de ser un simple fallo informático para convertirse en un riesgo financiero latente. Un descuido aquí puede frenar la cadena de suministro, hundir la reputación y poner en jaque la supervivencia misma del negocio.

CSTISA presenta este servicio de **Gestión de Vulnerabilidades** como una solución de visibilidad estratégica. Nuestro enfoque no se limita únicamente a satisfacer los requerimientos de marcos regulatorios y certificaciones internacionales (**BASC, OEA, TISAX o Ley 172-13**); nuestra prioridad es identificar y priorizar las brechas de seguridad reales antes de que sean explotadas.

A través de este proceso, transformamos datos técnicos en inteligencia de negocio, permitiendo que la gerencia tome decisiones informadas para blindar sus activos críticos, proteger sus márgenes de beneficio y proyectar una imagen de solidez ante sus socios comerciales y clientes finales.

2- REQUERIMIENTO Y ALCANCE:

El servicio se enfocará en validar la robustez de los activos que soportan los procesos críticos del negocio.

- **Alcance Externo:** Escaneo de IPs públicas, portales web, servicios de VPN y puntos de acceso expuestos a internet.
- **Alcance Interno:** Evaluación de servidores críticos (AD, ERP, Base de Datos), dispositivos de red (Firewalls, Switches) y estaciones de trabajo de personal clave.

3- METODOLOGIA

Nuestro proceso se basa en un **Ciclo Proactivo de Gestión de Brechas**, diseñado para identificar debilidades sin interrumpir la operatividad de su empresa. El flujo de trabajo se divide en cuatro fases críticas:

1. **Descubrimiento (Reconnaissance):** Identificación de activos en la red.
2. **Escaneo Técnico:** Ejecución de pruebas no intrusivas para detectar versiones vulnerables, configuraciones erróneas y parches faltantes.
3. **Análisis y Clasificación:** Filtrado de falsos positivos y categorización de riesgos según el sistema CVSS (Common Vulnerability Scoring System).
4. **Alineación de Cumplimiento:** Traducción de los hallazgos técnicos a los requisitos de las normativas vigentes (BASC, OEA, TISAX, Ley 172-13).

4- ALINEACION CON MARCO REGULATORIO DOMINICANO

Este servicio muestra como su organización cumple con las exigencias legales vigentes en el país:

- **Ley No. 172-13:** Protección de datos personales de clientes y empleados.
- **Ley No. 53-07:** Prevención de crímenes y delitos de alta tecnología.
- **Estándares BASC / OEA:** Evidencia técnica para auditorías de comercio seguro.
- **Reglamento de Seguridad Cibernética y de la Información:** Normativa que obliga a bancos, puestos de bolsa y remesadoras a realizar auditorías de vulnerabilidades.

5- ENTREGABLES

Al finalizar el servicio, se hará entrega de:

1. **Reporte Ejecutivo de Vulnerabilidades:** Clasificación de las vulnerabilidades por su nivel de criticidad (alto, medio, bajo, información) y por CVSS.
2. **Informe Técnico Detallado:** Listado de vulnerabilidades encontradas con su respectiva solución técnica (remediación).

6- REQUERIMIENTOS GENERALES

Para la ejecución exitosa, el cliente deberá proveer:

- Acceso temporal a la red interna (vía VPN o presencial).
- Listado de activos (IPs) a evaluar o segmento de red.
- Designación de un enlace técnico para coordinación.

7- EQUIPO DE TRABAJO

El proyecto será liderado por **[NOMBRE CONSULTOR]**, consultor especialista en Ciberseguridad, acompañado de personal técnico certificado en gestión de vulnerabilidades y defensa de redes. Contamos con herramientas de grado empresarial (como Nessus Professional) para garantizar la precisión de la data entregada a los auditores.