CONSULTORES EN SEGURIDAD
TECNOLOGICA E INFORMATICA

CSTISA Cyber-CheckUp

Empresa: -
Revisión: enero 27, 2026
Realizada por: Ángel Chaljub

1- INTRODUCCION

La seguridad digital ya no es solo cosa de expertos, es la base de un negocio sólido. Con el servicio **CSTISA Cyber-CheckUp**, reforzamos la protección de tu organización con un enfoque flexible que se ajusta a lo que realmente necesitas, seas un startup o una gran empresa.

Nuestra misión es proporcionar a la alta gerencia una hoja de ruta clara, objetiva y accionable basada en el marco internacional **NIST CSF 2.0**. No nos limitamos a identificar vulnerabilidades; analizamos la **Gobernanza**, protegemos los activos críticos y diseñamos la capacidad de respuesta necesaria para que, ante cualquier incidente, su organización no solo sobreviva, sino que se recupere con mayor fortaleza.

Nuestro enfoque combina el profesionalismo técnico con una organización ágil, convirtiéndonos en el aliado estratégico para acelerar la madurez de su seguridad de la información.

2- REQUERIMIENTO Y ALCANCE:

El objetivo es realizar un diagnóstico integral de la postura de seguridad de [Nombre de la Empresa].

- Alcance: Se limitará a la información facilitada por el cliente y se basará en las funciones esenciales del marco NIST CSF 2.0 (National Institute of Standards and Technology).

- Enfoque: Evaluación orientada a identificar riesgos críticos que afecten la disponibilidad, integridad y confidencialidad de sus datos.

3- METODOLOGIA

Utilizamos una técnica de entrevista técnica y funcional dirigida al personal responsable de IT o de los procesos internos de la empresa. Evaluaremos objetivamente las siguientes categorías internacionales.

ID Función	Función	
GV	Gobernanza	¿Está la ciberseguridad alineada con los objetivos del negocio?
ID	Identificar	¿Sabemos qué tenemos? (Inventario de laptops, servidores y nubes).
PR	Proteger	¿Qué barreras hay? (Antivirus, contraseñas, firewall).
DE	Detectar	¿Nos damos cuenta si entran? (Alertas de inicio de sesión inusual).
RS	Responder	¿Qué hacemos si nos hackean? (Plan de acción rápido).
RC	Recuperar	¿Cómo volvemos a trabajar? (Backups que funcionen).

4- ENTREGABLES

Al finalizar, se emitirá un **Reporte Ejecutivo de Resiliencia** que incluye:

1. Situación Actual: Diagnostico del estado real de sus activos
2. Postura de ciberseguridad (Scorecard): Calificación visual (tipo semáforo) basada en el criterio técnico de CSTISA
3. Recomendaciones y Plan de Acción: Acciones prioritarias para mitigar riesgos inmediatos
4. Hoja de Ruta (Roadmap): Proyectos a futuro sugeridos para fortalecer la empresa a largo plazo.
5. Alineación Legal: Comentarios breves sobre el cumplimiento básico de la Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología

Nota: CSTISA se enfoca en el diagnostico; no elaborará manuales o procedimientos internos que no existan en la organización.

5- REQUERIMIENTOS GENERALES

Para garantizar el éxito del servicio, solicitamos a [NOMBRE DE LA EMPRESA]:

- Disponibilidad del personal responsable de sistemas o procesos internos.
- Autorización para revisar configuración técnica y conocer las estrategias de desarrollo TIC.
- CSTISA garantiza la confidencialidad total y está dispuesta a firmar un acuerdo de no divulgación (NDA).

6- EQUIPO DE TRABAJO

Se asignará un Consultor de Seguridad experto en el marco NIST CSF 2.0. Funciones principales:

- Gestionar el plan de trabajo y validar los entregables.
- Liderar las presentaciones técnicas y la exposición ejecutiva de resultados.