

Temática

GOVERNANCE

SANS

¿Qué es?

La función mediante la cual una organización define, establece, comunica y supervisa su estrategia, expectativas y políticas de gestión de riesgos de seguridad cibernética.

Importancia para un CISO

- ✓ Visión estratégica y alineación con el negocio
- ✓ Gestión de riesgos a nivel empresarial (ERM)
- ✓ Definición de roles y responsabilidades
- ✓ Políticas y estándares organizativos
- ✓ Cadena de suministro y terceros
- ✓ Supervisión y rendición de cuentas

Componentes

Governance

- | | |
|--|---|
| <input type="checkbox"/> Strategy | <input type="checkbox"/> Roles and Responsibilities |
| <input type="checkbox"/> Business Alignment | <input type="checkbox"/> Workforce Planning |
| <input type="checkbox"/> Risk Management | <input type="checkbox"/> Resource Management |
| <input type="checkbox"/> Program Frameworks <ul style="list-style-type: none">• NIST CSF• ISO 27000 | <input type="checkbox"/> Data Classification |
| <input type="checkbox"/> Control Frameworks <ul style="list-style-type: none">• NIST 800-53• CIS Controls | <input type="checkbox"/> Security Policy |
| <input type="checkbox"/> Program Structure | <input type="checkbox"/> Creating a Security Culture |
| <input type="checkbox"/> Program Management | <input type="checkbox"/> Security Training <ul style="list-style-type: none">• Awareness Training• Role-Based Training |
| <input type="checkbox"/> Communications Plan | <input type="checkbox"/> Metrics and Reporting |
| | <input type="checkbox"/> IT Portfolio Management |
| | <input type="checkbox"/> Change Management |
| | <input type="checkbox"/> Board Communications |

Componentes

Control Frameworks

Implementar capacidades para asegurar la compañía en aspectos procedimentales, tecnológicos y de personal (Usar CIS Controls para aplicar controles como inventario de activos y gestión de parches.)

Risk Management

Evaluar el estado de las capacidades y las debilidades que la compañía tiene en ciberseguridad y que impactan sus objetivos estratégicos (Implementar un proceso trimestral de identificación y priorización de riesgos, donde ransomware se clasifique como riesgo crítico.)

Roles and Responsibilities

Definir una estructura de perfiles con funciones específicas de ciberseguridad que aborden su ciclo de vida (Definir que el CISO responde ante la junta, el SOC Manager lidera la operación y cada área de negocio nombra un "security champion"..)

Security Policy

Definir documentación que establezca los lineamientos y buenas prácticas que la compañía debe implementar para velar por el cumplimiento de sus objetivos estratégicos (Política que exija MFA para todos los accesos remotos y uso de VPN corporativa)



ESCUELA SUPERIOR DE GUERRA

“General Rafael Reyes Prieto”

Colombia