

SEGURANÇA CIBERNÉTICA



ekium.com.br



EKIUM

A COMPANY OF GROUPE SNEF

Tecnologia e Segurança Operacional.
Cibersegurança, SIS, Certificações
de Redes, Automação de Processos
e Integração de Sistema.



**SOLUÇÕES
INTEGRADAS**



**ENGENHARIA
FOCADA NA
EXECUÇÃO**



**METODOLOGIA
DE GESTÃO
DE PROJETO**



**TIME PRÓPRIO
DEDICADO**

Nossos números globais

+ 115 ANOS
de história.

+ 10.000 CLIENTES
que nos confiaram seus projetos.

+ 1.5 BILHÃO DE EUROS
em negócios por ano.

+ 12.500 COLABORADORES
a serviço dos clientes.

SEGURANÇA CIBERNÉTICA

OPERAÇÃO DE SISTEMA INTERLIGADO NACIONAL

Estabelece os controles de segurança cibernética a serem implementados no Ambiente Regulado Cibernético (ARCiber).

O novo ambiente regulado tem Impacto nas transmissoras e geradoras:

- Instalações da Rede de Operação;
- Centros de Operação dos agentes;
- Instalações da Rede de Supervisão diretamente conectadas ao ONS.

Conheça os requisitos mínimos e ações a serem executadas.

ETAPAS DA CERTIFICAÇÃO DE REDES:

Arquitetura tecnológica para o Ambiente.

- Segregação em zonas e conduites. IEC 62443 / NERC CIP. Implantação de firewall, IDS/IPS nas diversas camadas da arquitetura de automação.
- Isolamento das conexões externas e internas – Elaborar políticas e controle de acesso.
- Inventário permanente.
- Monitoramento de endpoints e redes industriais do ARCiber.
- Controle de portas físicas e lógicas.
- Antimalware para sistemas de automação e controle.

Governança de segurança da informação.

- Responsável técnico pela segurança cibernética do ARCiber.
- Políticas, papéis e responsabilidades do ARCiber.

Inventário de ativos.

- Inventário dos ativos de Hardware e Software a cada 24 meses.
- Monitoramento de conformidade com configuração segura.
- Gap Analise constante em relação ao ARCiber.

Gestão de vulnerabilidades.

- Análise de vulnerabilidades dos ativos.
- Testes e cronograma de implantação de correções.
- Verificação e correção de vulnerabilidades para novos equipamentos antes da implantação.

Gestão de acessos.

- Controle de acesso baseado em senha e função.
- Segurança de senha e política de atualização.
- Trilha de auditoria de acessos.
- Duplo fator de autenticação.
- Segurança de acesso para sistemas embarcados.

Monitoramento e resposta a incidentes.

- Logs de segurança retidos por no mínimo 12 meses.
- IPS/IDS/Firewall com monitoramento 24x7x365 com resposta imediata.
- Plano de resposta a incidentes cibernéticos baseado na BIA (Análise do impacto no negócio).
- Gestão de compartilhamento com a rede integrada.

