SEGURANÇA CIBERNÉTICA

snef
Brasil

SEGURANÇA CIBERNÉTICA
PARA A OPERAÇÃO DO 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:

a. Instalações da Rede de Operação

b. Centros de Operação dos agentes

c. Instalações da Rede de Supervisão diretamente conectadas ao ONS

- **SOLUÇÕES INTEGRADAS**
- **ENGENHARIA FOCADA NA EXECUÇÃO**
- **METODOLOGIA DE GESTÃO DE PROJETO**
- **TIME PRÓPRIO DEDICADO**

bsi. ISO 9001 Gestão da Qualidade

bsi. ISO 14001 Gestão do Meio Ambiente

bsi. OHSAS 18001 Gestão da Saúde e Segurança Ocupacional

SEGURANÇA CIBERNÉTICA

Para atender os requisitos mínimos devem ser executadas as seguintes ações, que são **suportadas e executadas pela SNEF.**

1. Arquitetura tecnológica para o Ambiente

a. Segregação em zonas e conduites. IEC 62443 / NERC CIP

b. Implantação de firewall, IDS/IPS nas diversas camadas da arquitetura de automação

c. Isolamento das conexões externas e internas – Elaborar políticas e controle de acesso

d. Inventário permanente

e. Monitoramento de endpoints e redes industriais do ARCiber

f. Controle de portas físicas e lógicas

g. Anti malware para sistemas de automação e controle

2. Governança de segurança da informação

a. Responsável técnico pela segurança cibernética do ARCiber

b. Políticas, papéis e responsabilidades do ARCiber

3. Inventário de ativos

a. Inventário dos ativos de Hardware e Software a cada 24 meses

b. Monitoramento de conformidade com configuração segura

c. Gap Analise constante em relação ao ARCiber

4. Gestão de vulnerabilidades

a. Análise de vulnerabilidades dos ativos

b. Testes e cronograma de implantação de correções

c. Verificação e correção de vulnerabilidades para novos equipamentos antes da implantação

5. Gestão de acessos

a. Controle de acesso baseado em senha e função

b. Segurança de senha e política de atualização

c. Trilha de auditoria de acessos

d. Duplo fator de autenticação

e. Segurança de acesso para sistemas embarcados

6. Monitoramento e resposta a incidentes

a. Logs de segurança retidos por no mínimo 12 meses

b. IPS/IDS/Firewall com monitoramento 24x7x365 com resposta imediata

c. Plano de resposta a incidentes cibernéticos baseado na BIA (Análise do impacto no negócio)

d. Gestão de compartilhamento com a rede integrada

Ondas de implantação:

Primeira onda
18 meses

Segunda onda
27 meses

Terceira onda
36 meses

Para saber mais, entre em contato:

maxcontrol@snef.com.br | www.snef.com.br

SNEF Brasil