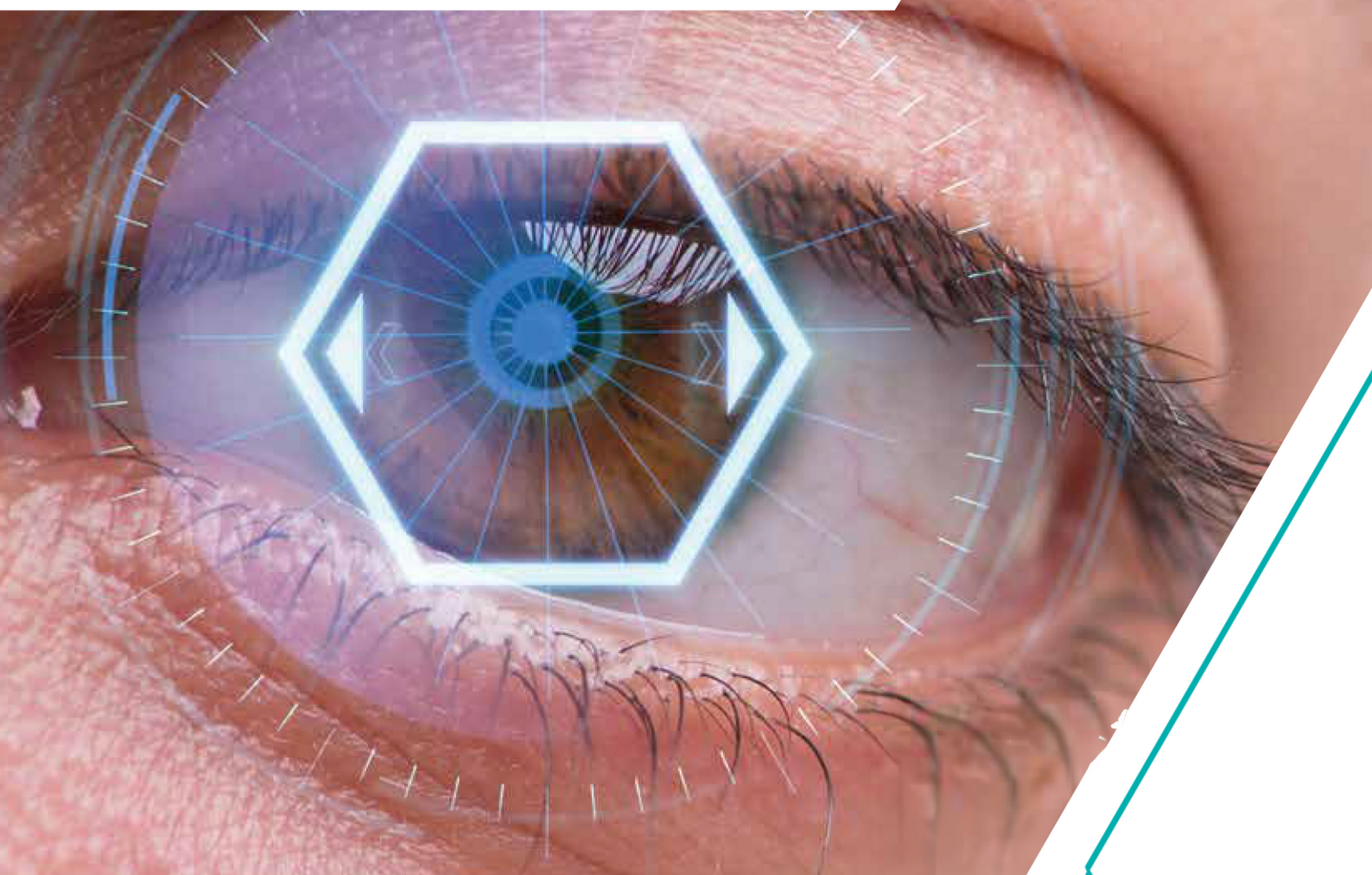


SEGURANÇA CIBERNÉTICA



SEGURANÇA CIBERNÉTICA PARA A OPERAÇÃO DO SISTEMA INTERLIGADO NACIONAL

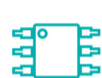
Estabelece os controles de segurança cibernética a serem implementados no Ambiente Regulado Cibernético (ARCiber).

O novo ambiente regulado tem Impacto nas transmissoras e geradoras:

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



SNEF



SOLUÇÕES INTEGRADAS



ENGENHARIA FOCADA NA EXECUÇÃO



METODOLOGIA DE GESTÃO DE PROJETO



TIME PRÓPRIO DEDICADO



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

- 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
- Anti malware para sistemas de automação e controle

2. Governança de segurança da informação

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

3. 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

4. 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

5. 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

6. 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

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