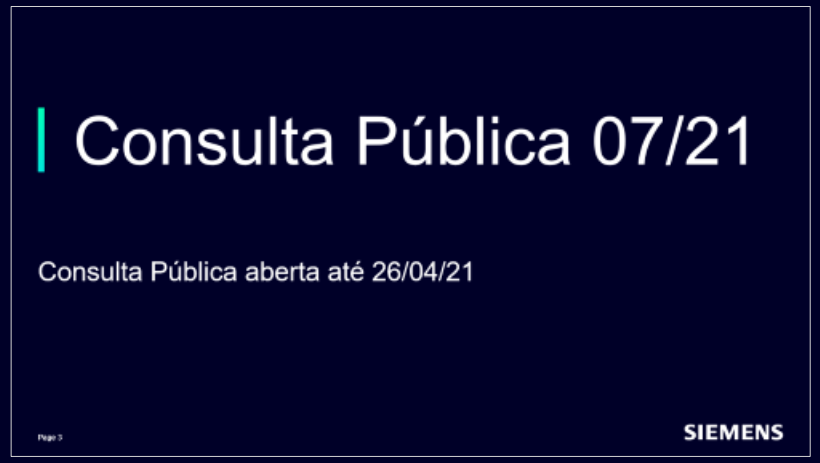
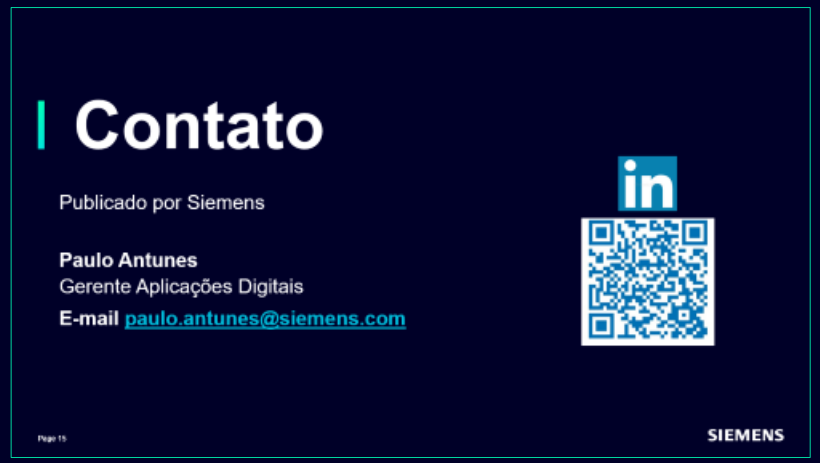
Cyber Security ANEEL CP 07/21

Obter subsídios para a Análise de Impacto Regulatório - AIR sobre a segurança cibernética no Setor Elétrico Brasileiro

SIEMENS

Tópicos da Apresentação





SIEMENS

Consulta Pública 07/21

Consulta Pública aberta até 26/04/21

SIEMENS

Consulta Pública 07/21

- **PROBLEMA**: risco de ocorrência de incidentes de segurança cibernética no setor elétrico

- Foram levantadas as soluções para os Objetivos Específicos agrupadas em Alternativas. Essas soluções foram filtradas por critérios de Razoabilidade, Proporcionalidade e Aplicabilidade resultando nas Alternativas apresentadas neste Relatório conforme lista a seguir:

    - **Alternativa 1**: não regular;
    - **Alternativa 2**: orientar e divulgar as melhores práticas para a segurança cibernética para os agentes setoriais;
    - **Alternativa 3**: regulamentar os itens da política de segurança cibernética; e
    - **Alternativa 4**: regulamentar requisitos mais prescritivos para segurança cibernética.

- **A alternativa que se sobressaiu nos dois tipos de análise foi a alternativa 3: regulamentar os itens da política de segurança cibernética.**

Consulta Pública 07/21

Alternativa 3: Regulamentar os itens da política de segurança cibernética.

97. Essa alternativa consiste em criar comandos regulatórios para estabelecer a obrigatoriedade de os agentes do setor estabelecerem suas políticas de segurança cibernética.

98. A finalidade dessa alternativa é garantir mediante *enforcement* regulatório a elaboração e implementação de políticas de segurança cibernética pelos agentes.

99. Essa alternativa será, primeiramente, implantada por meio de processo normativo padrão, para discussão com a sociedade de resolução da ANEEL. Em um segundo momento, serão elaboradas e implantadas as políticas de segurança cibernética pelas empresas e agentes, com correspondente acompanhamento da ANEEL.

100. Já para essa alternativa, as propostas de solução (na forma de possíveis ações a serem implementadas) são:

Consulta Pública 07/21

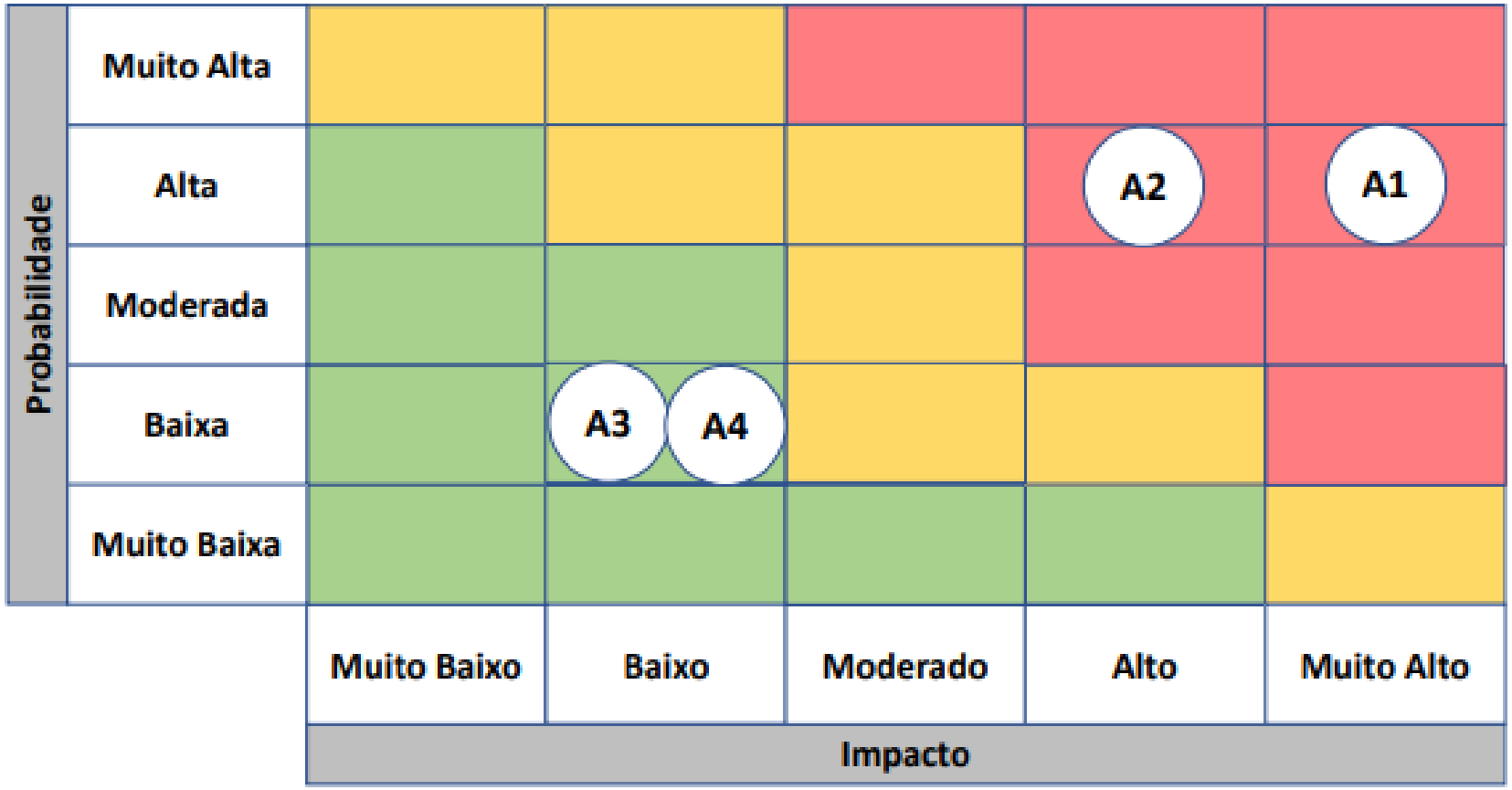


Figura 17 – Matriz de risco para o RISCO DE OCORRÊNCIA DE INCIDENTES DE SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO

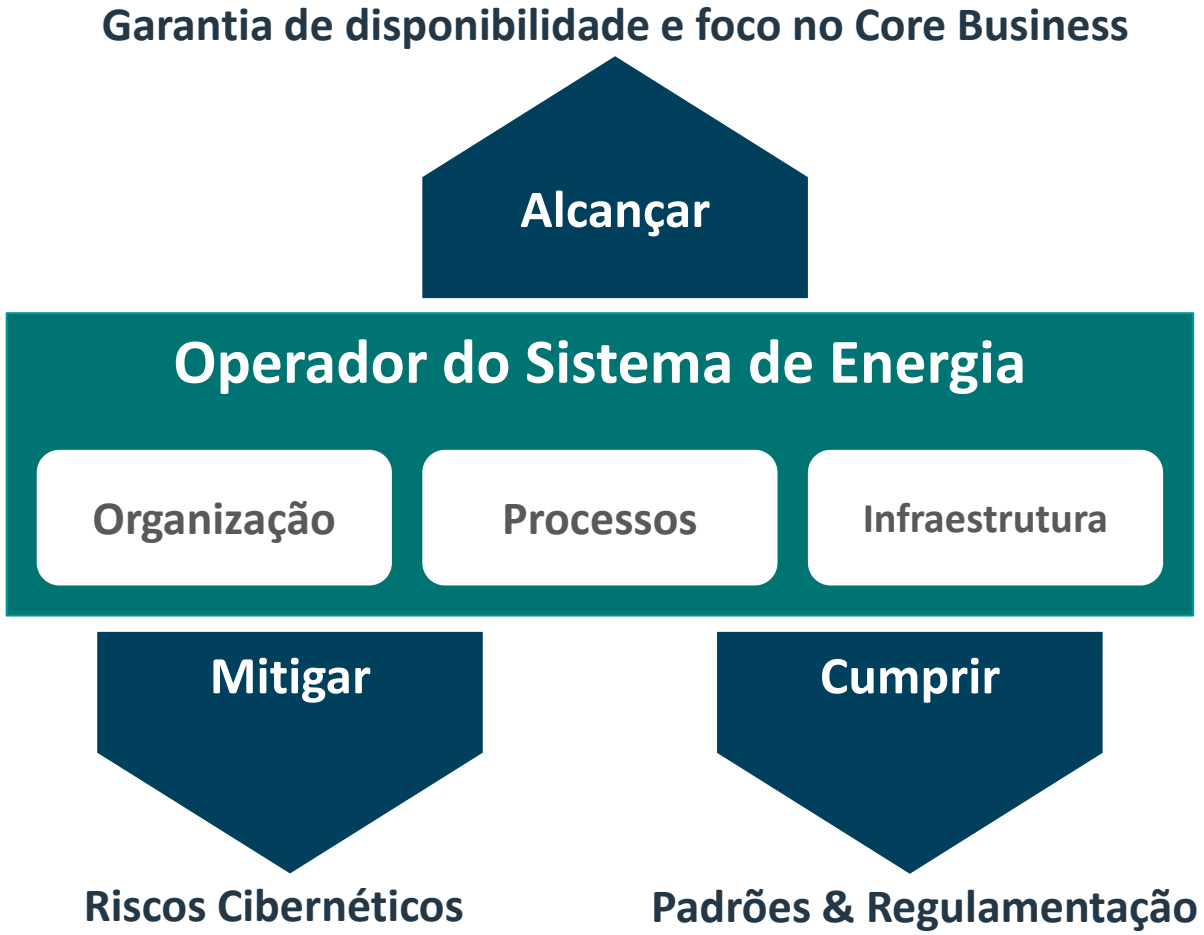
SIEMENS

Nossa Visão

Nosso entendimento sobre Cyber Security para Infraestruturas Críticas de Energia

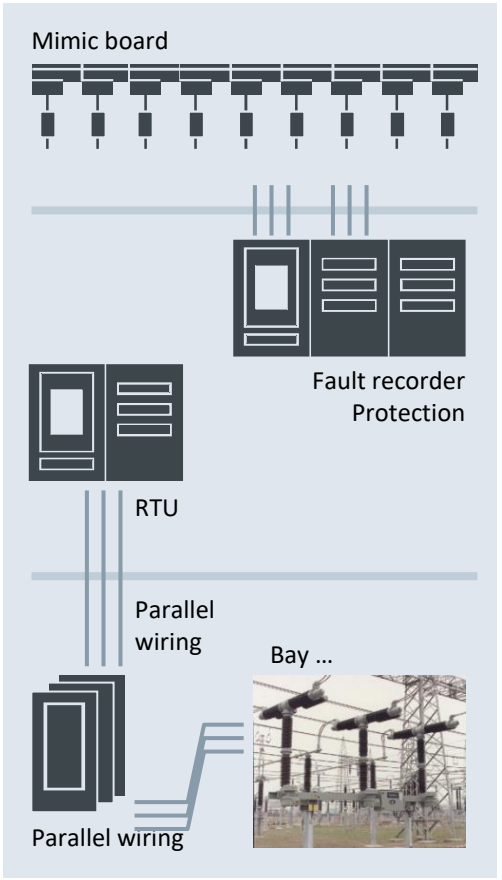
SIEMENS

Desafio e compromisso das Empresas

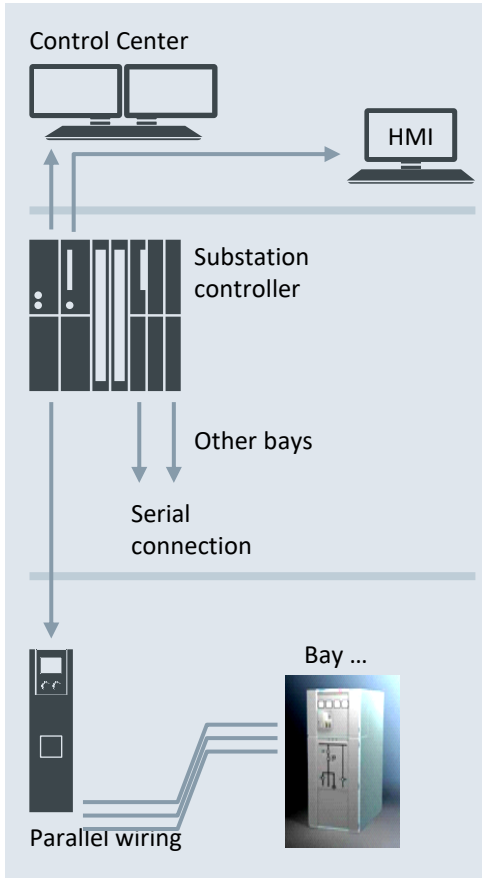


Subestação Digital 4.0
Evolução das Subestações de Energia

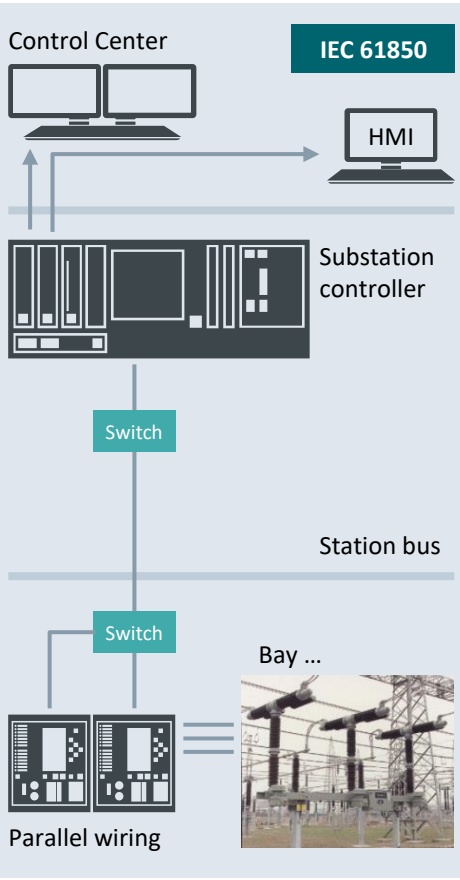
1st generation – Standard cabling



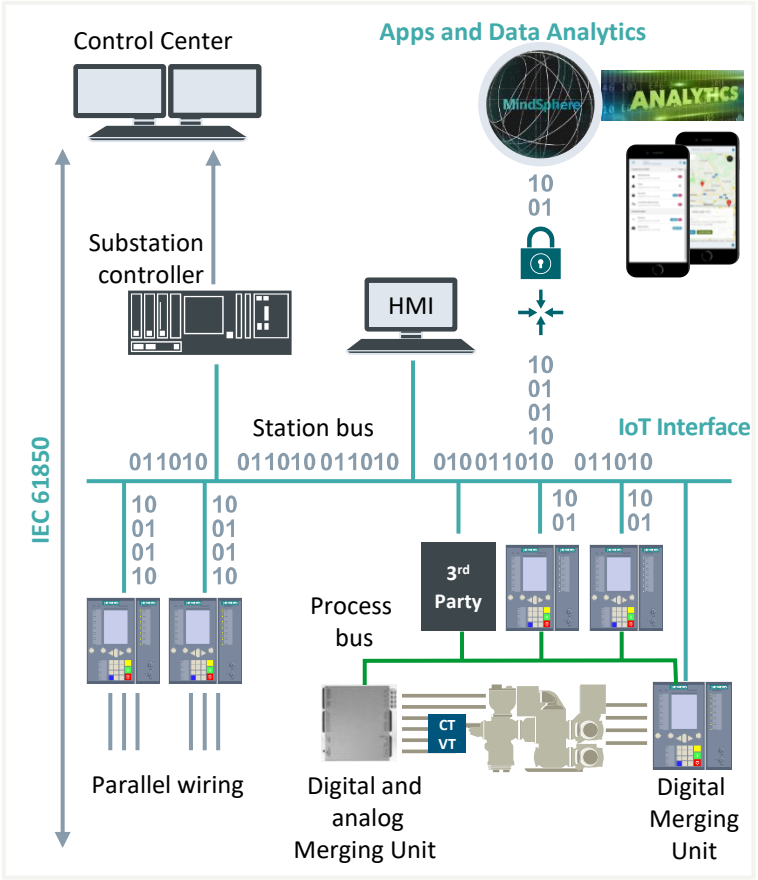
2nd generation – Point- to-point connections since 1985



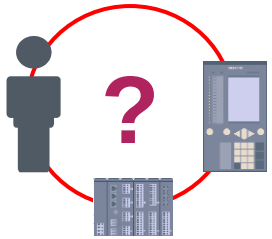
3rd generation – Digital Station bus since 2004



Digital Substation 4.0 - Process bus and IoT Connectivity

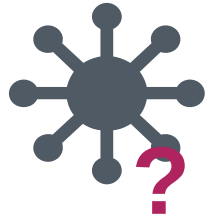


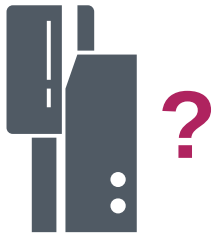
Os desafios de proteção em sistemas digitalizados



Quais são os ativos da minha rede?

Posso confiar no software e firmware do ambiente de TO?





Quem e o Quê tem acesso à TO?

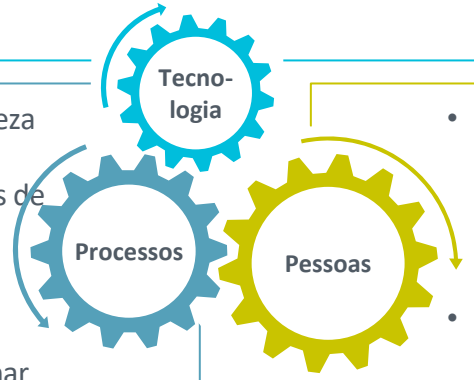
Posso depender dos dados de processo?

Posso confiar na minha rede de processos e no acesso remoto ao sistema?

Os parâmetros da minha rede de operação estão intactos e configurados corretamente?

Segurança Cibernética pede uma abordagem HOLÍSTICA!

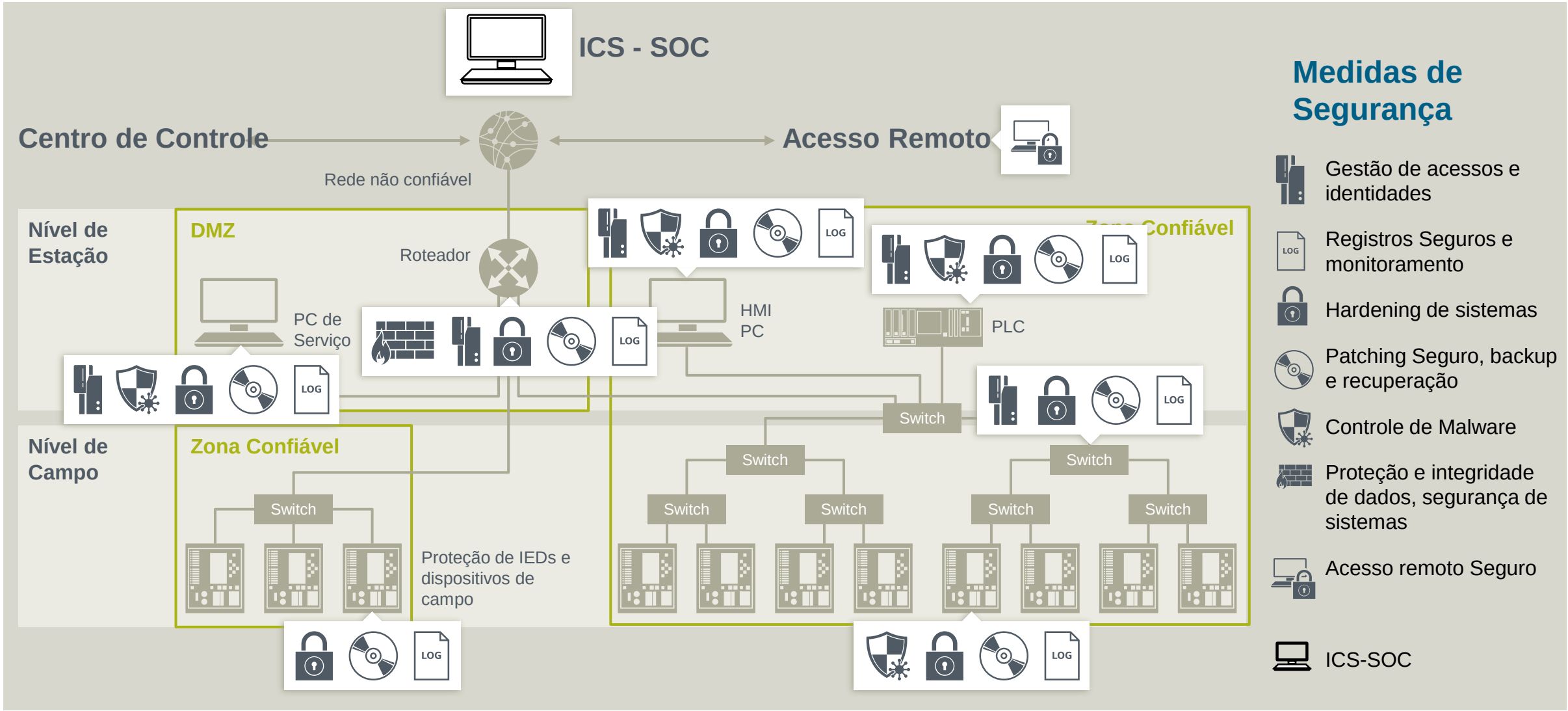
- Quais são os meus "ativos" mais importantes e em que quarto estão?
- Você precisa de diferentes zonas de segurança?
- A casa toda é segura ou apenas a porta da frente?
- Como você pode se certificar de que os moradores acessam apenas salas onde eles realmente precisam de acesso?
- Como você pode se certificar de que os quartos com "ativos" importantes não têm porta extra e/ou janelas?



- Como você pode ter certeza ter informado todos os moradores sobre as áreas de segurança e os ativos importantes?
- Todos os moradores são informados para fechar portas e janelas quando saem da casa?

- Todos os moradores sabem como agir caso uma chave seja perdida ou uma janela esteja quebrada?
- Existem regulamentos detalhados para treinar novos residentes em temas de segurança?
- Quem se certifica de que as pessoas que saem devolvem as chaves?

Arquitetura Segura - Princípio de Design - Defesa em Profundidade para TO



Nossa visão sobre a Cyber Security para o Setor Elétrico

- **A existência de uma regulamentação nacional para o setor elétrico** é base para que um país tenha infraestruturas críticas de energia menos expostas e vulneráveis, garantindo a segurança nacional e capacidade de reação em caso de incidentes;

- **Considerando o atual modelo de concessões do setor elétrico** para geração e transmissão de energia elétrica pela ANEEL, baseado no menor preço e que atenda os procedimentos de rede do ONS, o Brasil ainda está expandindo sua rede elétrica desconsiderando os requisitos de segurança cibernética. Logo, entendemos que seja criado um procedimento de requisitos mínimos de segurança cibernética no modelo prescritivo e seguidos em todos os futuros editais de contratação da Agência;

- **Atualmente existem muitas instalações de energia elétrica desprotegidas no Brasil**. Logo, apoiamos a adequação dessas instalações com base no procedimento de requisitos mínimos de segurança cibernética;

- **Avaliar, Implementar e Manter**: A Segurança Cibernética deve ser considerada como um processo de melhoria contínua ao longo do tempo, ou seja, as instalações precisam ser avaliadas, aprimoradas e mantidas conforme as características estabelecidas no procedimento de requisitos mínimos para o setor. Considerando sempre em sua aplicação os pilares das pessoas, processos e tecnologias seguras

SIEMENS

Nossa visão sobre a Cyber Security para o Setor Elétrico

- **Estamos vivendo o início da era da Internet da Energia (IoE),** que tem o potencial de agregar muito valor ao setor por meio da análise de dados em plataformas computacionais em nuvem. Por isso, a importância da segurança cibernética também para aplicações de IoE e que essa tecnologia esteja disponível para infraestruturas críticas de energia;

- **Uma vez que soluções IoE são aplicáveis a toda a cadeia produtiva do setor elétrico**, entendemos que Segurança Cibernética deve ter regulamentação aplicável às empresas que geram, transmitem e distribuem energia, reconhecendo a particularidade de cada elo da cadeia de valor do setor elétrico;

SIEMENS

Contato

Publicado por Siemens

Paulo Antunes
Gerente Aplicações Digitais
E-mail paulo.antunes@siemens.com

SIEMENS