PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

MESTRADO PROFISSIONAL EM GESTÃO DE REDES DE TELECOMUNICAÇÕES

TIAGO GERARD MACHADO

METODOLOGIA DE IDENTIFICAÇÃO DE NÍVEL DE MATURIDADE DE SEGURANÇA CIBERNÉTICA EM SMART GRID

CAMPINAS

2016

TIAGO GERARD MACHADO

METODOLOGIA DE IDENTIFICAÇÃO DE NÍVEL DE MATURIDADE DE SEGURANÇA CIBERNÉTICA EM SMART GRID

Dissertação apresentada como exigência para a obtenção do Título de Mestre em Engenharia Elétrica, ao programa de Pós-Graduação em Engenharia Elétrica, do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas.

Orientador: Prof. Dr. Alexandre de Assis Mota

TIAGO GERARD MACHADO

METODOLOGIA DE IDENTIFICAÇÃO DE NÍVEL DE MATURIDADE DE SEGURANÇA CIBERNÉTICA EM SMART GRID

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Tecnologia da Informação aplicada a Serviços em Redes de Telecomunicações.
Orientador: Prof. Dr. Alexandre de Assis Mota

Dissertação defendida e aprovada em 23 de maio de 2016 pela Comissão Examinadora constituída dos seguintes professores:

Prof. Dr. Alexandre de Assis Mota
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof.ª Dr.ª Lia Toledo Moreira Mota
Pontifícia Universidade Católica de Campinas

Prof.ª Dr.ª Marília Macorin de Azevedo
Centro Estadual de Educação Tecnológico Paula Souza

Dedico este trabalho a minha esposa Jennifer,

que sempre esteve ao meu lado em todas as

fases da minha vida. Te Amo!

Dedico este trabalho ao meu filho Matheus

que com o seu sorriso, sempre renova

minhas energias e me motiva a seguir.

Dedico aos meus pais Jorge Luiz Machado

e Dilma Gerard Machado e meu irmão

Fernando Gerard Bonavita de Almeida,

pelo carinho, amor e dedicação.

Dedico a todos os líderes e incentivadores

que passaram em minha vida.

AGRADECIMENTOS

Graças a Deus.

Ao Prof. Dr. Alexandre de Assis Mota,

Agradeço por confiar em meu trabalho e todo o direcionamento e suporte durante toda a orientação.

À Profa. Dra. Lia Toledo Moreira Mota,

Agradeço pelo aprendizado das matérias lecionadas e pela co-orientação.

Ao Prof. Dr. Omar Carvalho Branquinho,

Agradeço pelo conhecimento compartilhado sobre gerência de redes de telecomunicações.

Ao Prof. Dr. Marcelo Abbade,

Agradeço pelo conhecimento compartilhado em redes de telecomunicações.

Ao Prof. Dr Eric Alberto de Mello Fagoto,

Agradeço pelo aprendizado para a criação e apresentação de trabalhos científicos.

Ao Prof. Dr. David Bianchini,

Agradeço pelo aprendizado em pesquisas relacionadas a gestão de TIC.

Ao Grupo CPFL Energia S.A

Agradeço pela confiança e investimento.

Nossos sonhos podem se
transformar em realidade se os desejamos
tanto a ponto de correr atrás deles.

(Walt Disney)

Se quer viver uma vida feliz,
amarre-se a uma meta, não às pessoas nem
às coisas.

(Albert Einstein)

Nas grandes batalhas da vida, o
primeiro passo para a vitória é o desejo de
vencer

(Mahatma Gandhi)

RESUMO

O setor elétrico mundial está passando por um momento revolucionário com da internet das coisas no sistema elétrico de potência, ou seja, as redes elétricas inteligentes, no Brasil este movimento ainda é embrionário, mas está ganhando força nos últimos anos impulsionado pela necessidade de eficiência operacional e o novo padrão de consumidor mais participativo.As redes elétricas são essenciais para o bem-estar físico e econômico de uma nação, desta forma, com a implantação das soluções de redes elétricas inteligentes é imprescindível que a segurança da informação seja considerada para proteger os ativos críticos. Tradicionalmente o foco da segurança cibernética sempre foi na IT, com o objetivo de proteger as informações e os sistemas de informação de acessos não autorizados, utilização, modificação ou algum tipo de ação de que comprometa a confidencialidade, integridade ou disponibilidade da informação. A segurança cibernética para smart grid requer um foco combinado de segurança da informação para os sistemas de IT, para a rede de comunicação e para os equipamentos físicos da rede elétrica.Desta maneira, a dissertação tem por objetivo desenvolver uma metodologia de classificação do nível de maturidade de segurança cibernética nas redes elétricas inteligentes. A metodologia baseia-se em dois grandes pilares, primeiro na identificação dos ativos, ameaças e impactos e o segundo na realização de uma análise e classificação do nível de maturidade de 126 requerimentos que são agrupados em 16 grupos de requerimentos, sempre aplicados em um caso de uso específico.A metodologia foi aplicada em dois casos uso de sistemas de operação de uma rede elétrica inteligente de uma grande companhia de distribuição de energia. Os resultados permitiram identificar claramente que o sistema proprietário possui 51% dos requerimentos no nível mais baixo enquanto no novo sistema 47% dos requerimentos estão no nível mais alto.

ABSTRACT

The global energy sector is going through a revolutionary moment with the internet of things in the electric power system, the smart grids in Brazil this movement is still embryonic, but is gaining momentum in recent years driven by the need for operational efficiency and the new standard more participatory consumer.Electrical networks are essential for physical and economic well-being of a nation, in this way, with the implementation of smart grid solutions is imperative that information security is considered to protect critical assets. Traditionally the focus of cybersecurity has always been in IT, in order to protect the information and unauthorized access to information systems, use, modification or some kind of action that would compromise the confidentiality, integrity or availability of information. Cybersecurity for smart grid requires a combined focus of information security for IT systems to the communications network and the physical equipment of the electric grid.Thus, the thesis aims to develop a ranking methodology level cybersecurity maturity in smart grids. The methodology is based on two pillars, the first in identifying assets, threats and impacts and the second in carrying out a assessment for the analysis and classification of the 126 requirements maturity level that are grouped into 16 groups of requirements, always applied in a specific use case.The methodology was applied in two use cases of operating systems in a smart grid of a major power distribution company. The results clearly identify the proprietary system has 51% of the requirements at the lowest level while the new system 47% of applications are at the highest level.

LISTA DE FIGURAS

LISTA DE TABELAS

Sumário

1. **INTRODUÇÃO**

Atualmente está crescente a presença de dispositivos autônomos conectados na internet, até 2020 a previsão é que teremos aproximadamente 7.6 bilhões de habitantes no planta e cerca de 50 bilhões de dispositivos conectados na rede ou 6,5 dispositivos por pessoa (The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Cisco, 2011), uma grande parte serão sensores e atuadores que funcionarão na maioria do tempo sem interação humana, daí vem o termo internet das coisas, ou do inglês *IoT (Internet of Things)*. Esses equipamentos serão utilizados principalmente para automatizar serviços de infraestrutura urbana, como: transporte, educação, serviços de utilidade pública (água, energia, gás), saúde, entre outros.

O Setor de energia com a implantação das *smart grids* é um dos que está alavancando a adoção de sensores e atuadores com a utilização de solução de medição remota de consumo, atuação remota nos medidores e sistemas de *SCADA* para controle de subestações e chaves. Esses sensores e atuadores em conjunto com uma rede de alto desempenho e os sistemas especialistas formam o tripé que sustenta o conceito de *Smart Grid* que *o NIST (National Institute of Standards and Technology)* define como um complexo sistema de sistemas, que atende às diversas necessidades de muitas partes interessadas. Dispositivos e sistemas desenvolvidos de forma independente por diversos fornecedores, operados por diferentes concessionárias e utilizados por milhões de clientes, que devem trabalhar em conjunto.

As redes elétricas são essenciais para o bem-estar físico e econômico de uma nação, desta forma, com a implantação das soluções de *smart grid* é imprescindível que a segurança seja considerada para proteger os ativos críticos. Em 2014 o setor de energia recebeu 32% dos ataques cibernéticos em serviços de infraestrutura urbana no Estados Unidos de acordo com o relatório anual do ICS-CERT (Industrial Control Systems Cyber Emergency Response Team)

Tradicionalmente o foco da *cybersecurity*sempre foi na IT, para proteger as informações e os sistemas de informação de acessos não autorizados, utilização, modificação ou algum tipo de ação de que comprometa a confidencialidade, integridade ou disponibilidade da informação. *Cybersecurity* para smart grid requer um foco combinado de segurança da informação para os sistemas de IT, para a rede de comunicação e para os equipamentos físicos da rede elétrica.

Este documento tem como objetivo prover um guia de referência para as companhias de energia elétrica do Brasil que estão em processo de implantação de uma rede elétrica inteligente. O documento indicará requerimentos de segurança cibernética baseados nos conceitos *defence in depth*.

1.1. Revisão da literatura

Este capítulo destina-se a apresentar uma breve revisão bibliográfica do estado-da-arte de processos relacionados à identificação do nível de maturidade de segurança cibernética em redes elétricas inteligentes.

A indústria da eletricidade está agora à beira de uma nova era uma época que promete, através da evolução das atuais redes elétricas para as redes elétricas inteligentes, o que proporcionam um gerenciamento de energia mais eficaz e eficiente, melhorando a confiabilidade, reduzindo custos de produção, e proporcionando uma geração de energia ambientalmente amigável.

Komininos [2], em seu artigo concentra-se em questões relacionadas com a segurança da rede inteligente e casa inteligente, apresentando algumas das ameaças existentes para o ambiente de rede inteligente casa inteligente. As ameaças detectadas são categorizadas de acordo com a específicameta de segurança definida para o ambiente doméstico smart grid / smart home, eo seu impacto sobre a segurança geral do sistema é avaliada.

Metke [3] cita que é praticamente universal que é necessário para atualizar a rede elétrica para aumentar a eficiência global do sistema e a confiabilidade. Grande parte da tecnologia atualmente em uso pela rede é ultrapassada e em muitos casos não confiável. Houveram três grandes apagões nos últimos dez anos. A atualização da rede exigirá dependência significativa de inteligência distribuída e capacidades de comunicação de banda larga, consequentemente, as capacidades de acesso e comunicação exigem a mais tecnologia de segurança comprovada. O autor concentra o estudo nas principais tecnologias de segurança para um sistema de rede inteligente, incluindo infraestruturas de chaves públicas e computação segura.

Davis [4], citou que a integração das comunicações cibernéticas e sistemas de controle para a infraestrutura de rede de energia é generalizada etem um impacto profundo sobre a operação, confiabilidade e eficiênciada rede, tecnologias cibernéticas permitem uma gestão eficiente do sistema de energia, mas eles podem conter vulnerabilidades que precisam ser gerenciadas. Em seu trabalho, ele propõe um framework para avaliar os impactos confiabilidade operacional devido a ameaças à infraestrutura. O framework éum passo importante para abordar o desafio crítico decompreensão e análise de sistemas cibernéticos complexos.

Yan [5], resume os requisitos de segurança cibernética e as possíveis vulnerabilidades de comunicações de redes inteligentes, ele faz também um levantamento das soluções atuais sobre segurança cibernética para as redes de comunicações de smart grid.

Harb [6], cita alguns episódios históricos em seu artigo; em março de 2007, Idaho National Laboratório conduziu um experimento no qual danos materiais foram causados a um gerador diesel através de uma falha de segurança no seu sistema de controle. Além disso, durante a guerra na Geórgia em 2008, ataques cibernéticos originados da Rússia indisponibilizaram a rede elétrica da Geórgia durante o avanço do exército Russo em todo o país.Em abril de 2009, o jornal The Wall Street publicou que espiões cibernéticos haviam penetrado na rede elétrica dos Estados Unidos e deixaram para trás os programas de software que poderiam ser usados para interromper o sistema. Último, mas muito significativo, em 2010, o Stuxnet, um grande malware com muitos componentes e funcionalidades, explorou quatro funcionalidades de dia zero no sistema de controle industrial da Siemens. Por isso, é de extrema importância abordar o aspecto de segurança cibernética nas redes elétricas inteligentes.

Mo [7], discute a segurança em redes inteligentes sob o aspecto de que as metodologias e melhores práticas de segurança atualmente adotadas não são aplicáveis, não são viáveis, incompatíveis e inadequadas para os ambientes complexos da smart grid. Também comenta que o smart grid vai chegar a cada casa e construção, facilitando o acesso a potenciais atacantes a alguns componentes da rede. Embora a tecnologia de informações que inclua sistemas e redes (TI), o smart grid será exposto a uma ampla gama de ameaças de segurança. Por conta de sua abrangência também mais complexo garantir a segurança para cada subsistema. Além disso, a rede inteligente será não só grande mas também muito complexa, ela conectará sistemas

diferentes e redes, instalações de distribuição e equipamentos de geração com os pontos inteligentes de campo.

Hahn [8] agrupa oito pesquisas relacionadas a segurança cibernética de ambientes complexos e suas características, divididos em: pesquisa de vulnerabilidades, análise de impactos, avaliações de mitigação, desenvolvimento de métricas, validação de segurança, desenvolvimento de modelo de dados, interoperabilidade, segurança forense e treinamento.

Após este levantamento bibliográfico não foi encontrado um estudo com o foco na criação de uma metodologia de segurança cibernética específica para redes elétricas inteligentes.

1.2. Objetivos

O objetivo desta pesquisa é propor uma metodologia de identificação do nível de maturidade de segurança cibernética em soluções utilizadas nas redes elétricas inteligentes, o trabalho foi estruturado em 16 grupos de requerimentos de segurança cibernética para smart grid já mapeados no Guia de Segurança Cibernética do NIST que concentra os temas de estratégia, arquitetura e requerimentos de alto nível de segurança cibernética em redes elétricas inteligentes. [1]

1.3. Relevância do trabalho

O setor de energia está sofrendo uma revolução com a implantação de automação e inteligência nas redes elétricas, que são as redes elétricas inteligentes. Este movimento proporcionará maior eficiência na geração, transmissão e distribuição de energia elétrica.

Para que se obtenha uma rede elétrica inteligente é necessário que sejam implantados equipamentos inteligentes em campo, uma rede de comunicação de alta capacidade e resiliência e sistemas especializados e integrados. Desta maneira, a rede elétrica que é uma infraestrutura crítica para o país estará online e suscetível às ameaças presentes na internet, assim, sendo muito necessário a adoção de segurança cibernética nas redes elétricas inteligentes.

1.4. Estrutura do trabalho

O trabalho está dividido em sete capítulos que são relevantes para embasar o estudo e a sugestão da metodologia.

O capítulo 1 apresenta uma introdução breve de internet das coisas, redes elétricas inteligentes e segurança cibernética em redes elétricas inteligentes.

O capítulo 2 define o sistema elétrico de potência e seus três principais pilares geração, transmissão e distribuição de energia.

O capítulo 3 apresenta uma definição de internet das coisas e redes elétricas inteligentes.

O capítulo 4 trata especificamente de segurança cibernética e seus pilares de confidencialidade, integridade e disponibilidade, além da segurança cibernética para as redes elétricas inteligentes.

O capítulo 5 consolida todos os requerimentos de segurança cibernética de redes inteligentes e os agrupa em 16 grupos.

O capítulo 6 descreve a metodologia de identificação do nível de maturidade de redes elétricas inteligentes e consolida os resultados de dois casos de uso utilizados para homologar a metodologia.

Ao final estão as conclusões obtidas através da pesquisa, sugestões de trabalho futuros, referências bibliográficas e os anexos.

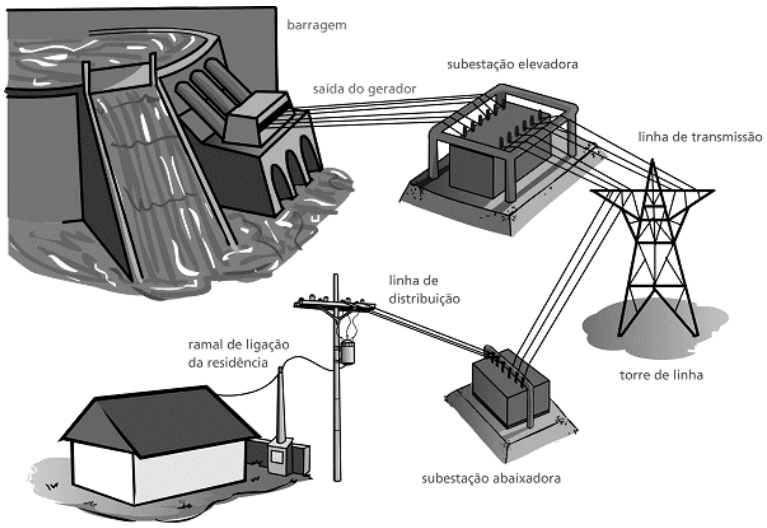
2. SISTEMA ELÉTRICO DE POTÊNCIA (SEP)

Os SEPs é um grande sistema interligado que engloba geração, transmissão e distribuição de energia elétrica que deve atender aos requisitos seguintes:

- Continuidade no fornecimento de energia aos consumidores;
- Conformidade para atendimento aos padrões estabelecidos pelosórgãos reguladores;
- Flexibilidade para que se adapte as contínuas mudanças de topologia;
- Segurança de maneira que não proporcione risco aos consumidores;
- Manutenção preventiva e corretiva para o fornecimento seja reestabelecido após uma pane.

Os sistemas elétricos, representado na figura 1, são subdivididos em três grandes blocos, geração, transmissão e distribuição.

Figura 1- Sistema Elétrico de Potência - http://mundoeletrica.com.br



2.1. Geração

É responsável pela produção da energia elétrica, obtidas através de recursos naturais. No ano de 2014 a geração de energia elétrica mundial ficou próxima a 23.800 TWh divididos em 66% termoelétrica, 11% de nuclear, 16% hidráulica e 4% eólica e solar juntas e 3% de outras fontes. No mesmo ano no Brasil a produção de energia atingiu o montante de 133,9 GW com 66,6% hidráulica, 28,3% termoelétrica,3,6% de eólica e 1,5 Nuclear, conforme ilustrado nas figuras 2 e 3.

Figura 2 - Matriz de Geração e Energia Elétrica Mundial

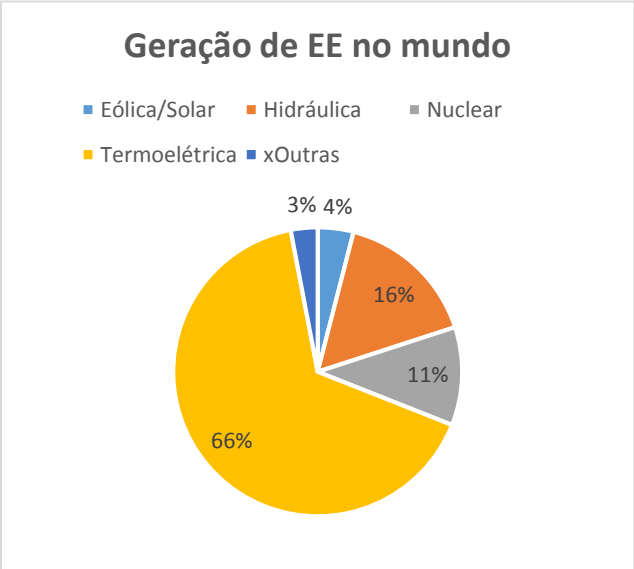
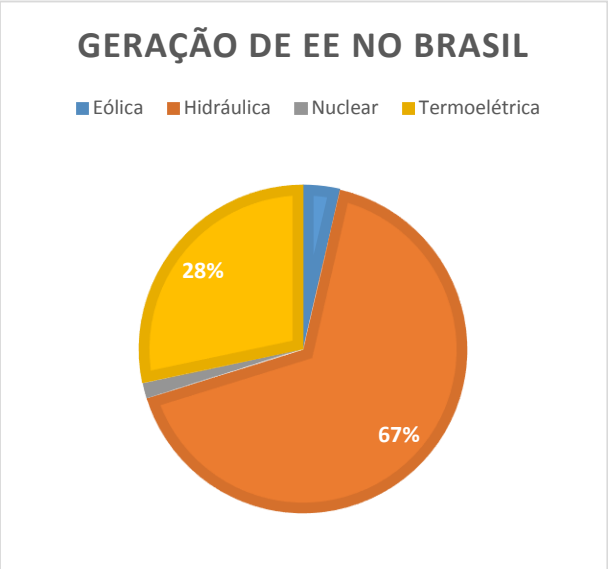
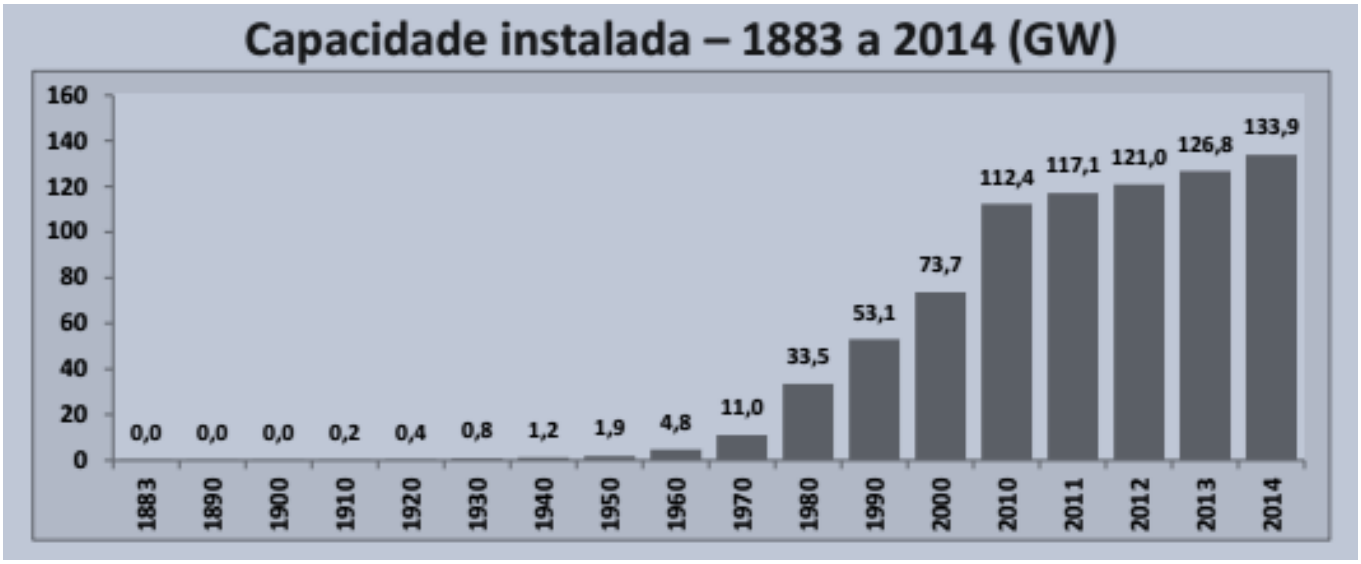


Figura 3 - Matriz de Geração de Energia Elétrica Brasileira



Conforme apresentado na figura 4, de 1970 a 2014, o Brasil passou de 11 GWh de capacidade a 133,9 GWh, com uma taxa de crescimento de 5,8% a.a. A participação da hidráulica sempre foi maior, variando de 87,4% em 1996 (máxima) a **67% em 2014 (mínima)**. A geração nuclear iniciou em 1985 e a eólica em 1992.

ura 4 - Evolução da Geração de Energia no Brasil – Fonte: ONS



Autoprodução de Energia Elétrica

Entende-se por autoprodução de E.E. a geração de eletricidade dos consumidos com instalações próprias de geração de energia elétrica, localizadas junto às unidades de consumo e que não utiliza a rede elétrica da concessionária de transmissão/distribuição, com isso, não necessita de investimentos adicionais no sistema elétrico. Este tipo de produção já representa 10% de toda energia consumida no Brasil. Prevê-se um expressivo crescimento da autoprodução até 2020, em torno de 7% ao ano em média, após o crescimento será em taxas mais baixas, aproximadamente 2,6% a.a., como demonstrado na figura seguinte.

Geração Distribuída de Energia Elétrica

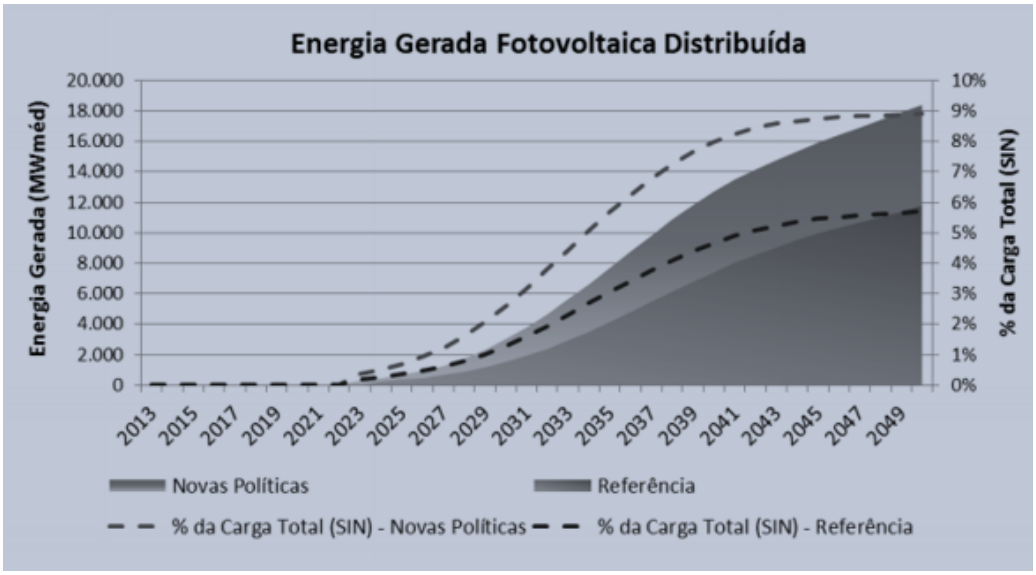
Segundo o site oficial da ANEEL,Desde 17 de abril de 2012, quando entrou em vigor a Resolução Normativa ANEEL nº 482/2012, o consumidor brasileiro pode gerar sua própria energia elétrica a partir de fontes renováveis ou cogeração qualificada e inclusive fornecer o excedente para a rede de distribuição de sua localidade. Conforme disposto na segunda edição do regulamento de Micro e Minigeração distribuída da ANELL, a micro e a minigeração distribuída consistem na produção de energia elétrica a partir de pequenas centrais geradoras que utilizam fontes renováveis de energia elétrica ou cogeração qualificada, conectadas à rede de distribuição por meio de instalações de unidades consumidoras. Para efeitos de diferenciação, a microgeração

distribuída refere-se a uma central geradora de energia elétrica, com potência instalada menor ou igual a 75 quilowatts (kW), enquanto que a minigeração distribuída diz respeito às centrais geradoras com potência instalada superior a 75 kW e menor ou igual a 3 megawatt (MW), para a fonte hídrica, ou 5 MW para as demais fontes. Os tipos da fonte de energia são painéis solares, turbinas eólicas, geradores a biomassa, etc.

A introdução da geração distribuída no planejamento energético de longo prazo é imprescindível, devido ao crescimento da demanda de energia e limitações ambientais e financeiras para o investimento em geração de energia centralizada.

Em especial, a maioria da capacidade instalada fotovoltaica mundial foi instalada em sistemas isolados. Na figura 5 é apresentado que no Brasil estima-se queaté 2050 seja gerado 18GW 9% da demanda total por placas fotovoltaicas.

Figura 5 - Evolução da Geração Fotovoltaica Distribuída – Fonte: ONS



2.2. Transmissão

São linhas constituídas por fios condutores suspensos em torres que possuem o objetivo de transportara energia elétrica dos centros de geração aos centros de consumo, conectando diretamente os consumidores de alta tensão e as empresas distribuidores que são encarregadas de transportar a energia aos consumidores de menor porte.

No Brasil, as linhas são classificadas de acordo com o nível de tensão:

A1 – Tensão igual ou superior a 230kV

A2 – Tensão de fornecimento de 88kV a 138 kV

A3 – Tensão de 69 kV

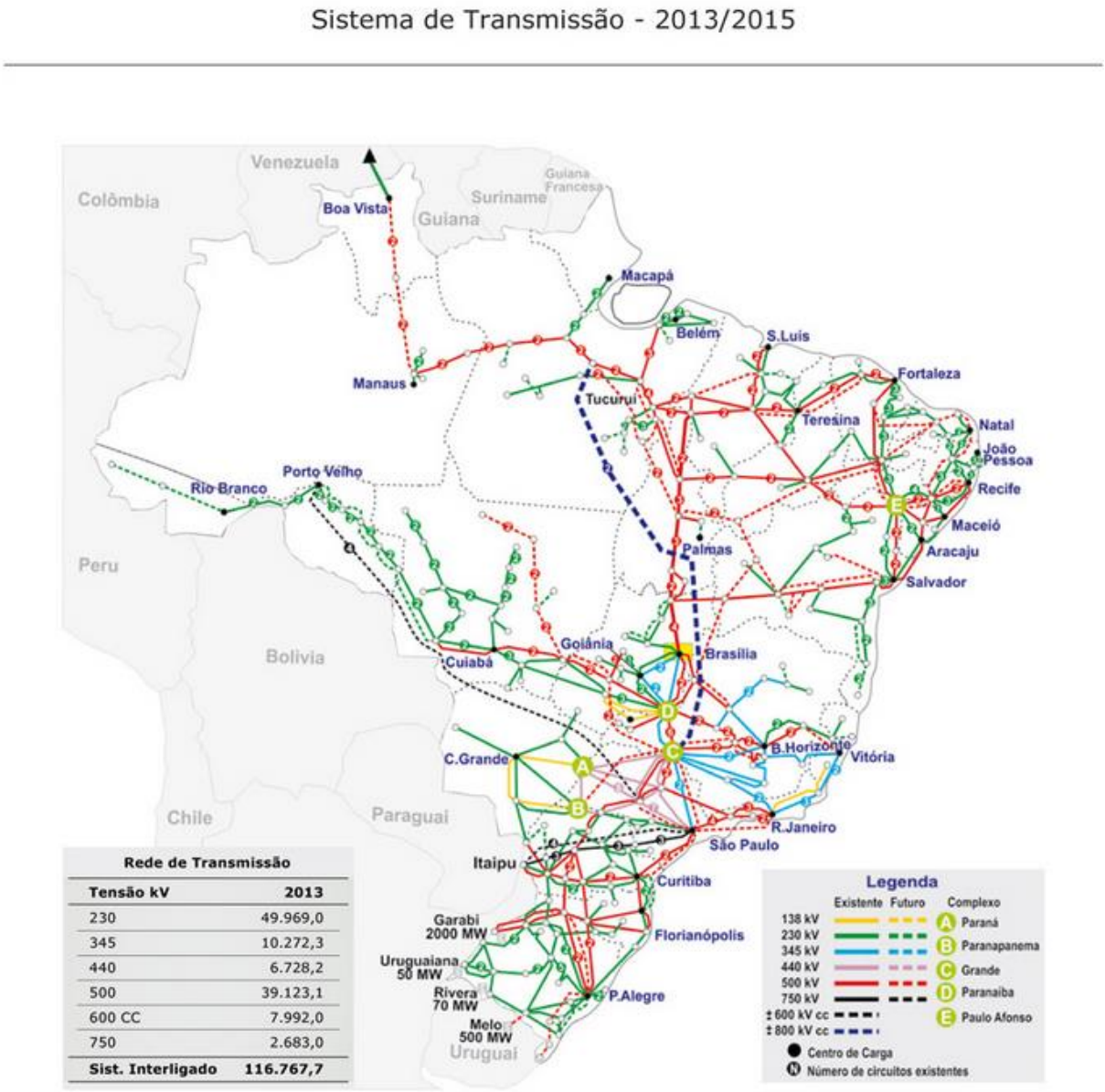
As classes A2 e A3, quando operadas por concessionárias de distribuição, são denominadas rede de subtransmissão.

Como ilustrado na figura 6, a extensão total das redes de transmissão brasileiras é de 116.767,7 Km, divididas em 49.969 Km de 230 kV, 10.272,3 de 345 kV, 6.728,2 e 40 kV, 39.123,1 Km de 500 kV, 7.992 de 600 kV e 2.683 Km de 750 kV.

Uma matéria publicada na power-technology cita a linha de transmissão do Rio Madeira no Brasil como a maior do mundo com 2.385km. (PowerTechnology, 2014)

“The Rio Madeira transmission link in Brazil, with an overhead length of 2,385km, is the world's longest power transmission line. The 600kV high-voltage direct current (HVDC) bipolar line was brought into commercial operation in November 2013 and is capable of transmitting 7.1GW of power”

Figura 6 - Sistema de Transmissão Brasileiro – Fonte: ONS



2.3. Distribuição

Realiza a distribuição da energia elétrica do sistema de transmissão até os consumidores finais.

No Brasil existem 63 concessionárias de energia, além de um conjunto de permissionárias que administram 465.823.183 unidades consumidoras de energia que são responsáveis por uma demanda de consumo de energia de 463.335 GWh divididos em 51% na região sudeste, 20% na região sul, 16% no nordeste, 8% no centro-oeste e somente 5% na região norte, como representado na figura 4

Figura 7 - Consumo de Energia por Região – Fonte: Aneel

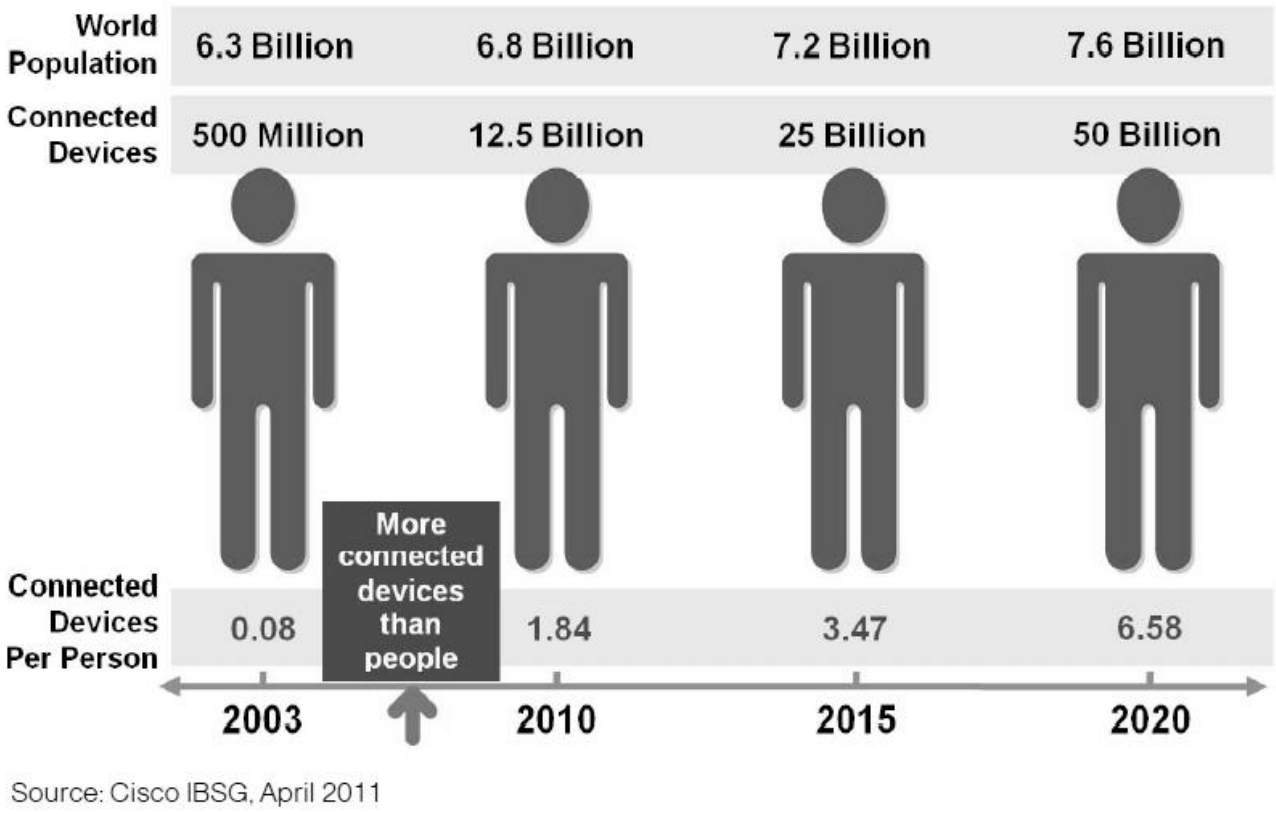
3. REDES ELÉTRICAS INTELIGENTES (SMART GRID)

A IoT refere-se a internet dos objetos e é uma nova evolução da internet que irá mudar drasticamente os negócios e a comunicação e interação da humanidade. Estes objetos se comunicam entre si e enviam as informações para os centros de dados através de uma rede de alta resiliência a capacidade para que sejam tratados e analisados por sistemas e analistas especializados.

Uma outra definição que está presente nos dias de hoje, é a internet de todos as coisas ou internet of every things – IoE que é a conexão entre pessoas, objetos e dados que utilizam processos bem estruturados para estruturar a comunicação.

Na figura 8 é apresentado que em 2010 houve uma explosão de dispositivos conectados na rede ocasionada principalmente pelos smartphones e tablets chegando a cerca de 12.5 bilhões de equipamentos conectados, enquanto isso a população mundial era de 6.8 bilhões de habitantes, ou seja, quase dois equipamentos por pessoa. No final ano de 2015 a expectativa é de 25 bilhões de e até 2020 a previsão que chegue até 50 bilhões chegando a 6.5 equipamentos por pessoa.

Figura 8 - Crescimento de Dispositivos Conectados



Os serviços urbanos serão diretamente beneficiados pela IoT, com a implantação de sensores de atuadores nos setores de utilizada pública (energia, água, gás), transporte, educação, saúde, segurança pública, governo, planejamento governamental e Edificações sustentáveis e com isso ter-se uma cidade inteligente ou smart city.

3.1. Definições de smart grid

A International Energy Agency, definie smart grid como uma rede elétrica que utiliza tecnologias avançadas digitais e outras para monitorar e gerenciar o transporte de eletricidade de todas as fontes de geração para atender aosconsumidores finais de energia variados. A smart grid, coordena as necessidade e capacidade de todos geradores, operadores de rede, consumidores finais e partes interessadas do mercado de energia, para minimizar o custo e impactos ambientais e maximizar a confiabilidade, resiliência e estabilidade do sistema.

A modernização das redes elétricas atualmente está em pauta em vários países, este esforça destina-se proporcionar um aumento da eficiência energética, confiabilidade, sustentabilidade e resiliência as redes. Um relatório do Electric Power Research Institute estima que para que os Estados Unidos operar total em uma smart grid será necessário um investimento de $500 bi em 20 amos.

Alguns benefícios da smart grid, são citados na sequência:

- Aumento da confiabilidade, segurança e eficiência energética;
- Otimização dinâmica dos recursos da rede elétrica;
- Implantação dos conceitos de demand response, demand-side resources e energy-efficency resources;
- Tecnologias de medição remota, monitoramento centralizado da rede elétrica e distribution automation;
- Integração da rede com os equipamentos inteligentes dos consumidores;
- Implantação e integração advanced electricity storage and peak-shaving Technologies, como veículos elétricos, aquecimento solar e geração solar;
- Compartilhamento de informações com o consumidor e disponibilização de opções de controle;

Segundo o framework do NIST as prioridades para implantação das funcionalidades da smart grid são:

Resposta a demanda e eficiência energética do consumidor – Demand Response and consumer energy efficiency: Que consiste em prover mecanismos e incentivos para os consumidores e as concessionárias para modificar a maneira de utilização da energia nos momentos de pico. A resposta a demanda é necessária para otimizar e balancear o suprimento de energia e a demanda. Aumentando o detalhamento das informações de consumo para os consumidores, eles poderão economizar energia.

Monitoramento da situação da rede – Wide-Area Situational Awareness (WASA): Com o objetivo de monitorar os elementos do sistema elétrico de conexão de grandes áreas geográficas em tempo real, para antecipar, prevenir ou responder a problemas antes que eles surjam.

Recursos Distribuídos de Energia – Distributed Energy Resources (DER): Geração ou armazenamento de energia que estão conectados na rede de distribuição, como dispositivos “atrás do medidor” geradores de energia locais do consumidor, veículos elétricos, baterias. Este sistema pode ser utilizado para geração de energia local e auxiliar o mercado de energia com a injeção do excedente gerado na rede de distribuição. As funcionalidades de DER avançadas possibilitam uma nova arquitetura de rede elétrica que irá incorporar as “microgrids”.

Armazenamento de Energia – Energy Storage: Atualmente o método convencional de armazenamento de energia são as represas das hidroelétricas, futuramente, o armazenamento de energia distribuído beneficiaria toda a cadeia de geração.

Meio de transportes elétricos – Eletric Transportation: Refere-se primariamente em possibilitar que veículos elétricos (electric vehicles PEVs), possam ser conectados à rede. Com isso, a emissão de gás carbônico será reduzida drasticamente.

Redes de Comunicação – Network Comunications: A variedade de redes de comunicação públicas ou privadas, cabeadas ou sem fio que serão utilizadas pelos domínios da smart grid.

Infraestrutura avançada de medição – Advanced Metering Infraestructure (AMI): Monitora próximo do tempo real o consumo de energia dos consumidores, consiste na comunicação entre hardware e software associada a um sistema de gerenciamento dos dados.

Gerenciamento da rede de distribuição – Distribution grid management: Foca em maximizar o desempeno dos transformadores, alimentadores e outros componentes de rede de distribuição.

Segurança cibernética – Cybersecurity: Destinada a garantir a confidencialidade, integridade e disponibilidade dos sistemas de informação e sistemas de controle, necessária para gerenciar, proteger e operar a smart grid, a tecnologia da informação e a infraestrutura de comunicação.

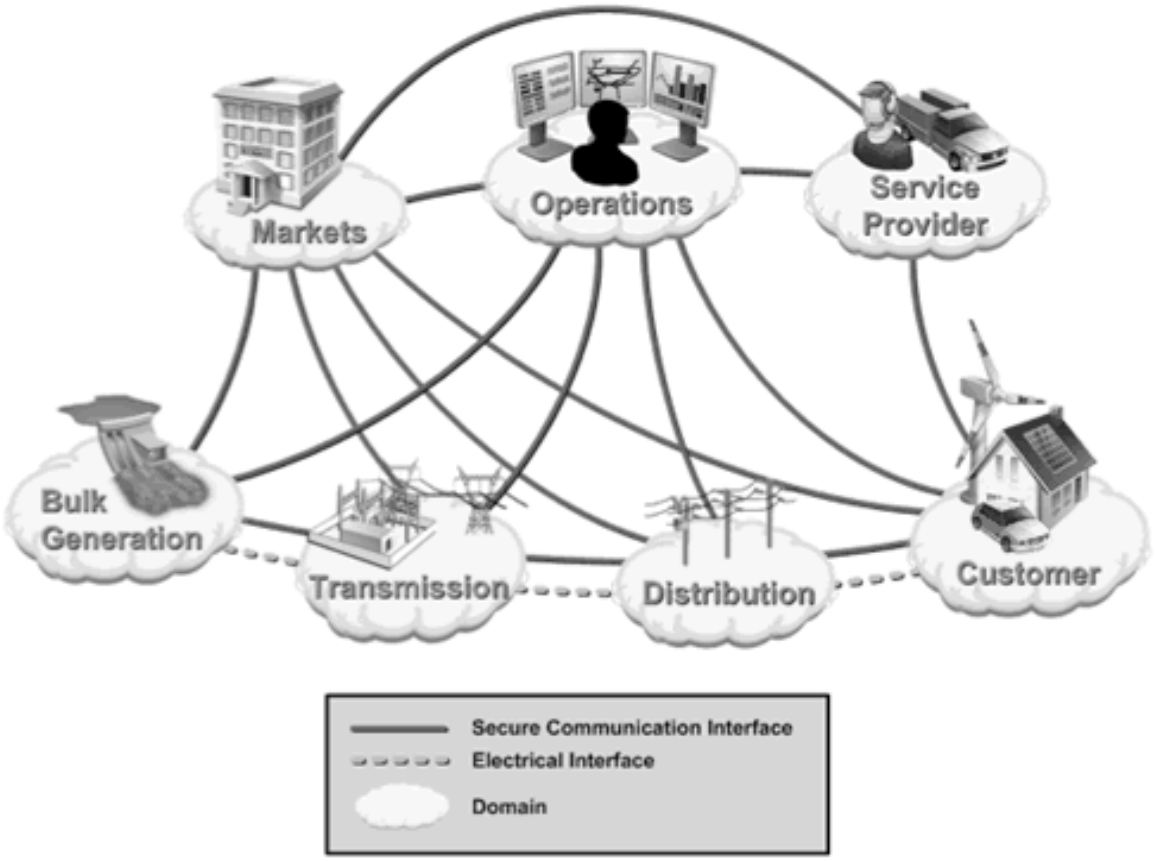
Arquitetura de Redes Inteligentes

O NIST define a arquitetura de redes inteligentes com um modelo que é composto de sete domínios listados e definidos a seguir:

- **Consumidor,** o usuário final da eletricidade, que também pode gerar, armazenar e gerenciar o uso da energia. Tradicionalmente os consumidores são definidos em três tipos: residencial, comercial e industrial;
- **Mercado,** Operadores e participantes do mercado de compra e venda de energia.
- **Provedores de Serviço,** são as organizações que prestam serviços elétricos para os consumidores e para as concessionárias;
- **Operação,** Gerenciadores do fluxo da energia em todos os níveis, desde a geração, transmissão e distribuição;
- **Geração,** Geração de energia, este domínio inclui a geração tradicional centralizada e a geração distribuída;
- **Transmissão,** responsável por transportar a energia por longas distâncias, mas também pode gerar e armazenar energia;
- **Distribuição,** Distribuidor de energia elétrica para os consumidores e geradas pelos consumidores para outros. Também pode armazenar e gerar energia elétrica.

Para habilitar a smart grid, os papéis de cada domínio devem interagir com os papéis de outros domínios, como representado na figura 9.

Figura 9 - Modelo Conceitual da Smart Grid - Fonte: NIST



3.1.1. Pilares da smart grid

Três grandes pilares sustentam de maneira macro smart grid, os equipamentos e pessoas, a rede de comunicação que pode ser privada ou terceirizada e cabeada e sem fio e os sistemas e operadores especializados para análise e tomada de decisão centralizada, representado na figura 10.

Figura 10 - Pilares do Smart Grid - Produção Própria

3.1.2. Equipamentos e pessoas

São as partes do sistema de rede elétrica inteligente que interagem diretamente com o SEP, os equipamentos podem ser: dispositivos de campo, medidores inteligentes, equipamentos do consumidor, veículos elétricos, medidores de temperatura. As pessoas são consumidores, colaboradores de manutenção de rede, manutenção de medidores, manutenção de ocorrências comerciais, etc..

3.1.3. Rede de comunicação

A smart grid é composta por muitosdiferentes tipos de redes públicas e privadas, com e sem fio. As redes incluem: uma capacidade de integração de serviço que conecta aplicações dentro de um domínio e para outros domínios e subdomíniosco m o qual compartilha informações. Elas são divididas da seguinte maneira e ilustrado na figura 11:

WAN - Wide Area Networks – WAN que conectam locais geograficamente distantes, é o backbone de comunicação.

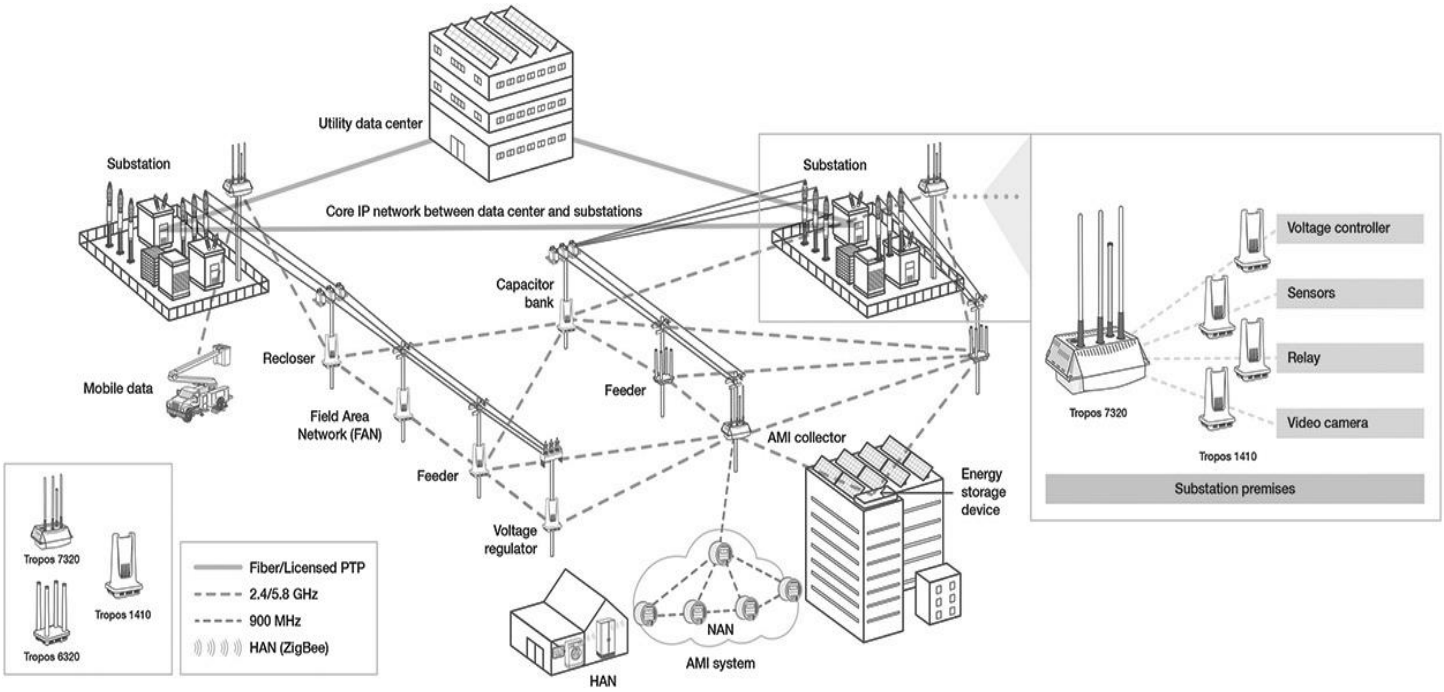
FAN - Field Area Network - FAN que conectam dispositivos como disjuntores e transformadores;

NAN - Neighborhood Area Network que conectam os medidores de energia e em alguns casos também conectam os dispositivos de campo;

HAN – Home Area Network conectam os equipamentos da residência ou do comércio do consumidor, os displays que por sua vez são conectadas a NAN através dos medidores.

Estas redes podem ser implementadas utilizando uma combinação de pública (por exemplo, a Internet) e redes privadas, em ambos os casos, exigirá implementação de segurança e controle de acesso para suportar o smart grid.

Figura 11 - Redes de comunicação Smart Grid



Dada esta variedade de ambientes de rede, a identificação de métricas de desempenho e requisitos operacionais essenciais de diferentes aplicações, atores, e domínios de além do desenvolvimento, implementação e manutenção de segurança e acesso apropriado controles é fundamental para o smart grid.

3.1.4. Sistemas

Os sistemas especializados são peças fundamentais para as redes inteligentes, eles são responsáveis por centralizar por integrar as informações geradas pelos sensores, atuadores,

clientes e colaboradores de campo e centro de operações. Na sequência, são citados e representados na figura 12 os principais sistemas que compõem a smart grid.

- AMI – Advanced Metering Infraestructure

  Trata-se de uma solução de medição avançada onde também é possível efetuar cortes e ligamentos remotos. A infraestrutura é composta dos medidores inteligentes (Smart Meters), da rede de comunicação e dos sistemas especializados, MDC – Meter Data Colection que é responsável por gerenciar a comunicação com os medidores e MDM – Meter Data Management que se comunica com o MDC e os sistemas internos da companhia.

- EMS - Energy Management System

  Solução com a funcionalidade monitoramento, controle e otimização da rede elétrica em tempo real, utilizada nos domínios de geração e transmissão. As funções de monitoramento e controle são chamadas de SCADA e os pacotes de otimização são chamados de ADVANCED APPLICATIONS.

  Possui as funcionalidades de: controle de equipamentos remotos, gestão de falta de energia, execução de análise da rede em tempo real, geração de relatórios com estatísticas da rede elétrica, cálculo e simulações na rede, treinamento de operadores, registro e gerenciamento de ativos de rede com posicionamento geoespacial.

- DMS–Distribution Management System

  Solução similar a EMS aplicada para o domínio de distribuição de energia, desenhado para o monitoramento e controle da rede de distribuição e suporte aos operadores e distribuição e operadores de campo.

- OMS – Outage Management System
  Este sistema tem como objetivo, em uma situação de falta de energia, consolidar as chamadas dos consumidores e prever a causa raiz da falta de energia, como um transformador inoperante.

- SCADA - Supervisory Control and Data Acquisition

  Sistema de comunicação remota com dispositivos de campo utilizado na distribuição, transmissão e geração para monitoramento e controle.

- GIS –Geographic Information System

  Solução que fornece gerenciamento geoespacial de ativos para apoiar o planejamento, desenho e análise da rede elétrica.

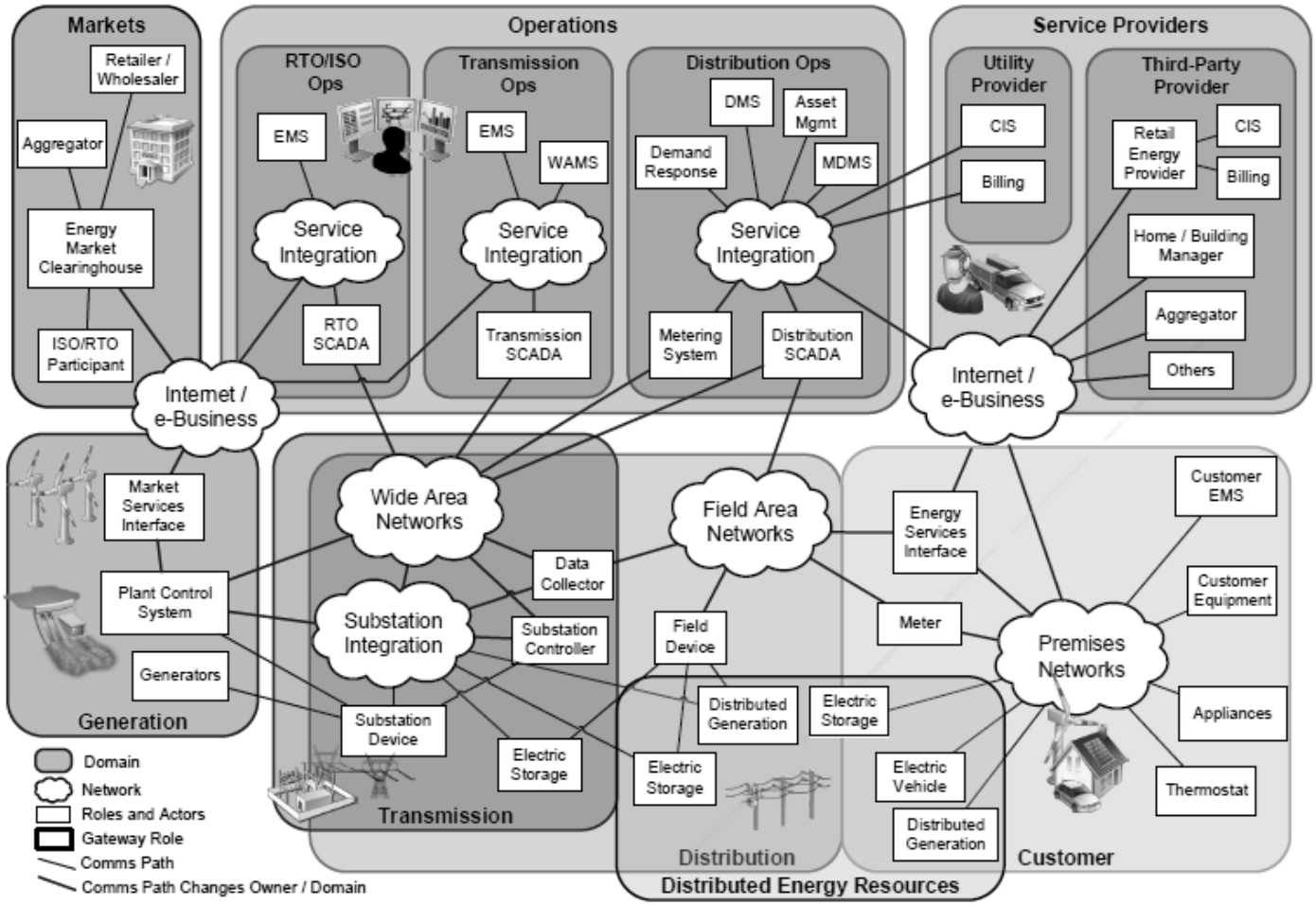
- CIS – Customer Information System

  Sistema de relacionamento com o consumidor, destinado a armazenar as informações de cadastro e gerenciar as interações.

- Billing System

  Solução responsável pelo gerenciamento e faturamento clientes residenciais, comerciais e industriais. Esse componente também permite gerir a cobrança dos clientes e a cobrança de taxas e impostos.

Figura 12 - Interligação entre domínios e sistemas. Fonte: NIST



4. SEGURANÇA CIBERNÉTICA

A segurança cibernética, tem como objetivo principal garantir a confidencialidade, integridade e disponibilidade da informação.

Confidencialidade

Garantir que somente pessoas autorizadas tenham acesso à informação e divulgação, incluindo os meios para proteger a privacidade pessoal e informações de propriedade

A perda de confidencialidade é a divulgação não autorizada de informações.

Integridade

Proteção contra modificação imprópria ou destruição de informação, e inclui a garantia de autenticidade de informações.

A perda de integridade é a modificação ou destruição de informações não autorizadas.

Disponibilidade

Garantir o acesso sempre que necessário e confiável para e uso de

A perda de disponibilidade é a impossibilidade de acesso ou uso de informações ou um sistema de informação.

4.1. Segurança cibernética no setor elétrico

Tecnologias de smart grid introduzirão milhões de novos componentes para a rede elétrica, muitos destes componentes serão fundamentais para a interoperabilidade e a confiabilidade, eles se comunicarão de forma bidirecional, e serão encarregados de manter a confidencialidade, integridade e disponibilidade vitais para a operação de sistemas de energia.

Segurança Cibernética para o smart grid suporta tanto a confiabilidade da rede elétrica quanto a confidencialidade (e privacidade) da informação que é transmitida.

Reconhecendo que a segurança nacional e econômica de um país depende da funcionalidade confiável de infraestruturas críticas. Desta forma, é necessário que se tenha uma abordagem estruturada de Segurança Cibernética para ajudar os proprietários e operadores de infraestruturas críticas para gerenciar riscos relacionados com a segurança cibernética ao mesmo tempo proteger a confidencialidade dos negócios, a privacidade individual e as liberdades civis.

Tradicionalmente, a segurança cibernética para a TI se concentra na proteção necessária para assegurar a confidencialidade, integridade e disponibilidade dos sistemas de comunicação de informações eletrônicas. Quando se trata de smart grid, segurança cibernética precisa ser adequadamente aplicada ao sistema de comunicação de TI combinada com o sistema de potência e os domínios para manter a confiabilidade da rede elétrica inteligente e privacidade de informação do consumidor.

A Ciber-segurança na rede elétrica inteligente deve incluir um equilíbrio entre sistema cibernético e processos em TI e operações e governança do sistema elétrico. Além disso, a segurança ea fiabilidade são de suma importância em sistemas elétricos de potência, todas as medidas de segurança cibernética nesses sistemas não devem impedir, as operações do sistema de energia.

Durante décadas, a operação do sistema de energia tem vindo a gerir a confiabilidade da rede elétrica em que a disponibilidade de energia tem sido a exigência principal, com a integridade da informação como um requisito secundário, mas cada vez mais crítica. A confidencialidade das informações dos clientes também é importante nos processos normais de cobrança de receitas e de preocupações com a privacidade.

Este novo cenário onde é necessário aplicar a segurança apresenta uma modalidade diferente de ataque, o Ciber-físico ataque, também chamados de ataques combinados, que causam maior impacto e / ou consequências diferentes que um cyber ou ataque físico pode causar individualmente. A fim de abordar os impactos aprimorados gerados por estes ataques combinados, os riscos e as vulnerabilidades para ambos cibernética e ataques físicos devem ser considerados.

Desta forma, é necessário que os pilares da segurança cibernética sejam garantidos para que se tenha uma smart grid segura, a seguiralguns exemplos de confidencialidade, integridade e disponibilidade aplicados ao setor de energia.

Disponibilidade é o objetivo de segurança mais importante para a confiabilidade do sistema de energia. A latência de tempo associada com a disponibilidade pode variar:

- ≤ 4 ms para relés de proteção;
- subseconds para monitoramento de área ampla consciência situacional transmissão;
- Segundos para dados da subestação e alimentador SCADA;
- Minutos para monitoramento de equipamentos não-crítica e algumas informações sobre preços de mercado;
- Horas / dias para a leitura do medidor e informações sobre preços de mercado a longo prazo; e
- dias / semanas / meses de coleta de dados de longo prazo tais como informações de qualidade de energia.

Integridade para operações do sistema de energia inclui garantia de que:

- Os dados não foram modificado sem autorização;
- Fonte de dados é autêntica;
- Carimbo de tempo associado com os dados é conhecido e autenticado; e
- Qualidade dos dados é conhecida e autenticada.

A confidencialidade é o mínimo crítico para a confiabilidade do sistema de energia. No entanto, a confidencialidade está se tornando mais importante, particularmente com a crescente disponibilidade de informações do cliente on-line

- Privacidade das informações dos clientes;
- Informações sobre o mercado eléctrico; e
- Informações corporativas gerais, tais como folha de pagamento, planejamento estratégico interno, etc

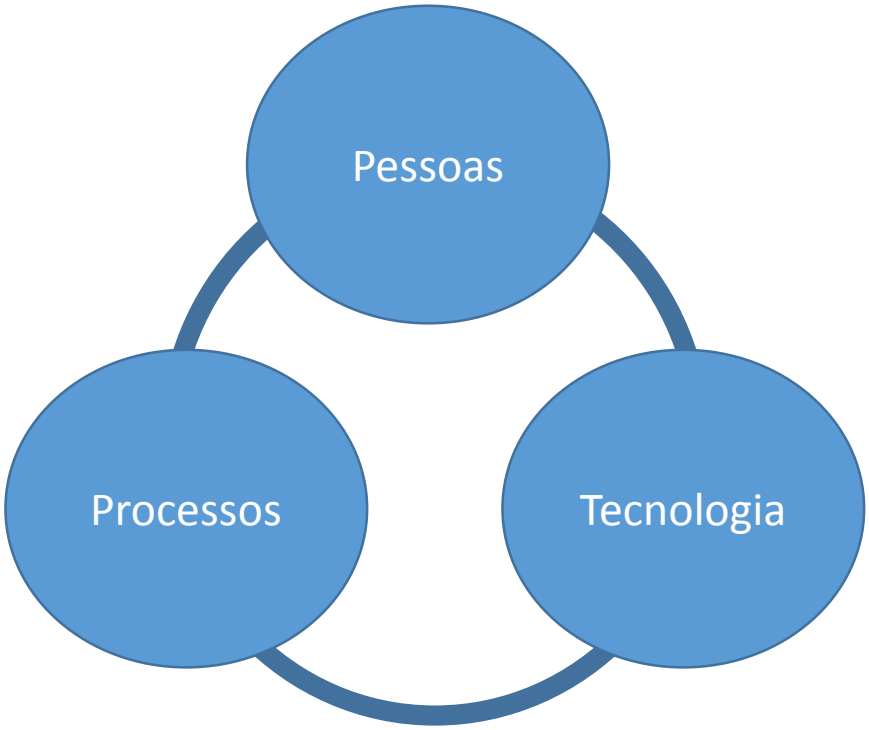
4.2. Estratégia de segurança cibernética proposta

A abordagem de defesa em profundidade (defence-in-depth) foi utilizada para guiar este trabalho em função de sua abrangência e pesquisas realizadas pelo NIST, ela concentra-se em defesa da informação (incluindo informações de clientes), ativos, sistemas de energia e comunicações e infra-estruturas de TI através de defesas em camadas (por exemplo, firewalls, sistemas de detecção de intrusão, software antivírus e de criptografia). Espera-se que múltiplos níveis de medidas de segurança sejam implementados, tanto por causa da grande variedade de métodos de

comunicação e características de desempenho, bem como, porque nenhuma medida de segurança única pode combater todos os tipos de ameaças.

A estratégia de defesa em profundidade requer uma abordagem equilibrada com foco em três elementos críticos: 1) pessoas, 2) de processo, e 3) tecnologia (veja a Figura a seguir) porque cada elemento só pode ser contornado. O objetivo de uma estratégia adequada de defesa em profundidade é fazer com que o trabalho dos atacantes fique muito mais difícil, para retardar o atacante, e permitir que a vítima possa ser alertada de atividades não autorizadas a tempo de evitar danos para a organização, como ilustrado na figura 13.

Figura 13 - Diagrama Defence-in-Depth



Devido à interligação dos sistemas de redes inteligentes, é essencial que os controles apropriados cibersegurança sejam implementados para proteger os sistemas menos críticos que infectam os sistemas mais críticos. Controles de segurança física, como portas fechadas, armários trancados, e ou áreas restritas são utilizados para mitigar o risco. Outros controles de segurança física, como circuito fechado de TV, leitores de cartão, etc., também são usados para monitorar e registrar entrada em áreas restritas.

Serviços de segurança cibernética (ou seja, as salvaguardas ou contramedidas), mecanismos e objetos devem ser aplicados em camadas, com um ou mais métodos de segurança implementados em cada camada. O principal objetivo destes métodos é mitigar o risco de um componente da estratégia de defesa a ser comprometida ou contornadas.

1. Defesa em vários lugares - Uma organização deve implantar serviços de segurança cibernética, mecanismos e objetos em vários locais para resistir a todas as abordagens de ataque.
- Serviços de Segurança - Funções que, quando fornecida em um ambiente de sistemas, servem para assegurar a proteção dos recursos, aplicando as políticas de segurança definidas da organização. Os serviços de segurança também são conhecidos como controles de segurança, requisitos e medidas defensivas.
- Mecanismos de Segurança - As ferramentas técnicas utilizadas para implementar os serviços de segurança listadas acima. Cada um dos mecanismos de segurança pode operar individualmente, ou em conjunto com os outros.
- Objetos de Segurança - Estes são itens que contêm a segurança da informação relevante sobre os usuários, grupos, privilégios, políticas, programas, senhas, chaves de criptografia, logs de auditoria, etc. objetos de segurança gerenciados descrever o que é gerido e como ele se comporta. A definição de objetos gerenciados de segurança inclui a especificação de seus atributos e seu comportamento, o que fornece uma descrição concreta do que é administrável.
O "como" da gestão é definido pelo gerenciamento de objetos constituídos de aplicativos e dados, que apoiam a gestão e utilização do resto do sistema. Este agrupamento, ou domínio de segurança, refere-se ao conjunto de entidades (objetos) de segurança que estão sob o escopo do conjunto de políticas de segurança de uma única organização.

2. defesas em camadas - Não existe tal coisa como 100% de segurança. Todas as abordagens de segurança cibernética têm vulnerabilidades inerentes. Criando a defesa em camadas (firewalls, diodos de dados, etc.) são formas de proteger contra essas vulnerabilidades.

3. Segurança robustez - componentes devem ter especificado robustez (resistência e confiabilidade) como uma função da criticidade e risco de que está protegido (isto é, o sistema SCADA, AMI, etc). Exemplos que aumentam a robustez de segurança incluem o fechamento do sistema, software antivírus, aplicação de patches, etc.

4. As relações de confiança - As relações de confiança entre os sistemas e as organizações precisam ser avaliadas, estabelecidas, e mantidas com base no risco apresentados aos sistemas, as funções que dão apoio a rede como um todo. O impacto potencial é a base para decidir sobre o tipo de conexão, os serviços de segurança selecionados, e à auditoria dos serviços de segurança do sistema anexados e processos de gestão relacionados.

5. Implantação de infraestrutura de criptografia - chave de apoio, privilégio e gerenciamento de certificado que permite a identificação positiva de entidades que utilizam tecnologias de informação e comunicação.

6. Implementação de sistemas de detecção / prevenção de intrusão - Prestação de detecção, relatórios, análise, avaliação e infraestrutura de resposta permitindo a detecção e resposta a intrusões e outros eventos anômalos rápida, e proporcionando o conhecimento da situação da rede elétrica.

7. Pessoal especializado - Um programa abrangente de educação, formação, experiência prática e consciência, é necessário. Profissionalização e licenciamento de certificação fornecem um quadro de peritos validados e reconhecidos de administradores de sistema.

8. Tipos de ameaças - As ameaças cibernéticas incluem negação de serviço, as sondas de vulnerabilidade não autorizadas, comando e controle botnet, exfiltração de dados, a destruição de dados ou até mesmo destruição física via alternância de software / dados críticos. Essas ameaças podem ser iniciadas e mantidas por uma mistura de malware, a engenharia social, ou altamente sofisticadas ameaças persistentes avançadas (Advanced Persistent Threat - APTs) que continuam por longos períodos de tempo. As ameaças cibernéticas mais sofisticadas são encobertas e não se destacam das atividades normal, e são extremamente difíceis de detectNíveis de Impacto

Tabela 1 - Nível de Impácto

	Níveis de Impacto		
	Baixo	**Moderado**	**Alto**
Confidencialidade	A divulgação não autorizada de informações poderia ser esperado para ter um efeito negativo **limitado** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A divulgação não autorizada de informações poderia ser esperado para ter um efeito negativo **sério** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A divulgação não autorizada de informações poderia ser esperado para ter um efeito **adverso grave ou catastrófico** sobre operações organizacionais, os ativos organizacionais, ou indivíduos.
Integridade	A modificação ou destruição de informação não autorizada poderia ser esperado para ter um efeito negativo **limitado** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A modificação ou destruição de informação não autorizada poderia ser esperado para ter um efeito negativo **sério** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A modificação ou destruição de informação não autorizada poderia ser esperado para ter um efeito negativo **adverso grave ou catastrófico** sobre as operações de organização, os ativos organizacionais, ou indivíduos.

Disponibilidade	A interrupção do acesso ou uso de informações ou um sistema de informação poderia ser esperado para ter um efeito negativo **limitado** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A interrupção do acesso ou uso de informações ou um sistema de informação poderia ser esperado para ter um efeito negativo **sério** sobre as operações de organização, os ativos organizacionais, ou indivíduos.	A interrupção do acesso ou uso de informações ou um sistema de informação poderia ser esperado para ter um efeito negativo **adverso grave ou catastrófico** sobre as operações de organização, os ativos organizacionais, ou indivíduos.

5. REQUERIMENTOS DE SEGURANÇA CIBERNÉTICA PARA SMART GRID

A Operação do sistema de energia apresenta muitos desafios de segurança que são diferentes da maioria das outras indústrias. Em muitos casos, equipamentos legados em sistemas de controle industrial que estão em uso nas operações do sistema de elétrico podem não ser capaz de incorporar todos os requisitos de segurança cibernética, mas precisam das proteções descritas pelos requisitos. Por exemplo, a Internet é diferente do ambiente operações do sistema de alimentação. Em particular, não são rigorosos requisitos de desempenho e confiabilidade que são necessários pelas operações do sistema elétrico. Como por exemplo:

A operação do sistema de alimentação deve continuar 24X7 com alta disponibilidade (por exemplo, 99,99% para o SCADA e maior para relés de proteção), independentemente de qualquer compromisso em matéria de segurança ou a implementação de medidas de segurança que dificultam as operações normais ou de sistema de energia de emergência.

A. A Operações do sistema de energia deve ser capaz de continuar durante qualquer ataque ou comprometimento na segurança (tanto quanto possível).
B. As operações devem se recuperar rapidamente depois de um ataque de segurança ou o compromisso de um sistema de informação.
C. Teste de medidas de segurança não pode ser permitido para impactar as operações do sistema de energia.

Não há um único conjunto de requisito de segurança cibernética que aborda cada uma das categorias de smart grid de interface lógica. Esta informação pode ser usada como diretrizes para as organizações de como elas desenvolvem sua estratégia de segurança cibernética, que devem realizar avaliações de risco, e selecionar e modificar os requisitos de segurança para implementações de sistemas de informação de rede inteligente.

Os critérios adicionais devem ser usados para determinar os requisitos de segurança cibernética antes de selecionar e implementar as medidas de segurança cibernética / soluções. Estes critérios adicionais devem ter em conta as características da interface, incluindo as restrições e as questões colocadas pelo dispositivo e da rede tecnologias, a existência de componentes /

dispositivos de legado, variando estruturas organizacionais, políticas regulatórias e legais e critérios de custo.

Os requerimentos de segurança da cibernética podem ser agrupados de em 16 Grupos de requerimentos:

CA - Controle de Acessos

CT - Conscientização e Treinamento

AR - Auditoria e Responsabilização

AA - Avaliação de Segurança e Autorização

GC - Gestão de Configuração

CO - Continuidade das Operações

IA - Identificação e Autenticação

GI - Gestão das Informações e Documentos

RI - Resposta a Incidentes

SF - Segurança Física

P - Planejamento

SP - Segurança Pessoal

GR - Gestão e Avaliação de Riscos

AS - Aquisição de Serviços

PC - Proteção da Comunicação

II - Integridade da Informação

A seguir nos itens 5.1 até 5.16 serão detalhados os grupos de requisitos.

5.1. Ca – controle de acessos

O foco do controle de acesso é garantir que os recursos sejam acessados apenas pessoas autorizadas, e garantir que estejam identificadas corretamente.

CA-1 - Política e Procedimento de Controle de Acesso

Requerimento:

A. A organização deve desenvolver, implantar, revisar e atualizar frequentemente as políticas e procedimentos de controle de acesso.
   O Documento deve conter os objetivos, papéis e responsabilidades do programa de segurança de controle de acesso no que se refere à proteção da organização e ativos; e o âmbito do programa de segurança de controle de acesso que se aplica a todos os funcionários da organização, contratados e terceiros.
   Procedimentos para abordar a implementação da política de segurança de controle de acesso e requisitos de proteção de controle de acesso associados.

B. Compromisso de gestão garante a conformidade com a política de segurança da organização e outras exigências regulamentares;
C. Assegurar que a política e os procedimentos de segurança de controle de acesso estão em conformidade com as leis federais, estaduais, tribal, e as leis e regulamentos territoriais.

CA-2 - Política e Procedimento de Acesso Remoto

Requerimentos:

A. O documento deve definir os métodos de acesso remoto aos sistemas de informação da smart grid;
B. Estabelecer restrições de uso e criar um guia para cada acesso permitido;

C. Forçar requerimentos para as conexões remotas aos sistemas de informação;
D. Liberar o acesso ao sistema somente antes das conexões;

CA-3 - Gerenciamento de contas

Requerimentos

A. Autorizar, estabelecer, ativar, modificar, desabilitar e remover as contas;
B. Definir os tipos de contas, direitos de acesso e privilégios;
C. Revisão de contas e privilégios;
D. Notificar o gerente de contas sempre que um colaborar for demitido, transferido ou tiver suas funções alteradas;
E. Ter um fluxo de aprovação antes de cada atividade.

CA-4 - Imposição de Acesso

Requerimentos

A. Configurar os sistemas para que forcem o cumprimento das regras definidas na política de controle de acessos.

CA-5 - Separação de Responsabilidades

Requerimentos

A. Estabelece e documentos para divisão de responsabilidades e separa funções necessárias para eliminar os conflitos de interesses e garantir a independência nas responsabilidades e funções das pessoas;
B. Reforça a separação das funções do sistema de informação de rede inteligente através de autorizações de acesso atribuído;
C. Restringe funções de segurança para a menor quantidade de usuários necessários para garantir a segurança do sistema de informação de smart grid.

CA-6 - Menor Privilégio

Requerimentos

A. Atribui o conjunto mais restritivo de direitos e privilégios ou acessos necessários pelos usuários para o desempenho de tarefas específicas;
B. Configura o sistema de informação da smart grid para aplicar o conjunto mais restritivo de direitos e privilégios ou acesso necessário pelos usuários.

CA-7 - Tentativas de Login

Requerimentos

A. O sistema de informação de smart grid impõe um limite de número de consecutivas tentativas de login inválidos por um usuário durante um período de tempo definido pela organização.
B. O sistema deverá bloquear o acesso após as tentativas inválidas

CA-8 - Controle Concorrente de Sessão

Requerimentos

A. Deve ser definido o número máximo de sessões concorrentes, que deve ser controlado por tipo de conta, por conta ou pela combinação das duas. O escopo deste requerimento é somente para usuários que acessam os sistemas, isso não se aplica para os acessos aos dispositivos inteligentes da rede elétrica.

CA-9 - Bloqueio de Sessão

Requerimentos

A. Para prevenir acesso indesejados, é necessário que seja definido um tempo para bloqueio automático das sessões após um período de inatividade;
B. Ao retornar as sessões os usuários devem utilizar das identificações necessárias;

CA-10 - Acesso Remoto

Requerimentos

A. A organização deve autenticar os acessos remotos e utilizar criptografia para garantir a confidencialidade da informação e integridade nas sessões remotas;
B. O sistema de informação de rede inteligente deve proteger o acesso sem fio usando autenticação e criptografia. Nota: aplica-se a autenticação do usuário, dispositivo, ou ambos, conforme necessário; e
C. A organização deve monitorar conexões remotas não autorizadas ao sistema de informação de smart grid, incluindo scanning para acessos não autorizados aos pontos de acesso wireless em uma freqüência definida pela organização e tomar as medidas adequadas se uma conexão não autorizada for descoberta.

CA-11 - Restrições de Acesso a Rede sem Fio

Requerimentos

A. Estabelecer restrições de uso e orientação de implementação para as tecnologias sem fio; e
B. Autorizar, monitor e gerenciar o acesso sem fio ao sistema de informação de smart grid.

CA-12 - Controle de Acesso para Dispositivos Móveis e Portáteis

Requerimentos

A. Estabelece restrições de uso e cria guias de utilização para dispositivos móveis controlados pela organização, incluindo o uso de mídias removíveis e mídias removíveis de propriedade pessoal;
B. Autorizar a conexão de dispositivos móveis a sistemas de informação de redes inteligentes;
C. Monitor as conexões não autorizadas de dispositivos móveis a sistemas de informação de redes inteligentes; e
D. Impõe requisitos para a conexão de dispositivos móveis a sistemas de informação de smart grid.

CA-13 - Utilização de Sistemas de Informação Externos

Requerimentos

A. Criar políticas e define padrões para a utilização de informações externas e conexão com sistemas de informações externos; e
B. Definir processos para armazenar e transmitir informações da organização utilizando um sistema de informação externa.

CA-14 - Senhas

Requerimentos

A. Desenvolver e reforçar as políticas e procedimentos para usuários do sistema de informação de redes inteligentes em matéria de geração e uso de senhas;
B. Estabelecer regras de complexidade, com base no nível de criticidade do sistema de informação de rede inteligente para ser acessado; e
C. Requer senhas sejam alteradas regularmente e ser revogada após um longo período de inatividade.

5.2. Conscientização e treinamento

CT-1 - Políticas e Procedimentos de Sensibilização e Formação

Requerimentos

A. Desenvolver, implementar, revisões e atualizações em uma frequência definida pela organização um treinamento da política de segurança de informação, que enderece:
    a. Os objetivos, funções e responsabilidades para o programa de segurança sensibilização e formação no que se refere à proteção pessoal da organização e ativos, e
    b. O âmbito do programa de segurança de sensibilização e formação que se aplica a todos os funcionários da organização, contratados e terceiros.
B. Procedimentos para abordar a implementação da política de segurança

CT-2 - Conscientização da Segurança a Informação

Requerimentos

A. Todos os procedimentos de design e sistema de informação de smart grid mudanças precisam ser revistos pela organização para inclusão no treinamento de conscientização de segurança organização; e
B. A organização inclui exercícios práticos de sensibilização para a segurança briefings que simulam ataques reais cibernéticos.

CT-3 - Treinamento de Segurança da Informação

Requerimentos

A. Executar os treinamento de segurança antes de autorizar o acesso ao sistema de informação de smart grid ou de executar tarefas atribuídas;
B. Executar sempre que exigido por mudanças no sistema de informações smart grid; e
C. Em uma frequência definida posteriormente a organização.

CT-4 - Contato com Associações e Grupos de Segurança

Requerimentos

A. É importante que a organização mantenha contato com associações e grupos de segurança da informação para estar atualizada com as últimas recomendações, práticas, técnicas e tecnologias de segurança informação e compartilhar informações sobre ameaças, vulnerabilidades e incidentes.

5.3. Auditoria e responsabilização

AR-1 - Políticas e Procedimentos de Auditoria e Responsabilidade

Requerimentos

A. Desenvolves e implementar revisões e atualizações em uma frequência definida pela organização
B. O documento de auditoria e prestação de contas deve conter:
    a. Os objetivos, funções e responsabilidades para o programa de auditoria e prestação de contas de segurança no que se refere à proteção pessoal da organização e ativos; e
    b. O escopo do programa de auditoria e prestação de contas de segurança que se aplica a todos os funcionários da organização, contratados e terceiros.
C. Procedimentos para abordar a implementação da política de segurança de auditoria e prestação de contas e requisitos associados de auditoria e prestação de contas.
D. Compromisso de Gestão segura a conformidade com a política de segurança da organização e outras exigências regulamentares; e
E. Assegurar que a política e os procedimentos de segurança de auditoria e prestação de contas estão em conformidade com as leis federais, estaduais, locais, tribal, e as leis e regulamentos territoriais.

AR-2 - Eventos Auditáveis

Requerimentos

A. Desenvolver, com base em uma avaliação de risco, a lista de eventos de sistema de informação de rede inteligente auditáveis em uma frequência definida pela organização;
B. Inclui a execução de funções privilegiadas na lista de eventos a serem auditados pelo sistema de informação de redes inteligentes; e
C. Rever a lista de eventos auditáveis com base nos dados atuais da ameaça, avaliação de risco e análise pós-incidente.

AR-3 - Conteúdo dos Registros Auditados

Requerimentos

A. Cada registro auditado deve conter:
    a. Data e hora do evento
    b. Componente do sistema de smart grid onde o evento ocorreu
    c. Tipo de evento
    d. Usuário/Identificação
    e. Resultado do evento

AR-4 - Monitoramento, Analise e Relatório de Auditoria

Requerimentos

A. Os comentários e análises de registros de auditoria de sistemas de informação de smart grid devem possuir uma freqüência definida pela organização para indicações de atividade inadequada ou incomum em relatórios descobertas para o gestor; e
B. Ajustar o nível de revisão de auditoria, análise e geração de relatórios no sistema de informação de redes inteligentes quando uma mudança no risco ocorre às operações organizacionais, os ativos organizacionais, ou indivíduos.

AR-5 - Ferramenta de Análise e Geração de Relatórios de Auditoria

Requerimentos

A. O sistema de informação da smart grid deve prover ferramentas capacitadas de análises e relatórios de auditoria.

AR-6 - Proteção das Informações de Auditoria

Requerimentos

A. As informações devem ser protegidas de acessos, modificações e exclusões não autorizadas

AR-7 - Retenção de Registros de Auditoria

Requerimentos

A. É indicado que seja definido um período de retenção dos logs de auditoria de maneira que seja garantida a investigação caso um incidente de segurança ocorra.

AR-8 - Condução de Auditorias Frequentes

Requerimentos

A. Deve conduzir processos de auditoria em uma frequência pré-estabelecida para garantir a conformidade aos requerimentos de segurança da informação, leis e regulação.

AR-9 - Qualificação do Auditor

Requerimentos

A. O auditor de segurança necessita:
    a. Entender o sistema de informação de smart grid e as práticas operacionais associadas;
    b. Entender os riscos envolvidos na auditoria; e
    c. Entender a política de segurança cibernética da organização e as políticas e procedimentos do sistema de informação da smart grid

AR-10 - Conformidade com Políticas de Segurança

Requerimentos

A. Execução de auditorias periódicas, afim de demonstrar a conformidade com as políticas de segurança, que incluem:
    a. Verificar se as políticas e procedimentos definidos em segurança cibernética, incluindo aqueles para identificar incidentes de segurança, estão sendo implementadas e seguidas;
    b. Garantir a conformidade com as políticas e procedimentos da organização;
    c. Identificar as preocupações de segurança, validar que o sistema de informação de rede inteligente está livre de compromissos de segurança, e

fornecer informações sobre a natureza e extensão dos compromissos caso eles ocorram;

d. Validar e garantir que os procedimentos de gestão de mudança produzem uma trilha de auditoria de revisões e aprovações de todas as mudanças;
e. Verificar se os mecanismos de segurança e práticas de gestão presentes durante a validação do sistema de informação de smart grid ainda estão no local e funcionamento;
f. Certificar a confiabilidade e disponibilidade do sistema de informação de rede inteligente para apoiar a operação segura.

AR-11 - Geração de registro auditáveis

Requerimentos

A. Fornecer capacidade de geração de registro de auditoria e gerar registros de auditoria para a lista selecionada de eventos auditáveis; e
B. Fornecer capacidade de geração de registro de auditoria e permitir que usuários autorizados para selecionar eventos auditáveis.

AR-12 - Não Repúdio

Requerimentos

A. O não repúdio protege os indivíduos contra alegações posteriores por um autor de não ter o autor de um documento particular, um remetente de não ter transmitido uma mensagem, um receptor de não ter recebido uma mensagem, ou responsável de não ter assinado um documento. Os serviços não repúdio são implementados utilizando diversas técnicas (por exemplo, as assinaturas digitais, recibos de mensagens digitais e madeireiras).

5.4. Avaliação de segurança e autorização

AA-1 - Avaliações de Segurança e Políticas e Procedimentos de Autorização

Requerimentos

A. Desenvolver, implantar, revisar e atualizar em uma frequência definida pela organização:
    a. A política de avaliação e autorização de segurança deve endereçar:
        i. Os objetivos, funções e responsabilidades para a avaliação da segurança e autorização do programa de segurança no que se refere à proteção pessoal da organização e ativos; e
        ii. O âmbito do programa de avaliação da segurança e autorização de segurança que se aplica a todos os funcionários da organização e terceiros contratados; e
    b. Procedimentos para tratar da realização da avaliação de segurança e de política de autorização e requisitos de avaliação da segurança e de proteção de autorização associados;
B. Compromisso de gestão garanta a conformidade com a avaliação de segurança e a autorização, política de segurança da organização e outras exigências regulamentares; e
C. Assegurar que a política e os procedimentos de segurança de avaliação de segurança e autorização cumprir a lei federal, estadual, municipal, tribal, e as leis e regulamentos territoriais.

AA-2 - Avaliação de Segurança

Requerimentos

A. Desenvolver um plano de avaliação de segurança que descreve o escopo da avaliação, incluindo
    a. Os requisitos de segurança e exigência melhorias em avaliação;

b. Os procedimentos de avaliação para ser usado para determinar requisitos de segurança eficácia; e
c. Ambiente de avaliação, a equipe de avaliação, e os papéis e responsabilidades de avaliação;

B. Avaliar os requisitos de segurança no sistema de informação de smart grid em uma frequência definida pela organização para determinar que os requisitos sejam corretamente executados, a funcionar como previsto, e produzir o resultado desejado no que diz respeito ao cumprimento dos requisitos de segurança para o sistema de informação de smart grid ;
C. Produzir um relatório de avaliação de segurança que documente os resultados da avaliação; e
D. Fornecer os resultados da avaliação de requisitos de segurança para uma autoridade administrativa.

AA-3 - Melhoria Contínua

Requerimentos

A. O programa de segurança da informação da organização deve implantar e executar práticas de contínuas para garantir que as lições aprendidas da indústria são incorporadas no sistema de informação da smart grid;

AA-4 - Conexões do Sistema de Informação da Smart Grid

Requerimentos

A. Autorizar todas as conexões do sistema de informação de smart grid para outros sistemas de informação;
B. Documentar as conexões do sistema de informações de smart grid e os requisitos de segurança associados para cada conexão; e
C. Monitorar as conexões do sistema de informações de smart grid em uma base contínua, verificando a aplicação dos requisitos de segurança documentados.

AA-5 - Monitoramento Contínuo

Requerimentos

A. A organização estabelece uma estratégia de monitoramento contínuo e implementa um programa contínuo de monitoramento que inclui:
    a. Requisitos de segurança em curso de avaliações de acordo com a estratégia de vigilância contínua organizacional; e
    b. Informar o estado de segurança do sistema de informação de rede inteligente para gerenciamento de autoridade em uma frequência definida a organização.

5.5. Gestão de configuração

GC-1 - Políticas e Procedimentos de gerenciamento de configuração

Requerimentos

A. A organização deve desenvolver, implantar, revisar e atualizar os documentos de gerenciamento de configuração em uma frequência previamente definida, e esses documento devem endereçar:
    a. Os objetivos, funções e responsabilidades para o programa de gerenciamento de configuração de segurança no que se refere à proteção pessoal da organização e ativos; e
    b. O âmbito do programa de segurança de gerenciamento de configuração como se aplica a todos os funcionários da organização, contratados e terceiros; e
    c. Procedimentos para abordar a implementação da política de segurança de gerenciamento de configuração e requisitos de proteção de gerenciamento de configuração associados;

B. Compromisso de Gestão, assegura a conformidade com a política de segurança da organização e outras exigências regulamentares; e
C. A organização deve assegurar que a política e os procedimentos de gerenciamento de configuração de segurança estão em conformidade com as leis federais, estaduais, locais, tribal, e as leis e regulamentos territoriais.

GC-2 - Linha de Base de Configuração

Requerimentos

A. A organização deve desenvolver documentos, e manter uma configuração de linha de base atual do sistema de informação de smart grid e um inventário dos componentes constituintes do sistema de informação de smart grid.

GC-3 - Controle de Alterações de Configuração

Requerimentos

A. Autorizar e documentar mudanças no sistema de informação de redes inteligentes;
B. Manter e Comentar registros de mudanças gestão de configuração para o sistema de informação de redes inteligentes;
C. Executar as atividades de Auditorias associados às alterações gestão de configuração para o sistema de informação de redes inteligentes; e
D. Testar, validar e documentar mudanças de configuração (por exemplo, patches e atualizações) antes de instalá-los no sistema de informação de smart grid operacional.

GC-4 - Monitoramento de Alteração de Configurações

Requerimentos

A. A organização deve implementar um processo para monitorar alterações no sistema de informação de redes inteligentes;

B. Antes de alterar a implementação e como parte do processo de aprovação de mudança, a organização deve analisar as mudanças no sistema de informação de smart grid para impactos potenciais de segurança; e

C. Depois que o sistema de informação de rede inteligente é alterado, a organização deve verificar os recursos de segurança para garantir que os recursos ainda estão funcionando corretamente.

GC-5 - Restrição de Acesso para Alteração de Configurações

Requerimentos

A. Definir, documentos e aprovar os privilégios de acesso individuais e impor restrições de acesso associadas a alterações na configuração do sistema de informação de redes inteligentes;
B. Gerar, manter e comentar registros que refletem todas essas mudanças;
C. Estabelecer termos e condições para a instalação de qualquer hardware, firmware ou software em dispositivos de sistema de informação de redes inteligentes; e
D. Realizar auditorias de mudanças no sistema de informação com uma frequência definida pela organização e se / quando alterações suspeitas não autorizadas tenham ocorrido.

GC-6 - Inventário de Componentes

Requerimentos

A. A organização deve desenvolver, documentar e manter um inventário de componentes que:
    a. Reflita com precisão a configuração atual sistema de informação de redes inteligentes;
    b. Fornece o nível adequado de granularidade considerada necessária para o acompanhamento e elaboração de relatórios e prestação de contas propriedade eficaz;
    c. Identifique os papéis e responsáveis pelo inventário componente;

d. Atualize o inventário de componentes do sistema, como parte integrante das instalações do componente, atualização do sistema, e as remoções; e
e. Garanta que a localização (lógico e físico) de cada componente está incluído dentro do limite do sistema de informação de smart grid.

GC-7 - Inclusão, Remoção e Eliminação dos Equipamentos

Requerimentos

A. A organização deve implementar políticas e procedimentos para tratar a inclusão, remoção e eliminação de todos os equipamentos de sistema de informação de redes inteligentes; e
B. Todos os componentes e informações do sistema de informação devem estar documentados, identificados e monitorados de modo a que a sua localização e função sejam conhecidas.

GC-8 - Plano de Gerenciamento de Configuração

Requerimentos

A. A organização deve desenvolver e implantar um plano de gerenciamento de configuração de deve endereçar os seguintes pontos:
    a. Papéis, responsabilidades e processos de gerenciamento de configuração e procedimentos;
    b. Definir os itens de configuração para o sistema de informação de redes inteligentes;
    c. Definir quando (no ciclo de vida de desenvolvimento do sistema) os itens de configuração são colocados sob gerenciamento de configuração;
    d. Definir os meios para identificar inequivocamente os itens de configuração ao longo do ciclo de vida de desenvolvimento do sistema;
    e. Definir o processo de gestão da configuração dos artigos controlados.

5.6. Continuidade das operações

CO-1 - Políticas e Procedimento de Continuidade de Operação

Requerimentos

A organização necessita desenvolver, implantar, revisar e atualizar as políticas e procedimento de continuidade de operação, em uma frequência previamente pré-definida, esses documentos devem endereçar:

A. Objetivos, funções e responsabilidades para a continuidade do programa de segurança de operações que se refere à proteção de pessoal da organização e ativos; e
B. O escopo da continuidade do programa de segurança de operações, uma vez que se aplica a todos os funcionários da organização, contratados e terceiros;
C. Procedimentos para abordar a implementação da continuidade da política de segurança e continuidade de operações associadas dos requisitos de proteção operações;
D. Compromisso de Gestão que assegure a conformidade com a política de segurança da organização e outras exigências regulamentares; e
E. A organização deve assegurar que os procedimentos de operações cumprem a lei federal, estadual, municipal, tribal, e as leis e regulamentos territoriais.

CO-2 - Plano de Continuidade da Operação

Requerimentos

A. Desenvolver e implementar um plano de continuidade das operações, lidar com a questão geral de manter ou restabelecer as operações em caso de uma interrupção indesejável para um sistema de informação de redes inteligentes;
B. O plano aborda papéis, responsabilidades atribuídas indivíduos com informações de contato e atividades associadas com a restauração operações do sistema de informações de smart grid após uma interrupção ou falha; e
C. A gestão de comentários de autoridade e aprovação do plano de continuidade de operações.

CO-3 - Papéis e Responsabilidades da Continuidade das Operações

Requerimentos

A. Definir os papéis e responsabilidades dos colaboradores e parceiros nos eventos significantes;
B. Identificar o líder e o tempo de recuperação, caso ocorra algum incidente.

CO-4 - Treinamento de Continuidade da Operação

Requerimentos

A. A organização deve treinar constantemente as partes interessadas em suas devidas funções para a continuidade de operações e oferecer cursos de reciclagem em uma frequência previamente definida.

CO-5 - Plano de teste da Continuidade da Operação

Requerimentos

A. O plano de continuidade deve ser testado e para determinar se os resultados serão efetivos em um momento real, além disso, é importante que este teste seja documentado;
B. Um executivo responsável pela operação, deve revisar os resultados do teste e executar as ações de correção caso necessário;
C. É importante que seja definida a frequência de teste do plano de continuidade da operação

CO-6 - Atualização de Plano de Continuidade da Operação

Requerimentos

A. É necessário que o plano de continuidade da operação seja constantemente revisado e atualizado sob o ponto de vista de sistema de smart grid, organizacional e tecnológico.

CO-7 - Site de Armazenamento Alternativo

Requerimentos

A. É importante que organização determine os requerimentos para um site de armazenamento alternativo
B. A organização deve identificar potenciais problemas de acessibilidade no local de armazenamento alternativo em caso de um rompimento ou desastre em toda a área e apresenta medidas explícitas de mitigação;
C. A organização deve identificar um local de armazenamento alternativo que está geograficamente separado do local de armazenamento primário para que ele não é suscetível aos mesmos perigos; e
D. A organização deve configurar o local de armazenamento alternativo para facilitar as operações de recuperação atempada e eficaz.

CO-8 - Serviço de Telecomunicações Alternativo

Requerimentos

A. A organização deve identificar serviços de telecomunicações alternativos para o sistema de informação de smart grid e iniciar os acordos necessários para permitir a retomada das operações do sistema dentro de um período de tempo definido pela organização quando os recursos do sistema de informações de smart grid primário não estão disponíveis.
B. Os contratos de serviços de telecomunicações principal e alternativo devem conter serviço prioritário de acordo com os requisitos de disponibilidade da organização;
C. Os serviços de telecomunicações alternativos não devem compartilhar um ponto único de falha com serviços de telecomunicações primárias;
D. Os prestadores de serviços de telecomunicações alternativos precisam ser suficientemente separadas de prestadores de serviços primários para que eles não sejam suscetíveis aos mesmos perigos; e
E. Prestadores de serviços de telecomunicações principal e alternativo precisam ter planos de contingência adequados.

CO-9 - Centro de Controle Alternativo

Requerimentos

A. A organização deve criar um centro de controle alternativo, e iniciar quaisquer acordos necessários para permitir a retomada das operações das funções críticas do sistema de informação para smart grid dentro de um período de tempo descrito previamente quando o centro de controle primário não está disponível. Equipamentos, telecomunicações e suprimentos necessários para retomar as operações dentro do prazo precisam estar disponíveis no centro de controle alternativo ou por um contrato em vigor para apoiar a entrega ao site;
B. O centro de controle alternativo deve estar geograficamente separado do centro de controle principal;
C. Identificar potenciais problemas de acessibilidade para o centro alternativo em caso de evento de grandes áreas de extensão;
D. O centro de controle deve possuir os serviços prioritários que devem ser definidos previamente pela organização.

5.7. Identificação e autenticação

IA-1 - Políticas e Procedimentos de Identificação e Autenticação

Requerimentos

A. A organização deve desenvolver, implementar, revisar e atualizar em uma frequência definida
B. A política de segurança de autenticação e identificação deve endereçar:
    a. Os objetivos, funções e responsabilidades de identificação e autenticação no que se refere à proteção pessoal da organização e ativos; e
    b. O âmbito de identificação e autenticação que se aplica a todos os funcionários da organização, contratados e terceiros; e

C. Procedimentos para tratar da implementação da política de identificação e segurança de autenticação e requisitos de identificação e autenticação de proteção associados;

IA-2 - Gerenciamento do Identificador

Requerimentos

A. A organização de recebe a autorização de uma entidade certificadora para atribuir uma identificação para os usuários e dispositivos;

IA-3 - Gerenciamento do Autenticador

Requerimentos

A. A organização deve gerenciar as credenciais de autenticação para usuários e dispositivos
B. Definir o conteúdo inicial autenticação de credencial, a definir de tamanho da senha e composição, os tokens;
C. Estabelecer procedimentos administrativos para a distribuição inicial de credencial; perdido, comprometida, ou danificado credenciais de autenticação; e revogar as credenciais de autenticação;
D. Alterar / atualizar credenciais de autenticação em uma frequência definida-organização; e
E. Especificar medidas para proteger as credenciais de autenticação.

IA-4 - Identificação e Autenticação do usuário

Requerimentos

A. O sistema de informação de smart grid deve identificar e autenticar os usuários de maneira única.

IA-5 - Identificação e Autenticação de Dispositivos

Requerimentos

A. O sistema de informação de smart grid deve identificar e autenticar os dispositivos de maneira única.
B. O sistema de informação de smart grid autentica dispositivos antes de estabelecer conexões de rede remota usando a autenticação bidirecional entre dispositivos utilizando criptografia; e

IA-6 - Resposta de Autenticação

Requerimentos

A. Durante o processo de autenticação, o sistema de autenticação e os usuário e dispositivos, devem fornecer respostas de para proteger as informações de possível exploração / utilização por pessoas não autorizadas.
B. O sistema de informação de smart grid obscurece o feedback de informações de autenticação durante o processo de autenticação (por exemplo, exibindo asteriscos quando um usuário digita uma senha). O feedback do sistema de informação de smart grid não fornece informações que permitiria que um usuário não autorizado a comprometer o mecanismo de autenticação.

5.8. Gestão das informações e documentos

GI-1 - Políticas e Procedimentos de Gerenciamento de Documentos e Informações

Requerimentos

A. A organização deve desenvolver, implementar, revisar e atualizar em uma frequência definida uma política de gerenciamento de documentos de informações que enderece:
    a. Os objetivos, funções e responsabilidades para o gerenciamento de documentos e informações; e
    b. O âmbito que se aplica a todos os funcionários da organização, contratados e terceiros; e

c. A recuperação de registros escritos e eletrônicos, equipamentos e outros suportes para o sistema de informação de redes inteligentes; e
d. A destruição de registros escritos e eletrônicos, equipamentos e outros suportes para o sistema de informação de redes inteligentes; e

GI-2 - Retenção de Documentos e Informações

Requerimentos

A. Desenvolver políticas e procedimentos que especifiquem a retenção de informações da organização;
B. Realizar revisões legais das políticas de retenção para garantir a conformidade com todas as leis e regulamentos aplicáveis;
C. Gerenciar os dados relacionados com o sistema de informação de smart grid, incluindo o estabelecimento de políticas e procedimentos de retenção, tanto para dados eletrônicos e de papel; e
D. Gerenciar o acesso aos dados relacionados ao sistema de informação de redes inteligentes com base em funções e responsabilidades atribuídas.

GI-3 - Manuseio da Informação

Requerimentos

A. Desenvolver e revisar frequentemente políticas e procedimentos que detalhem como manusear as informações, sob o ponto de vista de: acesso, compartilhamento, cópia, transmissão, distribuição, eliminação e destruição.

GI-4 - Troca de Informações

Requerimentos

A. Estabelecer acordos para a troca de informações, firmware e software entre a organização e as partes externas, como terceiros, fornecedores e empreiteiros.

GI-5 - Rotulagem Automatizada

Requerimentos

A. O sistema de informação de smart grid deve rotular automaticamente as informações no armazenamento, no processo e na transmissão de acordo com:
B. Requisitos de controlo de acesso;
C. Instruções de divulgação, manipulação, distribuição ou especiais; e
D. Caso contrário, conforme exigido pela grade informação política de segurança do sistema inteligente.

5.9. Resposta a incidentes

RI-1 - Políticas e Procedimentos de Resposta a Incidentes

Requerimentos

A. Desenvolver, implantar, revisar e atualizar políticas e procedimentos de resposta a incidentes que contemplem:
    a. Objetivos, papéis e responsabilidades para resposta a incidentes, para proteção das pessoas e ativos da organização;
    b. Escopo de aplicação do programa de resposta a incidentes que seja aplicado para todos os colaboradores, contratos e terceiros da organização;
B. Comitê de gestão que garanta a conformidade com as políticas de segurança da organização e requerimentos regulatórios;
C. Assegurar que as políticas e procedimentos cumprem as regulamentações federais, estaduais, locais e territoriais;

D. Identificar interrupções potenciais e classificar como causa, efeito e probabilidade

RI-2 - Papéis e Responsabilidades de Resposta a Incidentes

Requerimentos

A. Plano de segurança do sistema de informação de smart grid da organização define os papéis e responsabilidades específicas em relação a vários tipos de incidentes; e
B. O plano identifica pessoal responsável para liderar o esforço de resposta, caso ocorra um incidente. Equipes de resposta precisam ser formadas, incluindo o sistema de informações de redes inteligentes e de outros proprietários de processos, para restabelecer as operações.

RI-3 - Treinamento de Resposta a Incidentes

Requerimentos

A. Os funcionários são treinados nas suas funções de resposta a incidentes e responsabilidades no que diz respeito ao sistema de informação de smart grid e recebem atualizações em uma frequência definida pela organização.
B. A organização utiliza o sistema de informação de smart grid simulando eventos em continuidade do treinamento de operações para facilitar a resposta eficaz por pessoal em situações de crise; e
C. A organização emprega automatizado mecanismos para proporcionar um ambiente realista para treinamento no sistema.

RI-4 - Teste de Resposta a Incidentes

Requerimentos

A. A organização deve testar e exercitar a capacidade de resposta a incidentes em uma frequência previamente definida.

RI-5 - Monitoramento de Incidentes

Requerimentos

A. Rastrear e documentar os incidentes de segurança que ocorrerem nos sistemas de informação de smart grid.

RI-6 - Relatório de Incidentes

Requerimentos

A. O procedimento de relatório de incidentes deve incluir:
    a. O que é um relatório de incidentes;
    b. A granularidade da informação relatada;
    c. Quem recebe o relatório;
    d. O processo de transmissão da informação.

RI-7 - Investigação e Análise de Resposta a Incidentes

Requerimentos

A. Desenvolve e implementa políticas e procedimentos incluem um inquérito de resposta a incidentes e programa de análise;
B. Inclui investigação e análise de incidentes de sistemas de informação de smart grid no processo de planejamento; e
C. Desenvolve, testa, implanta e documenta uma investigação de incidentes e processo de análise.

RI-8 - Ações de Correção

Requerimentos

A. Revisar e investigar os resultados e determinar ações de correções sempre que necessário;
B. Incluir no plano processos e mecanismos para assegurar que as ações de correções identificadas serão completamente implantadas.

RI-9 - Backup do Sistema de Informação da Smart Grid

Requerimentos

A. Realizar backup de informações em nível de usuário contido no sistema de informação de smart grid em uma frequência pré-definida;
B. Realizar backups de informações em nível de sistema;
C. Realizar backups de documentação do sistema de informações, incluindo documentação relacionada com a segurança em uma frequência consistente com o tempo de recuperação definido pela organização; e
D. Proteger a confidencialidade e integridade das informações de backup no local de armazenamento.

RI-10 - Coordenação de Resposta a Incidentes

Requerimentos

A. Políticas e procedimentos devem delinear como a organização implementa o seu plano de emergência e coordenar esforços com as agências de aplicação da lei, reguladores, fornecedores de serviços Internet e outras organizações relevantes no caso de um incidente de segurança.

5.10. Segurança física e de ambiente

SF-1 - Políticas e Procedimentos de Segurança Física e da Ambiente

Requerimentos

A. Desenvolver, implementar, revisar e atualizar em uma frequência definida pela organização uma política de segurança física e ambiental documentado que enderece
    a. Os objetivos, funções e responsabilidades do programa de segurança física e ambiental no que se refere à proteção pessoal da organização e ativos; e
    b. O âmbito do programa de segurança física e ambiental, uma vez que se aplica a todos os funcionários da organização, contratados e terceiros; e
    c. Procedimentos para abordar a implementação da política de segurança física e ambiental e os requisitos físicos e de proteção do ambiente associados;
B. Compromisso de Gestão assegura a conformidade com a política de segurança da organização e outras exigências regulamentares; e
C. A organização assegura que a política e os procedimentos de segurança física e ambiental cumpram com as leis e regulamentos federais, estaduais, locais, tribais e territoriais.

SF-2 - Autorização de Acesso Físico

Requerimentos

A. A organização desenvolve e mantém listas de pessoal com acesso autorizado às instalações que contenham sistemas de informação de smart grid e questões credenciais de autorização (por exemplo, emblemas, cartões de identificação) adequados; e
B. Os funcionários designados no âmbito da revisão da organização e aprovar as listas de acesso em uma frequência definida previamente pela organização, a remoção do pessoal listas de acesso que não necessitam de acesso.

C. A organização autoriza o acesso físico ao estabelecimento onde o sistema de informação de smart grid reside com base na posição ou função;
D. A organização exige múltiplas formas de identificação para ter acesso às dependências em que o sistema de informação de smart grid reside; e
E. A organização requer autenticação multifator para ter acesso às dependências em que o sistema de informação de smart grid reside.

SF-3 - Acesso Físico

Requerimentos

A. Impor controle de acesso físico para todos os pontos de acesso físico ao estabelecimento onde o sistema de informação de smart grid reside;
B. Verificar as autorizações de acesso individuais antes de conceder acesso às dependências;
C. Controlar a entrada para instalações que contêm os sistemas de informação de redes inteligentes;
D. Proteger chaves, combinações e outros dispositivos de acesso físico;
E. Alterar as combinações, chaves e credenciais de autorização em uma frequência definida previamente pela organização e quando as chaves são perdidas, combinações são comprometidos, credenciais individuais são perdidas, ou as pessoas são transferidas ou rescindido.

SF-4 - Monitoramento de Acesso

Requerimento

A. Implantar monitores de acesso físico ao sistema de informação de rede inteligente para detectar e responder a incidentes de segurança física;
B. Avaliar logs de acesso físicos em uma frequência definida pela organização;
C. Monitorar em tempo real o alarme de intrusão e os equipamentos de vigilância;

D. Coordenar as revisões e investigações com capacidade de resposta a incidentes da organização; e
E. Garantir que investigação e resposta a incidentes de segurança física detectados, incluindo violações de segurança aparentes ou atividades suspeitas de acesso físico, sejam parte da capacidade de resposta a incidentes da organização.

SF-5 - Controle de Visitantes

Requerimentos

A. Possuir controle de acessos de visitantes de maneira que seja autenticados antes do acesso às dependências.

SF-6 - Registro de Visitantes

Requerimentos

A. A organização deve garantir que os visitantes sejam cadastrados para acesso às dependências, com as informações:
    a. Nome e organização do visitante
    b. Assinatura
    c. Documento e formulário de Identificação
    d. Data de acesso
    e. Justificativa da visita

SF-7 - Retenção de Log de Acesso Físico

Requerimentos

A. A organização deve reter os logs de acessos físico por um período previamente definido, de maneira que atenda as regulamentações internas e externas.

5.11. Planejamento

PL-1 - Plano de Segurança para Sistemas de Informação de Smart Grid

Requerimentos

A. Desenvolver um plano de segurança para cada sistema de informação de smart grid que alinha com arquitetura corporativa da organização;
B. Explicitamente define os componentes do sistema de informação de redes inteligentes;
C. Descrever as relações com e interligações a outros sistemas de informação de redes inteligentes;
D. Fornecer uma visão geral dos objetivos de segurança para o sistema de informação de redes inteligentes;
E. Descrever os requisitos de segurança em vigor ou previstas para o cumprimento desses requisitos; e
F. Revisar e aprovar pela autoridade de gestão antes de planejar sua implementação;
G. Revisar o plano de segurança para o sistema de informação de smart grid em uma frequência definida organização; e
H. Proceder à revisão do plano para lidar com as mudanças nas informações grade sistema / ambiente inteligente de operação ou problemas identificados durante a implementação do plano ou requisito de segurança avaliações.

PL-2 - Regras de Acompanhamento

Requerimentos

A. A organização estabelece e torna prontamente disponível para todos os usuários do sistema de informação inteligentes grid, um conjunto de regras que descreve as suas responsabilidades e comportamentos esperados em relação ao uso do sistema de informações da rede elétrica inteligente.

PL-3 - Avaliação de Impacto e Privacidade

Requerimentos

A. Realizar uma avaliação de impacto sobre a privacidade no sistema;

B. Avaliar o impacto sobre a privacidade, de maneira que seja aprovado por uma autoridade administrativa.

5.12. Segurança pessoal

SP-1 - Políticas e Procedimentos de Segurança Pessoal

Requerimentos

A. Desenvolver, implementar, revisar e atualizar em uma frequência definida pela organização uma política de segurança pessoal que enderece
    a. Os objetivos, funções e responsabilidades do programa de segurança do pessoal no que se refere à proteção pessoal da organização e ativos; e
    b. O âmbito do programa de segurança pessoal como se aplica a todos os funcionários da organização, contratados e terceiros; e
    c. Procedimentos para tratar da implementação da política de segurança do pessoal e os requisitos de proteção pessoal associado;
B. Compromisso de gestão que assegure a conformidade com a política de segurança da organização e outras exigências regulamentares; e
C. Assegurar que a política e os procedimentos de segurança pessoal cumprem as leis federais, estaduais, locais, tribal, e as leis e regulamentos territoriais.

SP-2 - Desligamento de Pessoas

Requerimentos

A. A organização deve revogar todos os acessos físicos e a sistemas, sempre que um colaborador direto ou terceirizado for desligado, além disso, deve garantir que todos os bens da companhia que estavam de posse do colaborador sejam devolvidos e as informações sejam transferidas para o colaborador substituto;

SP-3 - Transferência de Pessoas

Requerimentos

A. Sempre que um colaborador direto ou indireto for transferido de departamento ou de função, todos os acessos físicos e lógicos devem ser revisados, afim de garantir que este possui acesso somente aos recursos necessários de acordo com sua função

SP-4 - Termo de Acesso

Requerimentos

A. A assinatura do termo de acesso é aplicada para todas as partes, incluindo funcionários terceirizados e contratados, que necessitam acessar alguma localidade ou sistema da companhia, estes sempre devem assim o termo de acesso.

5.13. Gestão e avaliação de riscos

GR-1 - Políticas e Procedimentos de Gestão e Avaliação de Riscos

Requerimentos

A. A organização deve desenvolver, implantar, revisar e atualizar políticas e procedimentos de gestão e avaliação de riscos que endereço:
    a. Objetivos, papéis e responsabilidades do programa de gestão e avaliação de riscos;
    b. O escopo do programa, que deve ser aplicado para todos colaboradores, contratados e terceirizados;
B. De ter compromisso que garanta a conformidade a política e aos processos de gestão e avaliação de riscos;

GR-2 - Nível de Impacto

Requerimentos

A. Especificar os níveis de impactos que os eventos de segurança podem ocasionar;
B. Documentar os resultados do nível de impacto (incluindo a justificativa) no plano de segurança para o sistema de informação; e
C. Avaliar o sistema de informação de smart grid e níveis de impacto informação sobre uma frequência definida a organização.

GR-3 - Avaliação de Vulnerabilidades

Requerimentos

A. Acompanhar e avaliar o sistema de informação de rede inteligente de acordo com o plano de gestão de risco em uma frequência definida pela organização para identificar vulnerabilidades que possam afetar a segurança;
B. Analisar relatórios de verificação de vulnerabilidade e corrigir vulnerabilidades dentro de um período de tempo definido pela organização com base numa avaliação de risco;
C. Implantar ações utilizando as informações obtidas a partir do processo de varredura de vulnerabilidades com pessoal designado por toda a organização para ajudar a eliminar vulnerabilidades semelhantes em outros sistemas de informação de redes inteligentes;
D. Atualizar do sistema para corrigir eventuais vulnerabilidades identificadas, de acordo com informações da política de manutenção do sistema da organização; e
E. Atualizar a lista de vulnerabilidades de sistemas de informação de smart grid em uma frequência definida pela organização ou quando novas vulnerabilidades são identificadas e relatadas.

5.14. Aquisição de serviços

GR-1 - Políticas e Procedimentos para Aquisição de Serviços

Requerimentos

A. A organização deve desenvolver, implantar, revisar e atualizar políticas e procedimentos para aquisição de serviços, de maneira que endereço:
    a. Os objetivos, funções e responsabilidades do processo de aquisição de serviços;
    b. O âmbito do programa de aquisição de serviços como se aplica a todos os funcionários da organização, contratados e terceiros; e
    c. Procedimentos para tratar da implementação da política de aquisição de serviços e os requisitos de proteção pessoal associado;
B. Compromisso de gestão que assegure a conformidade com a política de segurança da organização e outras exigências regulamentares; e
C. Assegurar que a política e os procedimentos de aquisição de serviços cumprem as leis federais, estaduais, locais, tribal, e as leis e regulamentos territoriais.

GR-2 - Políticas de Segurança para Contratados e Terceirizados

Requerimentos

A. Garantir que fornecedores externos e prestadores de serviços que têm um impacto na segurança dos sistemas de informação de smart grid devem atender a política e os procedimentos da organização; e
B. Estabelecer procedimentos para remover o acesso externo de fornecedores e contratantes aos sistemas de informação de smart grid na conclusão / rescisão do contrato.

GR-3 - Aquisições

Requerimentos

A. Incluir os requisitos de segurança em contratos de aquisiçoes de sistemas inteligentes que estejam em conformidade com as leis, regulamentos e políticas de segurança definidas pela organização.

GR-4 - Softwares de Usuários

Requerimentos

A. Criar políticas e procedimentos para gerenciar os softwares de usuários instalados;
B. Caso possuam os privilégios necessários, os usuários têm a possibilidade de instalar software. Programa de segurança da organização identifica os tipos de software permissão para ser baixado e instalado (por exemplo, atualizações e patches de segurança para software existente) e tipos de software proibidos (por exemplo, software que é livre apenas para, não uso corporativo pessoal e software cujo pedigree com relação a ser potencialmente malicioso é desconhecida ou suspeita).

GR-5 - Princípios de Segurança para Engenharia

Requerimentos

A. Princípios de engenharia de segurança incluem:
    a. Requisitos de educação para o desenvolvimento para de todos os desenvolvedores envolvidos no sistema de informação de redes inteligentes;
    b. Especificação de uma norma mínima em matéria de segurança;
    c. Especificação de uma norma mínima para a privacidade;
    d. Criação de um modelo de ameaça por um sistema de informação de redes inteligentes;
    e. Atualização das especificações dos produtos para incluir limitações para as ameaças detectadas durante a modelagem de ameaças;
    f. Utilização de práticas seguras de codificação para reduzir os erros comuns de segurança;

g. Teste para validar a eficácia das práticas de codificação seguras;
h. Desempenho de uma auditoria de segurança final antes da autorização para operar para confirmar a adesão aos requisitos de segurança;
i. Criação de um plano de resposta de segurança documentados e testados no evento vulnerabilidade é descoberta;
j. Criação de um plano de resposta a privacidade documentado e testado no evento vulnerabilidade é descoberta; e
k. Realização de uma análise de causa raiz para entender a causa de vulnerabilidades identificadas.

GR-6 - Gestão de Configuração para Desenvolvimento de Sistemas

Requerimentos

A. Gerenciar e Controlar as alterações de sistemas durante o desenho, desenvolvimento, implantação e operação;
B. Trilhar as falhas de segurança; e
C. Incluir aprovações para as alterações

GR-7 - Testes de Desenvolvimento

Requerimentos

A. O desenvolvedor do sistema de informação de rede inteligente deve criar um teste de segurança e um plano de avaliação;
B. O desenvolvedor para deve apresentar o plano para a organização, para aprovação e implementar;
C. Os resultados do teste e avaliação devem ser submetidos à organização para aprovação; e
D. Testes de segurança do Desenvolvimento não devem ser executados no ambiente de produção.

5.15. Proteção da comunicação

PC-1 - Políticas e Procedimentos de Proteção da Comunicação

Requerimentos

A. A organização deve desenvolver, implantar, revisar e atualizar políticas e procedimentos de proteção da comunicação que endereço:
    a. Objetivos, papéis e responsabilidades do programa de proteção da comunicação;
    b. O escopo do programa, que deve ser aplicado para todos colaboradores, contratados e terceirizados;
        A. De ter compromisso que garanta a conformidade a política e aos processos de gestão e avaliação de riscos;

PC-2 - Separação das Comunicações

Requerimentos

A. É importante que a comunicação para telemetria / aquisição de dados e funcionalidades de gerencia sejam separadas fisicamente ou logicamente;

PC-3 - Isolamento de Funções de Segurança

Requerimentos

A. É necessário isolar as funções de segurança das funções que não são de segurança nos hardwares, software e ou firmwares

PC-4 - Proteção de ataques de Negação de Serviço

Requerimentos

A. O sistema deve reduzir ou limitar os efeitos de um ataque de negação de serviço, com base em uma lista de ataques definida previamente pela organização ou parceiros especializados;
B. Dispositivos de perímetro de rede podem filtrar certos tipos de pacotes para proteger os equipamentos da rede interna de ser diretamente afetados pelos ataques;
C. Deve restringir a capacidade dos usuários internos de lançar ataques de negação de serviço contra os recursos da rede;

PC-5 - Priorização de Recursos

Requerimentos

A. É valido que a utilização dos recursos seja priorizada, de maneira que processos não prioritários não causem lentidão ou interferência na rede e nos serviços de alta prioridade

PC-6 - Proteção de Fronteira

Requerimentos

A. A organização deve delimitaro sistema de informação de redes inteligentes;
B. Os monitores inteligentes devem ser implantados na rede de comunicações e controles na fronteira externa do sistema e nos limites internos;
C. A interface de gestão implementa medidas de segurança adequadas para a proteção da integridade e confidencialidade das informações transmitidas; e
D. A organização deve impedir o acesso do público em redes de sistemas de informação de smart grid internos da organização, exceto nos casos necessáriosonde devem ser feito com acompanhamento devido.

PC-7 - Integridade da Comunicação

Requerimentos

A. As informações trafegas por vias eletrônicas devem ser protegidas;
B. A Organização deve implantar mecanismos de criptografia para garantir a integridade;
C. A integridade de informação deve ser preservada durante a agregação, empacotamento, transformação e a transmissão.

PC-8 - Confidencialidade na Comunicação

Requerimentos

A. É necessário avaliar a implantação este requisito em um ou mais locais dentro das comunicações, cada local de agrega diferentes benefícios e também desvantagens;
B. É importante a implantação de mecanismos de criptografia;

PC-9 - Caminho Seguro

Requerimentos

A. É importante estabelecer um caminho seguro entre o usuário e o sistema de informação de smart grid;

PC-10 - Criação e Gestão de Chave de Criptografia

Requerimentos

A. Aplicar métodos seguros de criptografia e gerenciamento de chaves de criptografia;
B. Estabelecimento de chave inclui um processo de geração de chaves de acordo com um algoritmo especificado e tamanhos de chaves e tamanhos de chaves baseado em um padrão atribuído. A geração de chaves deve ser realizada através de um gerador de números aleatórios apropriado. As políticas de gerenciamento de chaves precisam abordar itens como mudanças periódicas chave, destruição de chaves e distribuição de chaves.

PC-11 - Transmissão de Parâmetros de Segurança

Requerimentos

A. O sistema de informação de smart grid associa de forma fiável os parâmetros de segurança com informações trocadas entre os sistemas de informação empresariais e do sistema de informação de smart grid;
B. Parâmetros de segurança podem ser explícitos ou implicitamente associados com as informações contidas no sistema de informação de smart grid.

PC-12 - Infraestrutura de Certificados de Chave Pública

Requerimentos

A. A organização deve emitir certificados de chave pública sob uma política de certificado apropriada ou obter certificados de chaves públicas no âmbito de uma política de certificado apropriado a partir de um provedor de serviços;

PC-13 - Códigos Móveis

Requerimentos

A. Estabelecer restrições de utilização e de orientação de implementação de tecnologias de código móvel com base no potencial de causar danos ao sistema de informação de smart grid se usado de forma maliciosa;
B. Documentar, monitorar e gerenciar o uso de códigos móveis dentro do sistema de informação de redes inteligentes; e
C. A autoridade de gestão deve autorizar o uso de códigos móveis.
D. Tecnologias de código móvel incluem, por exemplo, Java, JavaScript, ActiveX, PDF, Postscript, filmes Shockwave, animações em Flash, e VBScript. Restrições de utilização e implementação orientação necessidade de aplicam-se tanto a seleção e uso de códigos móveis instalados em servidores organizacionais e códigos móveis baixados e executados em estações de trabalho individuais.

PC-14 - Voz Sobre Internet Protocol (IP)

Requerimentos

A. Estabelecer restrições de utilização e orientação de implementação de tecnologias VoIP com base no potencial de causar danos ao sistema de informação de smart grid se usado de forma maliciosa; e
B. Autorizar, monitor e controlar o uso de VoIP no sistema de informação de smart grid.

PC-15 - Conexões Entre Sistemas

Requerimentos

A. Todas as conexões com sistemas externos devem ser identificadas e protegidas contra alteração ou danos;
B. O objetivo deste requisito é abordar a integridade da conexão fim a fim. Por exemplo, conexões de pontos de acesso externos ao sistema de informação de redes inteligentes precisam ser protegidas para garantir a segurança total do sistema de informação de smart grid. Os pontos de acesso incluem qualquer ponto final de comunicação conectado externamente (por exemplo, modems dial-up).

PC-16 - Funções de Segurança

Requerimentos

A. A organização deve desenhar, especificar e implantar funções e responsabilidades de segurança para os usuários do sistema de informação de smart grid;

PC-17 - Autenticidade de Mensagem

Requerimentos

A. O sistema de informação de smart grid deve fornecer mecanismos para proteger a autenticidade das comunicações de dispositivo para o dispositivo.
B. Autenticação de mensagens fornece proteção contra tráfego com mensagens corrompidas, os dispositivos configurados incorretamente, e entidades maliciosas.
C. Mecanismos de autenticação de mensagens devem ser implementados no nível de protocolo para ambos os protocolos seriais e roteáveis.

PC-18 – Serviço de Resolução de Nome e Endereço Seguro

Requerimentos

A. Os sistemas que fornecem serviços de resolução de nome / endereço são configurados para fornecer origem de dados adicionais e artefatos de integridade, juntamente com os dados oficiais retornados em resposta a consultas de resolução.

PC-19 - Aplicações Independentes de Sistemas Operacionais

Requerimentos

A. O sistema de informação da smart grid deve possuir aplicações que são independentes de sistemas operacionais, que podem ser executadas em vários sistemas operacionais. Tais aplicações promovem a portabilidade e reconstituição em diferentes arquiteturas de plataforma, aumentando assim a disponibilidade para funcionalidades críticas, enquanto uma organização está sob um ataque explorando vulnerabilidades em um determinado sistema operacional.

PC-20 - Heterogeneidade

Requerimentos

A. Os sistemas devem ser implantados utilizando tecnologias heterogêneas de maneira que reduza os impactos caso uma tecnologia seja explorada ou atacada.

PC-21 - Tecnologias de Virtualização

Requerimentos

A. A organização emprega técnicas de virtualização para apresentar componentes em ambientes como outros tipos de componentes ou componentes com diferentes configurações;
B. Técnicas de virtualização oferecem às organizações a capacidade de disfarçar componentes em ambientes de sistema de informação de smart grid, potencialmente reduzindo a probabilidade de ataques bem sucedidos sem o custo de ter múltiplas plataformas.

PC-22 - Particionamento de Aplicações

Requerimentos

A. É necessário que a organização separe as funcionalidades do sistema em infraestrutura distintas e também separe o gerenciamento das tecnologias e funções.
B. Funcionalidade inteligente de gestão de sistema de informação da rede inclui, por exemplo, funções necessárias para administrar bancos de dados, componentes de rede, estações de trabalho ou servidores, e normalmente requer o acesso de usuário privilegiado. Por isso, é importante a separação da funcionalidade da funcionalidade de usuário do gerenciamento de sistema de informação de rede inteligente é físico ou lógico.

5.16. Integridade da informação

II-1 - Políticas e Procedimento de Integridade da Informação

Requerimentos

A. A organização deve desenvolver, implantar, revisar e atualizar políticas e procedimentos de integridade da Informação que enderece:
    a. Objetivos, papéis e responsabilidades do programa de integridade da informação;
    b. O escopo do programa, que deve ser aplicado para todos colaboradores, contratados e terceirizados;
    c. Ter compromisso que garanta a conformidade a política integridade da Informação

II-2 - Falha e Remediação

Requerimentos

A. Identificar, relatar, e corrigir falhas do sistema de informação de redes inteligentes;
B. Testar as atualizações de software relacionados com a falha de remediação para garantir a eficácia e identificar os efeitos colaterais potenciais nos sistemas de informação organizacionais de smart grid antes da instalação; e
C. Incorporar a remediação no processo de gerenciamento de configuração organizacional.

II-3 - Proteção de Códigos Maliciosos e SPAM

Requerimentos

A. Implantar mecanismos de proteção de código malicioso; e
B. Atualizar os mecanismos de proteção de código malicioso (incluindo definições de assinatura) sempre que novas versões estejam disponíveis de acordo com a política e os procedimentos de gerenciamento de configuração organizacional; e
C. Impedir que os usuários contornem os recursos de proteção de código malicioso.

II-4 - Ferramentas e Técnicas de Monitoramento

Requerimentos

A. A capacidade de monitoramento do sistema pode ser alcançada através de uma variedade de ferramentas e técnicas (por exemplo, sistemas de detecção de intrusão, sistemas de prevenção de intrusão, o software de proteção de código malicioso,software de monitoramento de registro, software de monitoramento de rede, e rede de ferramentas de análise forense). A granularidade da informação recolhida pode ser determinada pela organização com base nos seus objetivos de monitoração e da capacidade do sistema de informação de rede inteligente para apoiar tais atividades.

II-5 - Restrições e Alertar de Segurança

Requerimentos

A. Receber alertas de segurança de rede inteligente sistema de informação, sugestões e diretrizes de organizações externas; e
B. Gerar e divulgar alertas internos de segurança, avisos, e as diretivas consideradas necessárias.

II-6 - Integridade de Software e Informações

Requerimentos

A. É importante monitorar e identificar alterações não autorizadas em informações e software;
B. A organização deve empregar técnicas de verificação de integridade no sistema de informação de rede inteligente para procurar evidências de adulteração de informações, erros e / ou omissões.

II-7 - Validação de Entrada de Informações

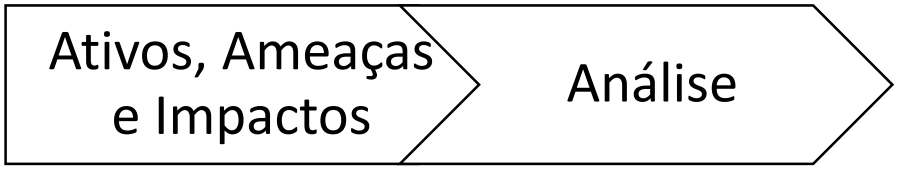
Requerimentos

A. Aplicar mecanismos para verificar exatidão, integridade, validade e autenticidade da informação
B. Regras para a verificação da sintaxe de entrada de informações (conjunto de caracteres, comprimento, intervalo numérico, valores aceitáveis) para garantir que as entradas correspondem as definições especificadas em formato e conteúdo.

6. RESULTADOS

A metodologia de identificação do nível de maturidade de segurança cibernética na smart grid consiste em identificar um caso de uso como primeira etapa, realizar um levantamento para identificação dos ativos, ameaças e impactos como segunda etapa e uma análise para identificação do cumprimento e aplicação dos requisitos de segurança como terceira etapa, como apresentado na figura 14.

Figura 14 - Fluxo da Metodologia



Na fase de análise deve ser avaliado e documentado o nível em que cada requisito está implantado no caso de uso em questão, que são classificados em nível 1, nível 2, nível 3 ou nível 4, com isso, será possível identificar o nível de maturidade de cada grupo de requisitos o nível de maturidade geral do caso de uso e consequentemente o nível de maturidade de segurança cibernética dos sistemas de smart grid de uma organização ou até mesmo de uma cidade, e também deixar explícito os pontos a serem melhorados.

6.1. Casos de uso simulados

Com o objetivo de homologar a efetividade da metodologia, todo o fluxo foi aplicado em um sistema de smart grid que suporta o gerenciamento remoto das religadoras de uma grande distribuidora de energia brasileira. Neste cenário, considerou-se como caso de uso o sistema atual de SCADA que foi desenvolvido internamente e um sistema de mercado.

Levantamento de Ativos

Sensores e atuadores de controle da rede elétrica (Remotas), Rede de comunicação entre as remotas e o datacenter, Sistemas centralizados de processamento (SCADA), Centro de Operação, Operadores e Estações de Operação

Ameaças

Ataque de negação de serviços, destruição física de equipamentos, que podem ser iniciados através de engenharia social, malwares ou ataques avançados persistentes (APT – Advanced Persistent Threats)

Impactos

Interrupção no fornecimento de energia, perdas financeiras com compensações aos consumidores, risco de vida aos eletricistas com energização não autorizada, entre outros

Análise

Na comparação dos cenários ficou comprovada a eficiência da metodologia, onde o sistema proprietário e o novo sistema foram classificados no nível de maturidade 1. No detalhamento de requisitos ficou claro que para que o novo sistema seja classificado como nível de maturidade 2 será necessário investimento somente em um centro de operações de contingência, diferente do sistema proprietário que possui vários requisitos classificados no nível 1.

Grupo de Requerimentos de Controle de Acessos

O foco do controle de acesso é garantir que os recursos sejam acessados somente pelos recursos apropriados, e que os recursos estão corretamente identificados. Além de analisar os mecanismos necessários para monitorar as atividades de acesso para atividade imprópria. Na tabela seguinte é possível visualizar a distribuição dos níveis de maturidade organizados do nível 1 – N1 ao nível 4 – N4.

Tabela 2 - Nível de Maturidade de Controle de Acessos

Caso de Uso	**Sistema Proprietário**				**Novo Sistema**			
Requerimento	N1	N2	N3	N4	N1	N2	N3	N4
CA-1 - Política e Procedimento de Controle de Acesso	x					x		
CA-2 - Política e Procedimento de Acesso Remoto	x					x		
CA-3 - Gerenciamento de contas		x						x
CA-4 - Imposição de Acesso		x						x
CA-5 - Separação de Responsabilidades		x						x
CA-6 - Menor Privilégio		x						x
CA-7 - Tentativas de Login	x							x
CA-8 - Controle Concorrente de Sessão		x						x
CA-9 - Bloqueio de Sessão		x						x
CA-10 - Acesso Remoto			x					x
CA-11 - Restrições de Acesso a Rede sem Fio				x				x
CA-12 - Controle de Acesso para Dispositivos Móveis e Portáteis			x					x
CA-13 - Utilização de Sistemas de Informação Externos			x					x
CA-14 - Senhas			x					x
CA - Resultado	3	6	4	1	0	2	0	12

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 21% no nível 1, 43% no nível 2, 29% no nível 3 e 7% no nível 4

Novo sistema: 0% no nível 1, 14% no nível 2, 0% no nível 3 e 86% no nível 4

Figura 15 - Nível de Maturidade de Controle de Acesso do Sistema Proprietário

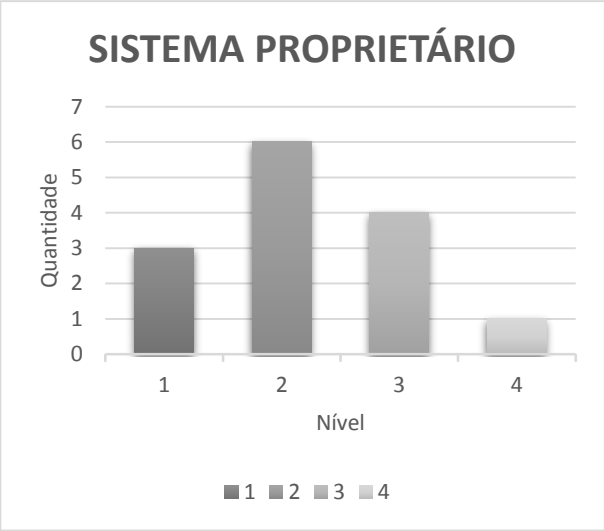
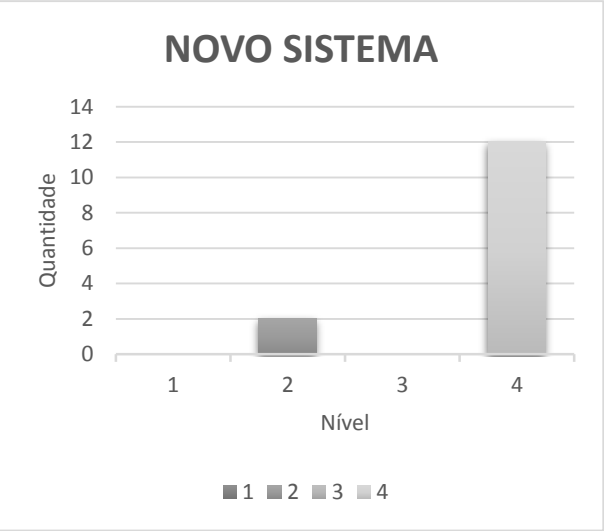


Figura 16 - Nível de Maturidade de Controle de Acesso do Novo Sistema



Grupo de Requerimentos de Conscientização e Treinamento

O objetivo deste grupo de requerimentos é consolidar requerimentos que garantam que a companhia possua políticas, processos e ferramentas de divulgação das melhores práticas de segurança cibernética para conscientização das partes envolvidas diretamente e indiretamente com os sistemas da rede elétrica inteligente.

Tabela 3 - Nível de Maturidade de Conscientização e Treinamento

Caso de Uso		**Sistema Proprietário**					**Novo Sistema**			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
CT-1 - Políticas e Procedimentos de Sensibilização e Formação		x						x		
CT-2 - Conscientização da Segurança a Informação		x							x	
CT-3 - Treinamento de Segurança da Informação		x							x	
CT-4 - Contato com Associações e Grupos de Segurança		x								x

CT - Resultado		4	0	0	0		0	1	2	10

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 21% no nível 1, 43% no nível 2, 29% no nível 3 e 7% no nível 4

Novo sistema: 0% no nível 1, 14% no nível 2, 0% no nível 3 e 86% no nível 4

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 100% no nível 1

Novo sistema: 0% no nível 1, 8% no nível 2, 15% no nível 3 e 77% no nível 4

Figura 17 - Nível de Maturidade de Conscientização e Treinamento do Sistema Proprietário

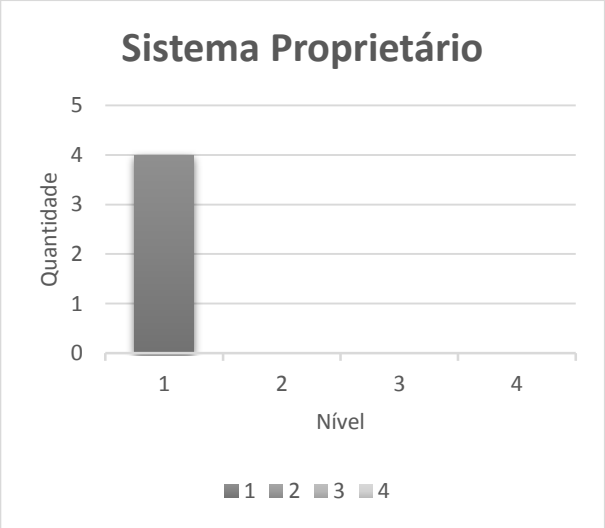
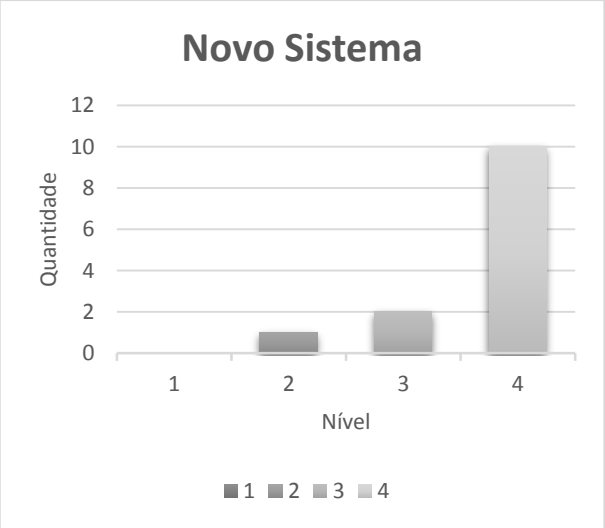


Figura 18 - Nível de Maturidade de Conscientização e Treinamento do Novo Sistema



Grupo de Requerimentos de Auditoria e Responsabilização

Tabela 4 - Nível de Maturidade de Auditoria e Responsabilização

Caso de Uso	Sistema Proprietário				Novo Sistema			
Requerimento	N 1	N 2	N 3	N 4	N 1	N 2	N 3	N 4
AR-1 - Políticas e Procedimentos de Auditoria e Responsabilidade	x					x		
AR-2 - Eventos Auditáveis		x					x	
AR-3 - Conteúdo dos Registros Auditados		x					x	
AR-4 - Monitoramento, Analise e Relatório de Auditoria		x					x	
AR-5 - Ferramenta de Análise e Geração de Relatórios de Auditoria	x						x	
AR-6 - Proteção das Informações de Auditoria		x						
AR-7 - Retenção de Registros de Auditoria		x					x	
AR-8 - Condução de Auditorias Frequentes		x						x
AR-9 - Qualificação do Auditor	x							x
AR-10 - Conformidade com Políticas de Segurança	x							x
AR-11 - Geração de registro auditáveis		x						x
AR-12 - Não Repúdio	x							x
AR – Resultado	5	7	0	0	0	1	5	5

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 42% no nível 1 e 58% no nível 2

Novo sistema: 9% no nível 2, 46% no nível 3 e 45% no nível 4

Figura 19 - Nível de Maturidade de Auditoria e Responsabilização do Sistema Proprietário

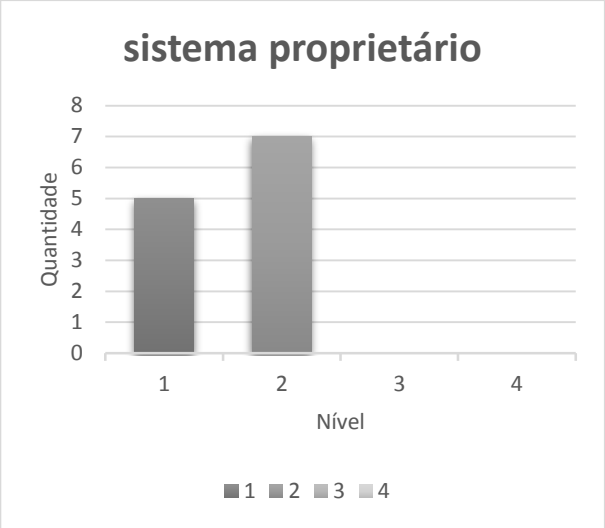
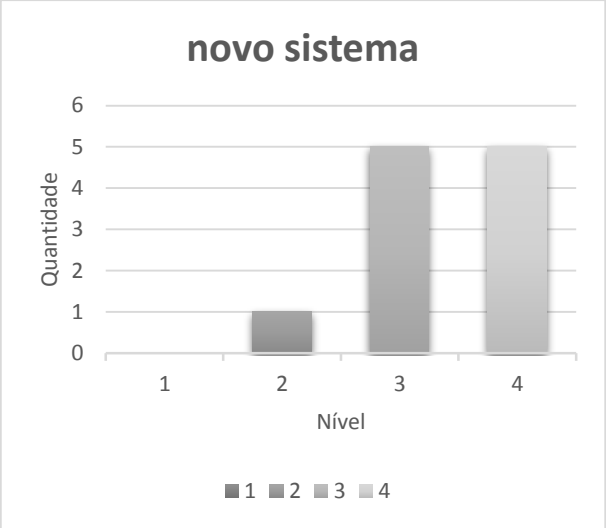


Figura 20 - Nível de Maturidade de Auditoria e Responsabilização do Novo Sistema



Grupo de Requerimentos Avaliação de Segurança e Autorização

Tabela 5 - Nível de Maturidade de Avaliação de Segurança e Autorização

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
AA-1 - Avaliações de Segurança e Políticas e Procedimentos de Autorização		x						x		
AA-2 - Avaliação de Segurança		x							x	
AA-3 - Melhoria Contínua			x							x
AA-4 - Conexões do Sistema de Informação da Smart Grid			x							x
AA-5 - Monitoramento Contínuo			x							x
AA - Resultado		2	3	0	0		0	1	1	3

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 40% no nível 1 e 60% no nível 2

Novo sistema: 20% no nível 2, 20% no nível 3 e 60% no nível 4

Figura 21 - Nível de Maturidade de Avaliação de Segurança e Autorização do Sistema Proprietário

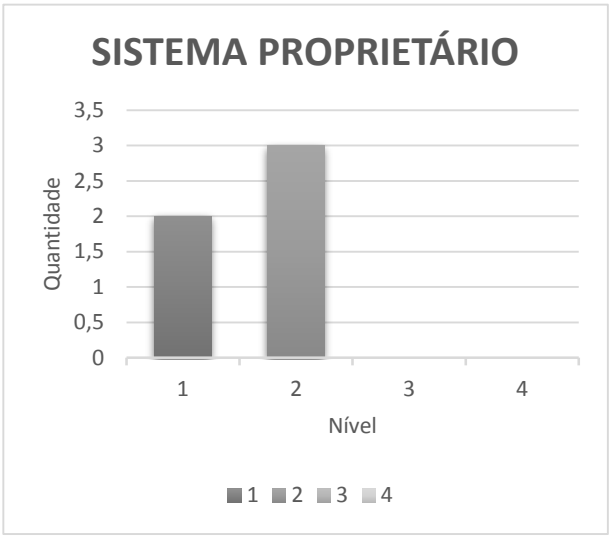
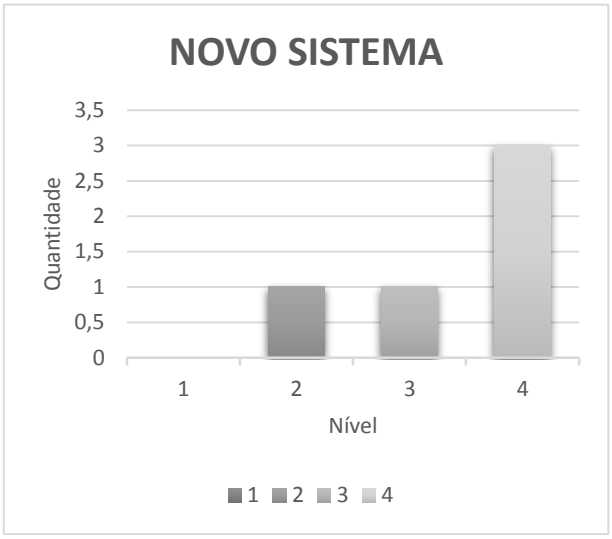


Figura 22 - Nível de Maturidade de Avaliação de Segurança e Autorização do Novo Sistema



Grupo de Requerimentos de Gestão de Configuração

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
GC-1 - Políticas e Procedimentos de gerenciamento de configuração		x						x		
GC-2 - Linha de Base de Configuração			x						x	
GC-3 - Controle de Alterações de Configuração		x							x	
GC-4 - Monitoramento de Alteração de Configurações		x							x	
GC-5 - Restrição de Acesso para Alteração de Configurações			x							x
GC-6 - Inventário de Componentes			x							x
GC-7 - Inclusão, Remoção e Eliminação dos Equipamentos		x							x	
GC-8 - Plano de Gerenciamento de Configuração		x							x	
GC - Resultado		5	3	0	0		0	1	5	2

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 62% no nível 1 e 38% no nível 2

Novo sistema: 12% no nível 2, 63% no nível 3 e 25% no nível 4

Figura 23 - Nível de Maturidade de Gestão de Configuração do Sistema Proprietário

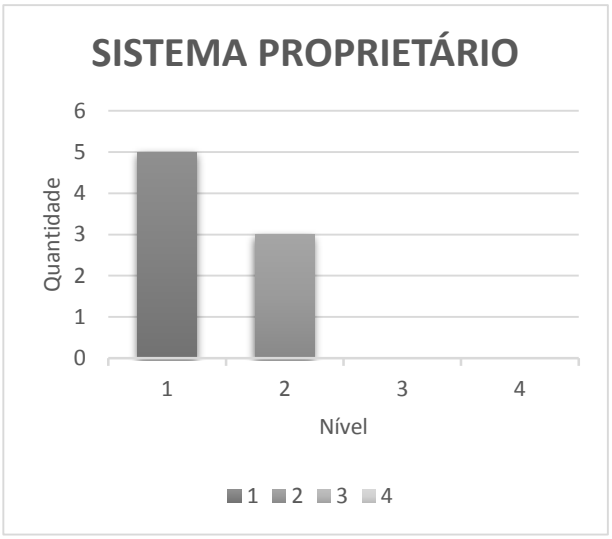
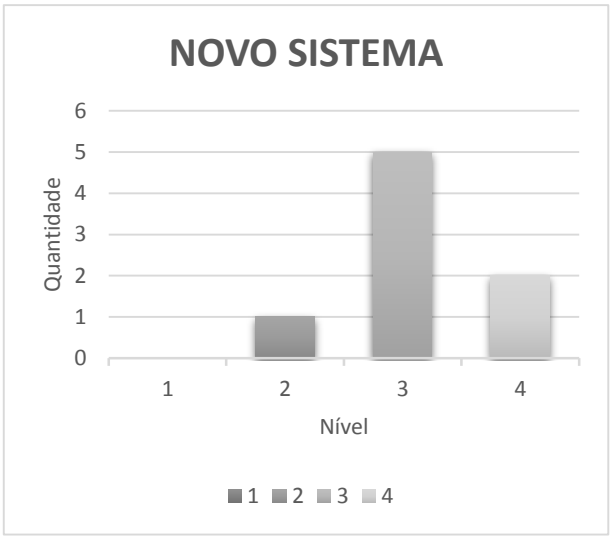


Figura 24 - Nível de Maturidade de Gestão de Configuração do Novo Sistema



Grupo de Requerimentos de Continuidade das Operações

Tabela 6 - Nível de Maturidade de Continuidade das Operações

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
CO-1 - Políticas e Procedimento de Continuidade de Operação		x							x	
CO-2 - Plano de Continuidade da Operação		x							x	
CO-3 - Papéis e Responsabilidades da Continuidade das Operações		x							x	
CO-4 - Treinamento de Continuidade da Operação		x							x	
CO-5 - Plano de teste da Continuidade da Operação		x							x	
CO-6 - Atualização de Plano de Continuidade da Operação		x							x	
CO-7 - Site de Armazenamento Alternativo		x								x
CO-8 - Serviço de Telecomunicações Alternativo		x								x
CO-9 - Centro de Controle Alternativo		x					x			
CO - Resultado		9	0	0	0		1	0	6	2

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 100% no nível 1

Novo sistema: 11% no nível 1, 0% no nível 2, 67% no nível 3 e 22% no nível 4

Figura 25 - Nível de Maturidade de Continuidade de Operações do Sistema Proprietário

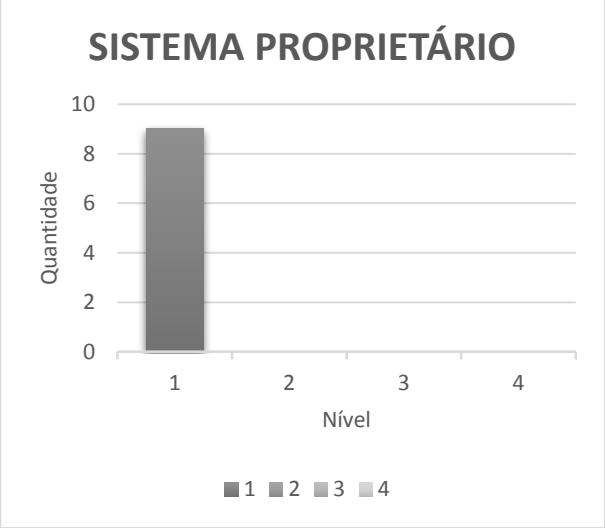
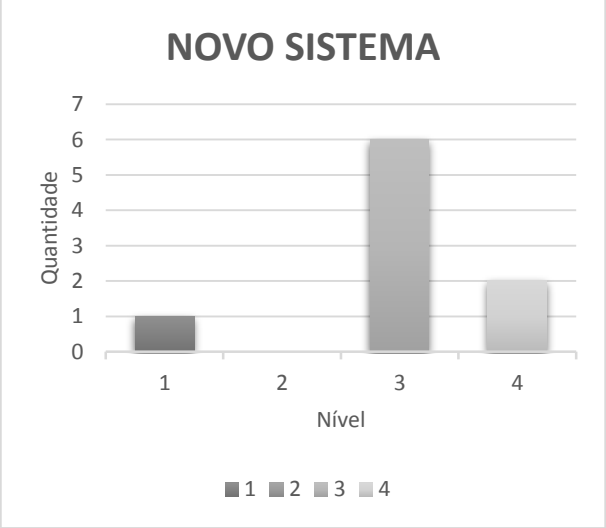


Figura 26 - Nível de Maturidade de Continuidade de Operações do Novo Sistema



Grupo de Requerimentos de Identificação e Autenticação

Tabela 7 - Nível de Maturidade de Identificação e Autenticação

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
IA-1 - Políticas e Procedimentos de Identificação e Autenticação		x						x		
IA-2 - Gerenciamento do Identificador		x							x	
IA-3 - Gerenciamento do Autenticador			x						x	
IA-4 - Identificação e Autenticação do usuário				x					x	
IA-5 - Identificação e Autenticação de Dispositivos			x						x	
IA-6 - Resposta de Autenticação				x					x	
IA - Resultado		2	2	2	0		0	1	5	0

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 34% no nível 1, 33% no nível 2, 33% no nível 3 e 0% no nível 4

Novo sistema: 0% no nível 1, 17% no nível 2, 83% no nível 3 e 0% no nível 4

Figura 27 - Nível de Maturidade de Identificação e Autenticação do Sistema Proprietário

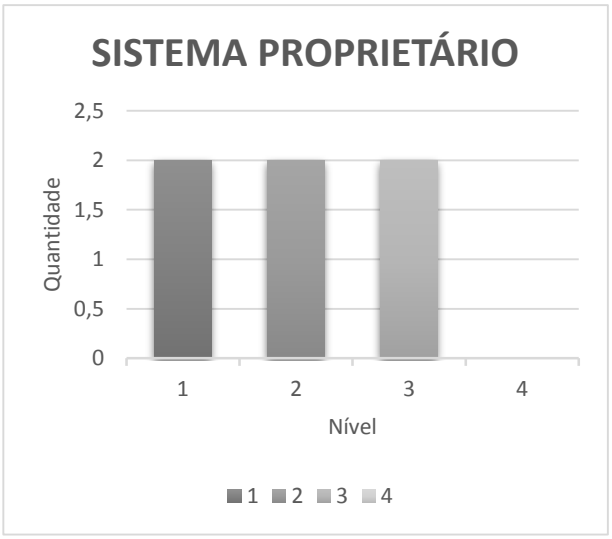
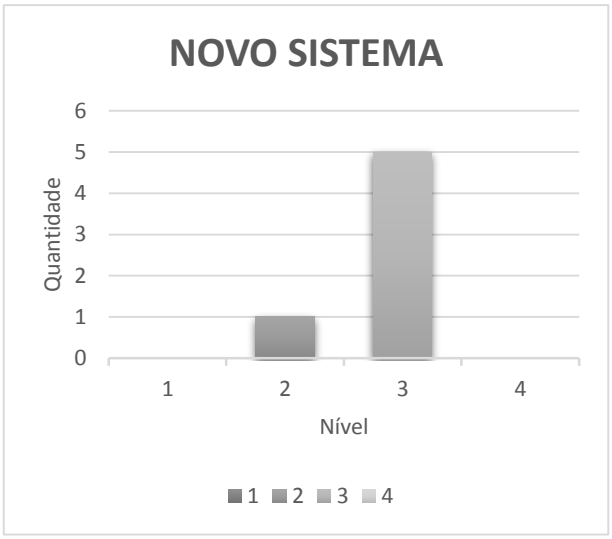


Figura 28 - Nível de Maturidade de Identificação e Autenticação do Novo Sistema



Grupo de Requerimentos de Gestão das Informações e Documentos

Tabela 8 - Nível de Maturidade de Gestão das Informações e Documentos

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
GI-1 - Políticas e Procedimentos de Gerenciamento de Documentos e Informações		x						x		
GI-2 - Retenção de Documentos e Informações		x						x		
GI-3 - Manuseio da Informação		x						x		
GI-4 - Troca de Informações		x						x		
GI-5 - Rotulagem Automatizada		x						x		
GI - Resultado		5	0	0	0		0	5	0	0

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 100% no nível 1

Novo sistema: 100% no nível 2

Figura 29 – Nível de Maturidade de Gestão das Informações e Documentos do Sistema Proprietário

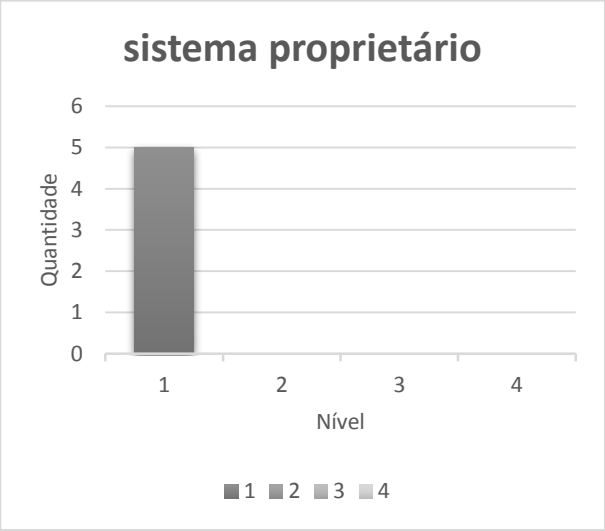
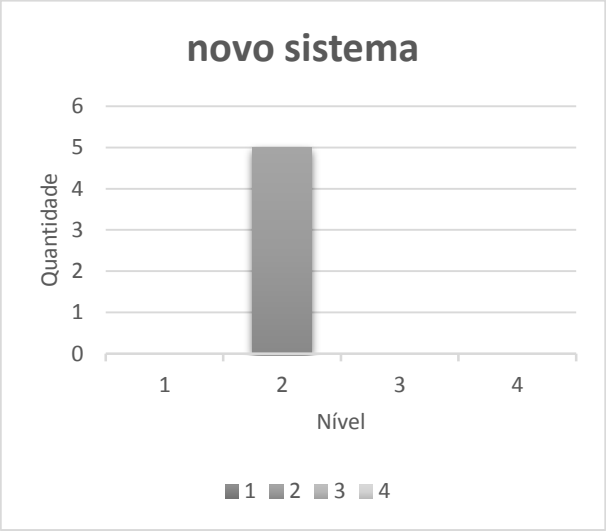


Figura 30 - Nível de Maturidade de Gestão das Informações e Documentos do Novo Sistema



Grupo de Requerimentos de Resposta a Incidentes

Tabela 9 - Nível de Maturidade de Resposta a Incidentes

Caso de Uso		Sistema Proprietário					Novo Sistema		
Requerimento		N1	N2	N3	N4		N 1	N 2	N 3	N 4
RI-1 - Políticas e Procedimentos de Resposta a Incidentes		x						x		
RI-2 - Papéis e Responsabilidades de Resposta a Incidentes		x						x		
RI-3 - Treinamento de Resposta a Incidentes		x							x	
RI-4 - Teste de Resposta a Incidentes		x							x	
RI-5 - Monitoramento de Incidentes		x							x	
RI-6 - Relatório de Incidentes		x							x	
RI-7 - Investigação e Análise de Resposta a Incidentes			x						x	
RI-8 - Ações de Correção			x						x	
RI-9 - Backup do Sistema de Informação da Smart Grid			x							x
RI-10 - Coordenação de Resposta a Incidentes			x						x	
RI - Resultado		6	4	0	0		0	2	7	1

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 60% no nível 1 e 40% no nível 2

Novo sistema: 0% no nível 1, 20% no nível 2, 70% no nível 3 e 10% no nível 4

Figura 31 - Nível de Maturidade de Resposta a Incidentes do Sistema Proprietário

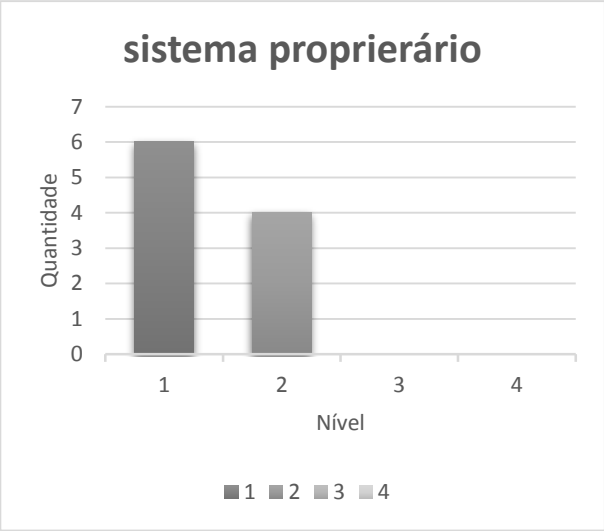
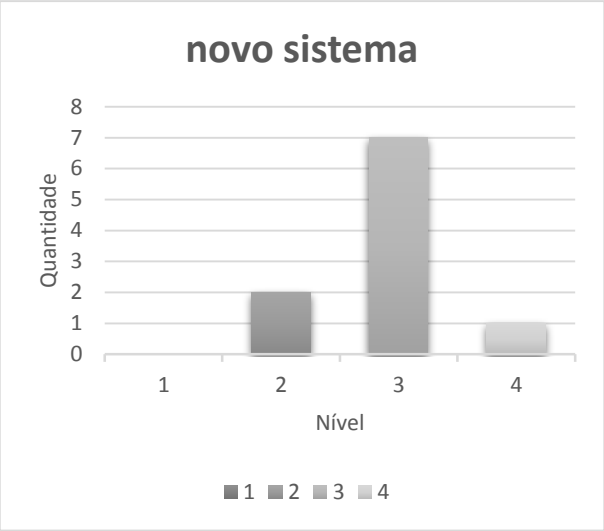


Figura 32 - Nível de Maturidade de Resposta a Incidentes do Novo Sistema



Grupo de Requerimentos de Segurança Física

Tabela 10 - Nível de Maturidade de Segurança Física

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
SF-1 - Políticas e Procedimentos de Segurança Física e da Ambiente		x						x		
SF-2 - Autorização de Acesso Físico			x					x		
SF-3 - Acesso Físico			x					x		
SF-4 - Monitoramento de Acesso			x					x		
SF-5 - Controle de Visitantes			x					x		
SF-6 - Registro de Visitantes			x					x		
SF-7 - Retenção de Log de Acesso Físico			x					x		
SF - Resultado		1	6	0	0		0	7	0	0

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 14% no nível 1 e 86% no nível 2

Novo sistema: 100% no nível 2

Figura 33 - Nível de Maturidade de Segurança Física do Sistema Proprietário

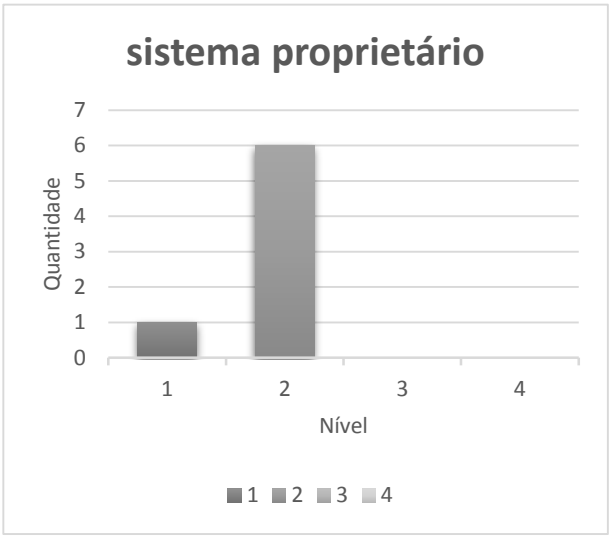
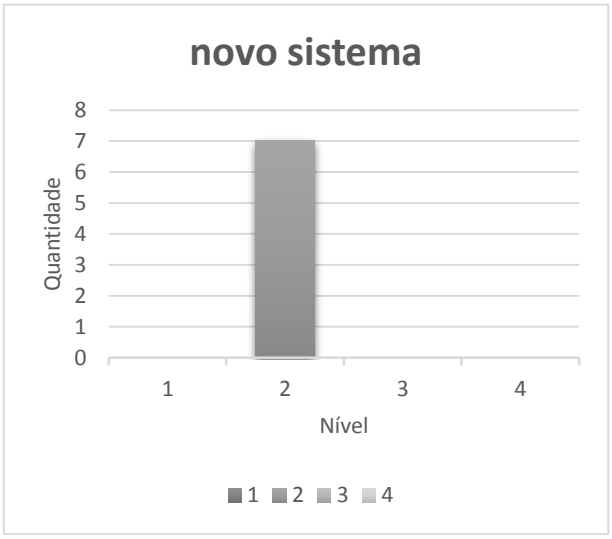


Figura 34 - Nível de Maturidade de Segurança Física do Novo Sistema



Grupo de Requerimentos de Planejamento

Tabela 11 - Nível de Maturidade de Planejamento

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
PL-1 - Plano de Segurança para Sistemas de Informação de Smart Grid		x						x		
PL-2 - Regras de Acompanhamento		x							x	
PL-3 - Avaliação de Impacto e Privacidade		x						x		
PL - Resultado		3	0	0	0		0	2	1	0

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 100% no nível 1

Novo sistema: 67% no nível 2 e 33% no nível 3

Figura 35 - Nível de Maturidade de Planejamento do Sistema Proprietário

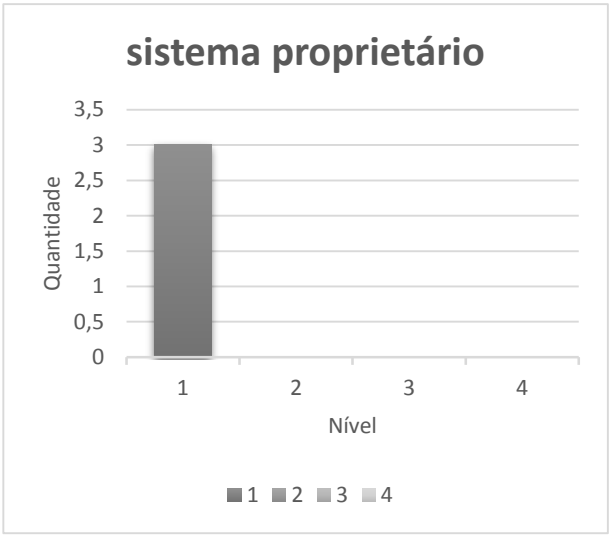
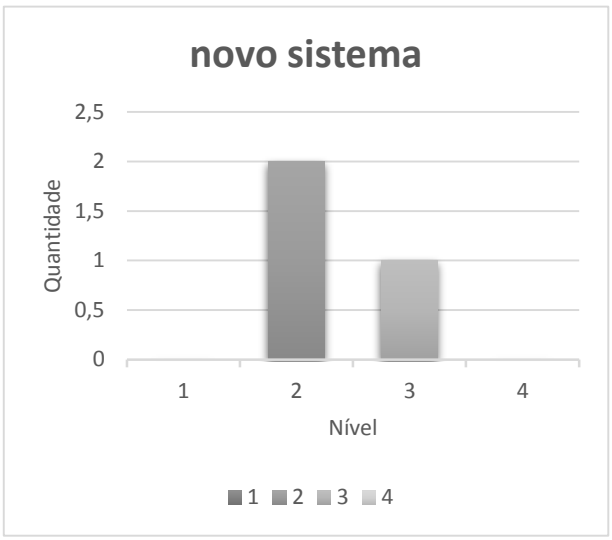


Figura 36 - Nível de Maturidade de Planejamento do Novo Sistema



Grupo de Requerimentos de Segurança Pessoal

Tabela 12 - Nível de Maturidade de Segurança Pessoal

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
SP-1 - Políticas e Procedimentos de Segurança Pessoal		x						x		
SP-2 - Desligamento de Pessoas			x							x
SP-3 - Transferência de Pessoas			x							x
SP-4 - Termo de Acesso		x								x
SP - Resultado		2	2	0	0		0	1	0	3

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 50% no nível 1 e 50% no nível 2

Novo sistema: 25% no nível 2 e 75% no nível 4

Figura 37 - Nível de Maturidade de Segurança Pessoal do Sistema Proprietário

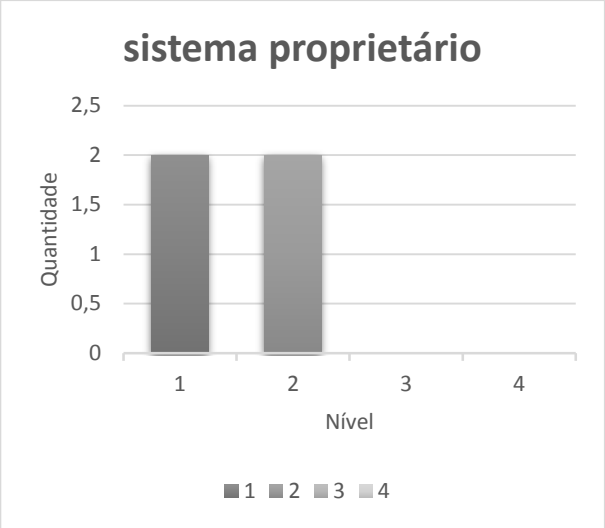
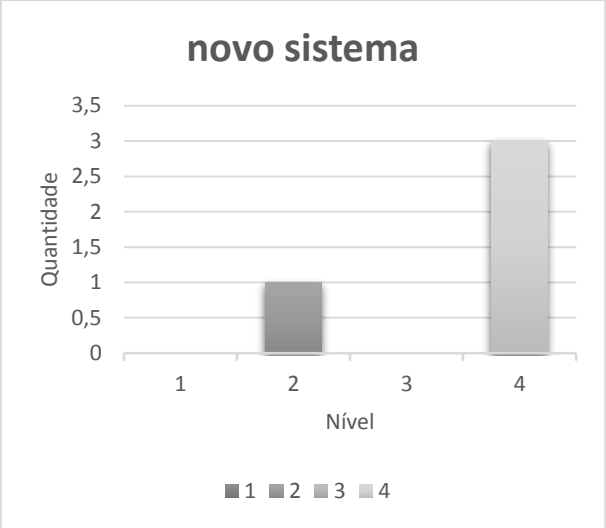


Figura 38 - Nível de Maturidade de Segurança Pessoal do Novo Sistema



Grupo de Requerimentos de Gestão e Avaliação de Riscos

Tabela 13 - Nível de Maturidade de Gestão e Avaliação de Riscos

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
GR-1 - Políticas e Procedimentos de Gestão e Avaliação de Riscos		x						x		
GR-2 - Nível de Impacto		x						x		
GR-3 - Avaliação de Vulnerabilidades		x						x		
GR - Resultado		3	0	0	0		0	3	0	0

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 100% no nível 1

Novo sistema: 100% no nível 2

Figura 39 - Nível de Maturidade de Gestão e Avaliação de Riscos do Sistema Proprietário

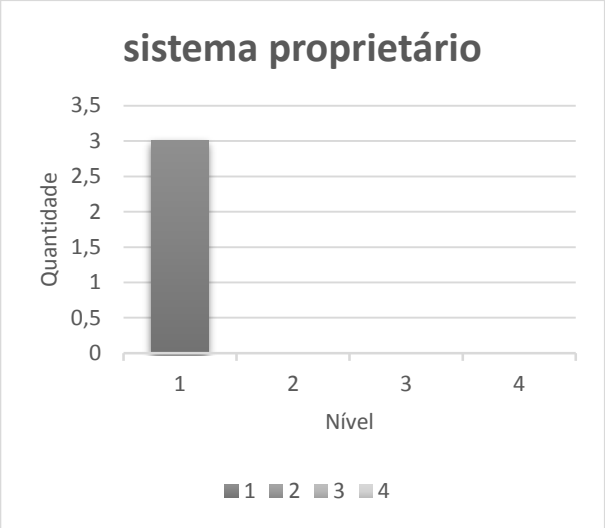
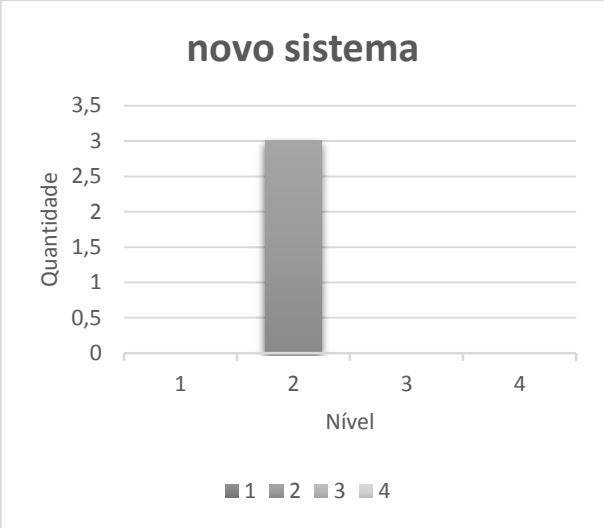


Figura 40 - Nível de Maturidade de Gestão e Avaliação de Riscos do Novo Sistema



Grupo de Requerimentos de Aquisição de Serviços

Tabela 14 - Nível de Maturidade de Aquisição de Serviços

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
AS-1 - Políticas e Procedimentos para Aquisição de Serviços		x						x		
AS-2 - Políticas de Segurança para Contratados e Terceirizados		x						x		
AS-3 - Aquisições		x							x	
AS-4 - Softwares de Usuários		x							x	
AS-5 - Princípios de Segurança para Engenharia		x							x	
AS-6 - Gestão de Configuração para Desenvolvimento de Sistemas		x								x
AS-7 - Testes de Desenvolvimento			x							x
AS - Resultado		6	1	0	0		0	2	3	2

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 86% no nível 1 e 14% no nível 2

Novo sistema: 28% no nível 2, 43% no nível 3 e 29% no nível 4

Figura 41 - Nível de Maturidade de Aquisição de Serviços do Sistema Proprietário

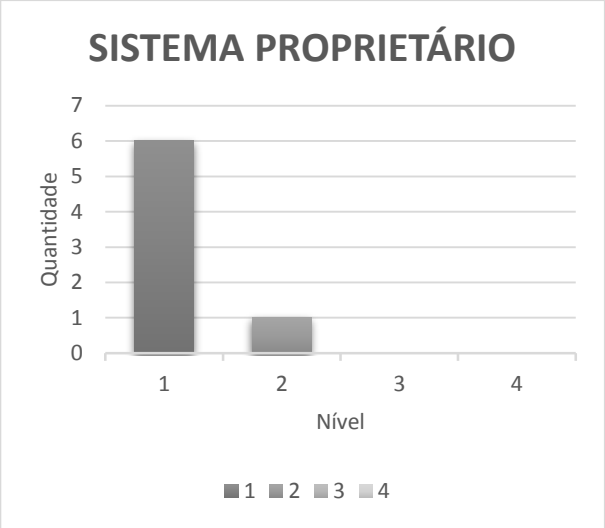
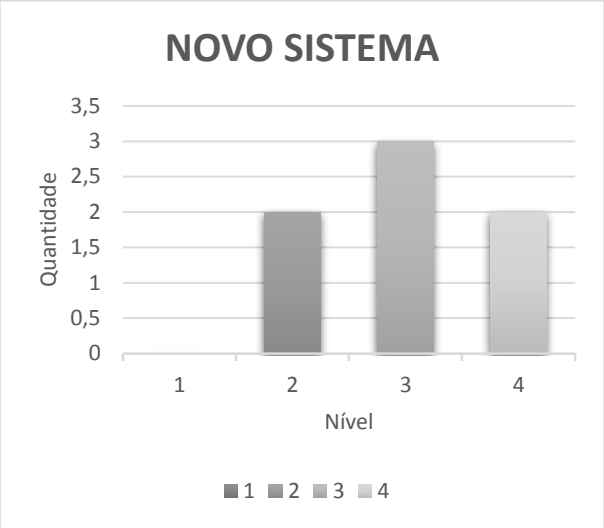


Figura 42 - Nível de Maturidade de Aquisição de Serviços do Novo Sistema



Grupo de Requerimentos de Proteção da Comunicação

Tabela 15 - Proteção da Comunicação

Caso de Uso		Sistema Proprietário					Novo Sistema			
Requerimento		N 1	N 2	N 3	N 4		N 1	N 2	N 3	N 4
PC-1 - Políticas e Procedimentos de Proteção da Comunicação		x						x		
PC-2 - Separação das Comunicações				x						x
PC-3 - Isolamento de Funções de Segurança			x							x
PC-4 - Proteção de ataques de Negação de Serviço			x							x
PC-5 - Priorização de Recursos			x							x
PC-6 - Proteção de Fronteira				x						x
PC-7 - Integridade da Comunicação			x							x
PC-8 - Confidencialidade na Comunicação			x							x
PC-9 - Caminho Seguro			x							x
PC-10 - Criação e Gestão de Chave de Criptografia		x								x
PC-11 - Transmissão de Parâmetros de Segurança		x								x
PC-12 - Infraestrutura de Certificados de Chave Pública		x								x
PC-13 - Códigos Móveis		x								x
PC-14 - Voz Sobre Internet Protocol (IP)		x							x	
PC-15 - Conexões Entre Sistemas			x							x
PC-16 - Funções de Segurança			x							x
PC-17 - Autenticidade de Mensagem				x						x

PC-18 – Serviço de Resolução de Nome e Endereço Seguro				x					x
PC-19 - Aplicações Independentes de Sistemas Operacionais			x						x
PC-20 - Heterogeneidade			x						x
PC-21 - Tecnologias de Virtualização				x					x
PC-22 - Particionamento de Aplicações			x						x
PC - Resultado		6	11	5	0		0	1	1	20

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 27% no nível 1, 50% no nível 2 e 23% no nível 3

Novo sistema: 4% no nível 2, 5% no nível 3 e 91% no nível 4

Figura 43 - Nível de Maturidade de Proteção da Comunicação do Sistema Proprietário

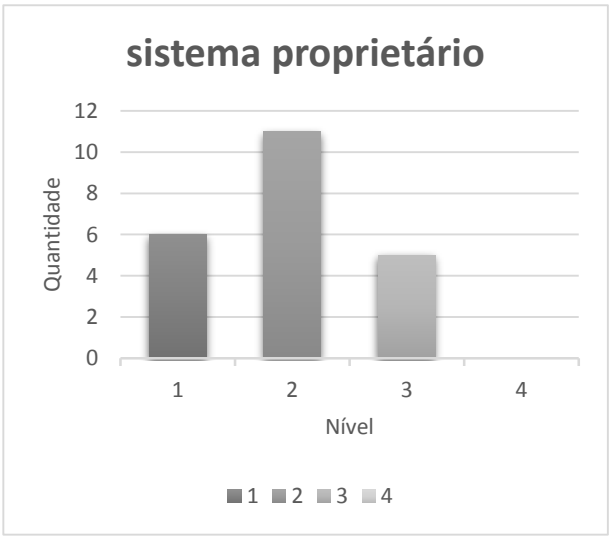
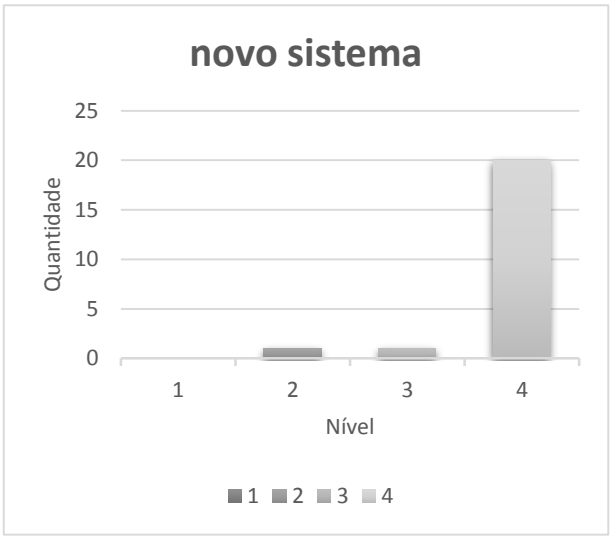


Figura 44 - Nível de Maturidade de Proteção da Comunicação do Novo Sistema



Grupo de Requerimentos de Integridade da Informação

Tabela 16 - Nível de Maturidade de Integridade da Informação

Caso de Uso	Sistema Proprietário				Novo Sistema			
Requerimento	N 1	N 2	N 3	N 4	N 1	N 2	N 3	N 4
II-1 - Políticas e Procedimento de Integridade da Informação	x					x		
II-2 - Falha e Remediação	x					x		
II-3 - Proteção de Códigos Maliciosos e SPAM		x						x
II-4 - Ferramentas e Técnicas de Monitoramento		x						x
II-5 - Restrições e Alertar de Segurança		x						x
II-6 - Integridade de Software e Informações		x					x	
II-7 - Validação de Entrada de Informações	x						x	
II - Resultado	3	4	0	0	0	2	2	3

Neste cenário, os sistemas tiveram seus requerimentos classificados da seguinte maneira:

Sistema proprietário: 43% no nível 1 e 57% no nível 2

Novo sistema: 28% no nível 2, 29% no nível 3 e 43% no nível 4

Figura 45 - Nível de Maturidade de Integridade da Informação do Sistema Proprietário

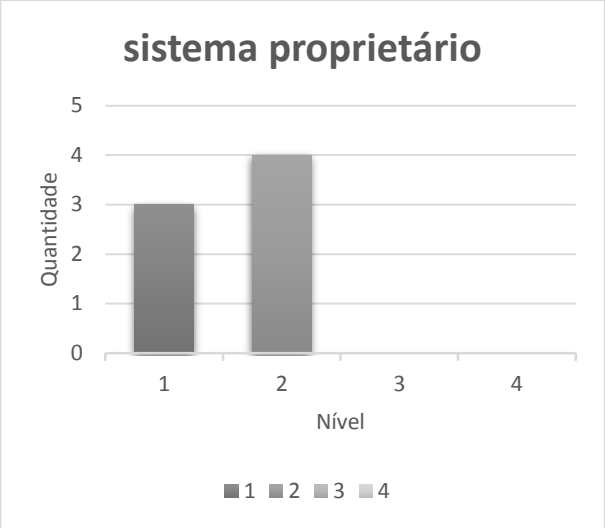
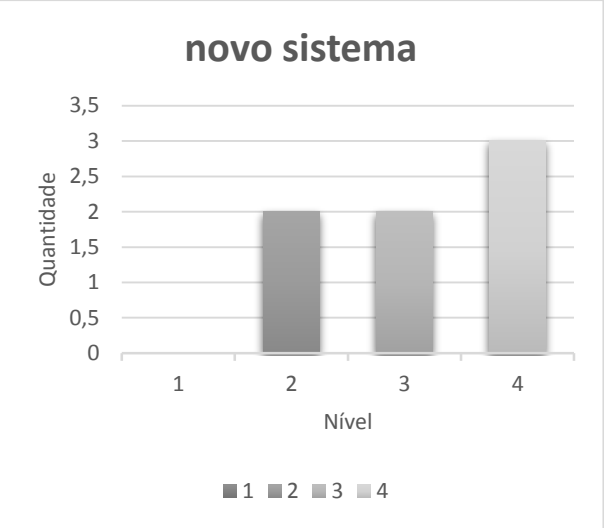


Figura 46 - Nível de Maturidade de Integridade da Informação do Novo Sistema



Nos gráficos a seguir, é possível identificar que no caso de uso do sistema proprietário, 51% dos requerimentos foram classificados como de nível 1, 39% de nível 2, 9% de nível 3 e 1% de nível 4, no novo sistema, 1% dos requerimentos são de nível 1, 24% de nível 2, 28% de nível 3 e 47% de nível 4. Está claro que o novo sistema e os processos que o suportam possuem um nível de maturidade maior do que o sistema proprietário, mas considerando que o elo mais fraco da corrente define o nível de maturidade o novo sistema também foi classificado no nível 1. Na sequência serão comparados o nível de maturidade de todos os grupos de requerimentos, de maneira que será possível identificar onde será necessário investir para que o nível de maturidade do caso de uso novo sistema seja migrado para o nível 2, 3 ou 4.

Figura 47 - Nível de Maturidade do Sistema Proprietário

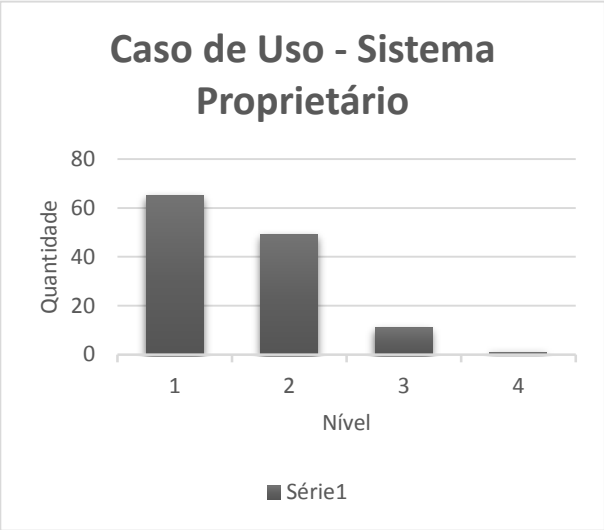
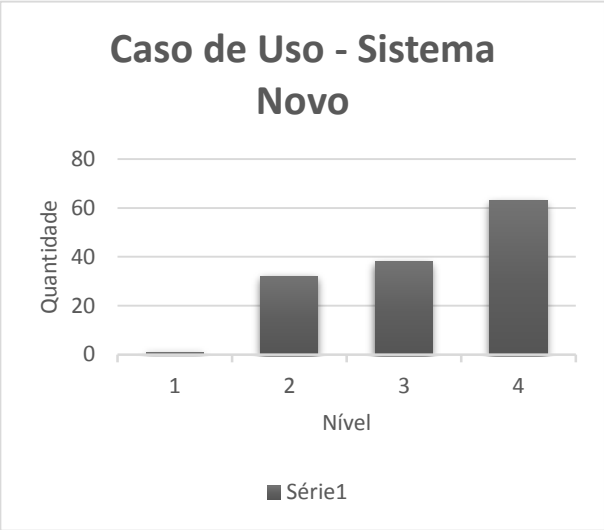


Figura 48 - Nível de Maturidade do Novo Sistema



7. CONCLUSÃO

A implantação de um modelo de identificação do nível de maturidade de segurança da informação em redes elétricas inteligentes é extremamente necessária, visto que o setor de energia está passando um momento de digitalização com a adoção de tecnologias de informação e comunicação na operação do setor elétrico.

Neste contexto, este trabalho descreveu uma metodologia para avaliação do nível de maturidade de segurança cibernéticabaseada na classificação de 16 grupo de requerimentos.

Com os resultados obtidos, foi possível identificar a eficiência do modelo, bem como a flexibilidade de aplicação em vários casos de uso, deixando bem claro que o requisito que possui o menor nível de maturidade irá definir o nível de maturidade de todo o caso de uso.

A metodologia proposta é robusta, na medida em que permite a avaliação e classificação dos requerimentos para os sistemas utilizados no gerenciamento de uma rede elétrica inteligente.

Por fim, a proposta deste trabalho também pode ser transportada com facilidade para outros sistemas inteligentes e também permite a adição de novos grupos de requisitos, que por ventura venham a se tornar relevantes no futuro, com um mínimo esforço de adaptação.

Como evolução deste trabalho, recomenda-se que sejam aprofundados os seguintes temas:

- Aplicação da metodologia em caso de uso distintos, como a rede de comunicação, equipamentos de campo, etc...
- Proposta de criação de um grupo federal para monitoramento de segurança da informação de infraestrutura urbana crítica;

7.1. Trabalhos publicados

- MACHADO, T, MOTA, A; MOTA, L, Vulnerability Analysis of IEEE802.11 Wireless Urban Networks - v2015 National Conference on Information Technology and Computer Science (CITCS 2015) ISBN: 978-1-60595-229-1

- RIBEIRO, A, MACHADO, T, MOTA, A; MOTA, L, Sistema Híbrido de Transporte de Dados Técnico Operacional, XXI SENDI, Nov/2014

- MACHADO, T, MOTA, A; MOTA,Segurança Cibernética e Privacidade na Smart Grid: Desafios e Requerimentos, BtSym Unicamp, 2015

Referências Bibliográficas

1. National institute of standards and technology nist - nistr 7628 revision 1- guidelines for smart grid cybersecurity – volume 1,2 and 3 - 2014;
2. Komninos, n, survey in smart grid and smart home security: issues, challenges and countermeasures, 2014, ieee communication surveys & tutorials, vol. 16, no. 4, fourth quarter 2014;
3. Anthony r. Metke and randy l. Ekl, security technology for smart grid networks, 2010, ieee transactions on smart grid, vol. 1, no. 1, june 2010;
4. Katherine r. Davis, a cyber-physical modeling and assessment framework for power grid infrastructures, ieee transactions on smart grid, vol. 6, no. 5, september 2015
5. Ye yan, a survey on cyber security for smart grid communications, ieee communications surveys & tutorials, vol. 14, no. 4, fourth quarter 2012
6. Elias bou-harb, communication security for smart grid distribution networks, ieee communications magazine, january 2013
7. Yilin mo, cyber–physical security of a smart grid infrastructure, proceedings of the ieee | vol. 100, no. 1, january 2012
8. Adam hahn, cyber-physical security testbeds: architecture, application, and evaluation for smart grid, ieee transactions on smart grid, vol. 4, no. 2, june 2013
9. Relatório de capacidade instalada de ee, 2014, núcleo de estudos estratégicos de energia / spe/mme
10. International energy agency, technology roadmap smart grids, oecd/iea, Paris – 2011
11. International standards organization/international electrotechnical commission, information technology—security techniques—information security management system—requirements, iso/iec 27001:2013
12. Um pouco sobre o sistema elétrico de potência. Disponível em: http://www.mundodaeletrica.com.br/um-pouco-mais-sobre-o-sistema-eletrico-de-potencia-sep/
13. DadosRelevantes NOS, 2013, Disponível em: http://www.ons.org.br/download/biblioteca_virtual/publicacoes/dados_relevantes_2013/html/07-04-novas-instalacoes-de-transmissao-2012.html?expanddiv=07
14. http://www.abradee.com.br/setor-eletrico/redes-de-energia-eletrica

15. **The world’s longest power transmission lines**, fev. 2014. Disponível em: http://www.power-technology.com/features/featurethe-worlds-longest-power-transmission-lines-4167964/

APÊNDICE 1 – Descrição do Nível de Maturidade dos Requisitos

Caso de Uso				
Requerimento	Nível 1	Nível 2	Nível 3	Nível 4
CA-1 - Política e Procedimento de Controle de Acesso	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CA-2 - Política e Procedimento de Acesso Remoto	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CA-3 - Gerenciamento de contas	Não Possui	Implantado Isoladamente	Possui Equipe de gestão de contas e Fluxo de Aprovação	Possui integração com um sistema específico de gestão de contas e acessos e integração plena com o sistema de RH
CA-4 - Imposição de Acesso	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
CA-5 - Separação de Responsabilidades	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
CA-6 - Menor Privilégio	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
CA-7 - Tentativas de Login	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
CA-8 - Controle Concorrente de Sessão	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos

CA-9 - Bloqueio de Sessão	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
CA-10 - Acesso Remoto	Não Possui	Possui autenticação	Monitora os acessos não autorizados	Possui criptografia e dupla autenticação nos acessos remotos
CA-11 - Restrições de Acesso a Rede sem Fio	Não Possui	Possui autenticação	Monitora os acessos não autorizados	Possui integração com um sistema específica de gestão de acessos
CA-12 - Controle de Acesso para Dispositivos Móveis e Portáteis	Não Possui	Possui autenticação	Possui sistema de gestão específico dos dispositivos móveis - MDM	Possui bloqueio das configurações, rede privada e limitada para todos equipamentos
CA-13 - Utilização de Sistemas de Informação Externos	Não Possui	Possui políticas e padrões de integração	Políticas e padrões revisados	Possui um sistema específico para gerenciamento centralizado das integrações
CA-14 - Senhas	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos e integração plena com o sistema de RH
CT-1 - Políticas e Procedimentos de Sensibilização e Formação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CT-2 - Conscientização da Segurança a Informação	Não Possui	Divulga manuais e procedimentos	Executa palestras constantes	Investe em palestras e informações externas para os colaboradores
CT-3 - Treinamento de Segurança da Informação	Não Possui	Divulga manuais e procedimentos	Executa palestras constantes	Investe em palestras e informações externas para os colaboradores
CT-4 - Contato com Associações e Grupos de Segurança	Não Possui	Possui acesso a fóruns e grupos online	Participa de um grupo nacional	Participa de um grupo internacional

AR-1 - Políticas e Procedimentos de Auditoria e Responsabilidade	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
AR-2 - Eventos Auditáveis	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-3 - Conteúdo dos Registros Auditados	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-4 - Monitoramento, Analise e Relatório de Auditoria	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-5 - Ferramenta de Análise e Geração de Relatórios de Auditoria	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-6 - Proteção das Informações de Auditoria	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-7 - Retenção de Registros de Auditoria	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AR-8 - Condução de Auditorias Frequentes	Não Possui	Auditoria já realizada	Auditorias internas frequentes	Auditorias internas e externas frequentes para manter certificações
AR-9 - Qualificação do Auditor	Não Possui	Possui auditor interno	Possui auditor interno específico	Possui departamento de auditoria com diversas especialidades distintas
AR-10 - Conformidade com Políticas de Segurança	Não Possui	Compliance com as políticas internas	Compliance com as políticas nacionais	Compliance com as políticas internacionais
AR-11 - Geração de registro auditáveis	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos

AR-12 - Não Repúdio	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de contas e acessos
AA-1 - Avaliações de Segurança e Políticas e Procedimentos de Autorização	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
AA-2 - Avaliação de Segurança	Não Possui	Avaliação já executada	Possui um plano com escopo definido	Avalia os relatórios e atualiza o plano frequentemente
AA-3 - Melhoria Contínua	Não Possui	Implanta as lições aprendidas internamente	Implanta as lições aprendidas da indústria	Patrocina simulações de invasão ao seu próprio ambiente
AA-4 - Conexões do Sistema de Informação da Smart Grid	Não Possui	Possui todas as conexões documentadas	Monitoras as conexões entre os sistemas	Possui um sistema centralizado de gestão das conexões entre sistemas.
AA-5 - Monitoramento Contínuo	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de monitoramento a nível de serviço e impacto
GC-1 - Políticas e Procedimentos de gerenciamento de configuração	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GC-2 - Linha de Base de Configuração	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão linha de base
GC-3 - Controle de Alterações de Configuração	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de gestão de configuração de sistemas e equipamentos
GC-4 - Monitoramento de Alteração de Configurações	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de monitoramento de alterações de configurações

GC-5 - Restrição de Acesso para Alteração de Configurações	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de restrição de controle de alterações
GC-6 - Inventário de Componentes	Não Possui	Implantado Isoladamente	Revisados constantemente	Possui integração com um sistema específico de inventário de componentes
GC-7 - Inclusão, Remoção e Eliminação dos Equipamentos	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GC-8 - Plano de Gerenciamento de Configuração	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CO-1 - Políticas e Procedimento de Continuidade de Operação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CO-2 - Plano de Continuidade da Operação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CO-3 - Papéis e Responsabilidades da Continuidade das Operações	Não Possui	Possuem papéis e responsabilidades definidos	Possui responsáveis definidos	Possui os líderes definidos
CO-4 - Treinamento de Continuidade da Operação	Não Possui	Documentos existentes e disponíveis	Documentos atualizados frequentemente	Treinamento executados constantemente com todas as partes envolvidas
CO-5 - Plano de teste da Continuidade da Operação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CO-6 - Atualização de Plano de Continuidade da Operação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
CO-7 - Site de Armazenamento Alternativo	Não Possui			
CO-8 - Serviço de Telecomunicações Alternativo	Não Possui	Possui serviço de telecomunicações alternativo parcialmente redundante	Possui serviço de telecomunicações alternativo totalmente redundante e	Possui serviço de telecomunicações alternativo totalmente redundante e com o chaveamento automático

			com o chaveamento manual	
CO-9 - Centro de Controle Alternativo	Não Possui	Possui Centro alternativo, totalmente dependente do principal	Possui Centro alternativo, totalmente independente do principal e que garante a continuidade dos principais processos	Possui Centro alternativo, totalmente independente do principal e que garante a continuidade de todos os processos
IA-1 - Políticas e Procedimentos de Identificação e Autenticação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
IA-2 - Gerenciamento do Identificador	Não Possui	Utiliza certificados digitais para garantir o remente e o destinatário das mensagens	Possui um entidade certificadora interna	Possui um entidade certificado pública
IA-3 - Gerenciamento do Autenticador	Não Possui	Possui sistema de autenticação para os usuários	Possui sistema de autenticação para os dispositivos	Possui sistema centralizado específica de autenticação e procedimentos e normas.
IA-4 - Identificação e Autenticação do usuário	Não Possui	Identifica os usuários de maneira única	Não possui usuários genéricos	Possui sistema centralizado específica de autenticação e identificação e procedimentos e normas.

IA-5 - Identificação e Autenticação de Dispositivos	Não Possui	Identifica os dispositivos de maneira única	Não possui dispositivos genéricos	Possui sistema centralizado específica de autenticação e identificação e procedimentos e normas.
IA-6 - Resposta de Autenticação	Não Possui	O sistema de autenticação fornece resposta aos usuários	O sistema de autenticação fornece resposta aos dispositivos	Sistema de autenticação fornece resposta criptografada aos usuários
GI-1 - Políticas e Procedimentos de Gerenciamento de Documentos e Informações	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GI-2 - Retenção de Documentos e Informações	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GI-3 - Manuseio da Informação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GI-4 - Troca de Informações	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GI-5 - Rotulagem Automatizada	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
RI-1 - Políticas e Procedimentos de Resposta a Incidentes	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
RI-2 - Papéis e Responsabilidades de Resposta a Incidentes	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
RI-3 - Treinamento de Resposta a Incidentes	Não Possui	Divulga manuais e procedimentos	Executa treinamento constantes com as partes interessadas	Executa Simulações de incidentes periodicamente
RI-4 - Teste de Resposta a Incidentes	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
RI-5 - Monitoramento de Incidentes	Não Possui	Monitora incidentes isoladamente	Monitora os incidentes nos	Monitoramento com base no impacto financeiro

			serviços de negócio	
RI-6 - Relatório de Incidentes	Não Possui	Gera relatórios dos incidentes isoladamente	Gera relatórios com uma periodicidade pré-definida	Possui um dono para o processo de geração de relatórios de incidentes
RI-7 - Investigação e Análise de Resposta a Incidentes	Não Possui	Atua somente no reestabelecimento pontual	Soluciona a causa raiz do problema	Identifica, soluciona e documenta a causa raiz do problema
RI-8 - Ações de Correção	Não Possui	Implanta as ações de correção	Implanta as ações previamente aprovadas	Implanta as correções utilizando um processo de gestão de mudanças e gestão de configuração
RI-9 - Backup do Sistema de Informação da Smart Grid	Não Possui	Executa backups isolados	Possui Replicação de dados e processo de restauração manual	Possui Replicação de dados e processo de restauração automático
RI-10 - Coordenação de Resposta a Incidentes	Não Possui	Possui os coordenadores pré-definidos	Possui os coordenadores pré-definidos e sempre disponíveis	Possui treinamento em períodos pré-determinados
SF-1 - Políticas e Procedimentos de Segurança Física e da Ambiente	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
SF-2 - Autorização de Acesso Físico	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
SF-3 - Acesso Físico	Não Possui	Possui controle de acessos manual	Possui controle de acessos automático e eletrônico	Possui controle de acesso com dupla proteção e liberado após aprovação

SF-4 - Monitoramento de Acesso	Não Possui	Possui controle manual isolado	Possui controle informatizado	Possui equipe específica para este processo
SF-5 - Controle de Visitantes	Não Possui	Possui controle manual isolado	Possui controle informatizado	Possui equipe específica para este processo
SF-6 - Registro de Visitantes	Não Possui	Possui controle manual isolado	Possui controle informatizado	Possui equipe específica para este processo
SF-7 - Retenção de Log de Acesso Físico	Não Possui	Possui controle manual isolado	Possui controle informatizado	Possui equipe específica para este processo
PL-1 - Plano de Segurança para Sistemas de Informação de Smart Grid	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
PL-2 - Regras de Acompanhamento	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
PL-3 - Avaliação de Impacto e Privacidade	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
SP-1 - Políticas e Procedimentos de Segurança Pessoal	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
SP-2 - Desligamento de Pessoas	Não Possui	Possui controle manual isolado	Controle feito por grupo de acessos	Controle integrado ao sistema de RH
SP-3 - Transferência de Pessoas	Não Possui	Possui controle manual isolado	Controle feito por grupo de acessos	Controle integrado ao sistema de RH
SP-4 - Termo de Acesso	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GR-1 - Políticas e Procedimentos de Gestão e Avaliação de Riscos	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GR-2 - Nível de Impacto	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
GR-3 - Avaliação de Vulnerabilidades	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente

AS-1 - Políticas e Procedimentos para Aquisição de Serviços	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
AS-2 - Políticas de Segurança para Contratados e Terceirizados	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
AS-3 - Aquisições	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
AS-4 - Softwares de Usuários	Não Possui	Possui as licenças e instaladores	Possui os instaladores armazenados e organizados em área central	Possui self service e controle automatizado de licenças
AS-5 - Princípios de Segurança para Engenharia	Não Possui			
AS-6 - Gestão de Configuração para Desenvolvimento de Sistemas	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
AS-7 - Testes de Desenvolvimento	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-1 - Políticas e Procedimentos de Proteção da Comunicação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
PC-2 - Separação das Comunicações	Não Possui	Possui rede de perímetro segregada	Possui rede da operação segregada	Possui segregação de rede por serviço/solução
PC-3 - Isolamento de Funções de Segurança	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-4 - Proteção de ataques de Negação de Serviço	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-5 - Priorização de Recursos	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-6 - Proteção de Fronteira	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica

PC-7 - Integridade da Comunicação	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-8 - Confidencialidade na Comunicação	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-9 - Caminho Seguro	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-10 - Criação e Gestão de Chave de Criptografia	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-11 - Transmissão de Parâmetros de Segurança	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-12 - Infraestrutura de Certificados de Chave Pública	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-13 - Códigos Móveis	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-14 - Voz Sobre Internet Protocol (IP)	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-15 - Conexões Entre Sistemas	Não Possui	Possui utilizando diversos protocolos	Organizada em um protocolo padrão	Possui solução de Midware corporativa
PC-16 - Funções de Segurança	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-17 - Autenticidade de Mensagem	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-18 – Serviço de Resolução de Nome e Endereço Seguro	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica

PC-19 - Aplicações Independentes de Sistemas Operacionais	Não Possui	Aplicações independentes dos sistemas operacionais de desktop	Aplicações independentes dos sistemas operacionais de dispositivos móveis	Aplicações independentes dos sistema operacionais de desktops, servidores e dispositivos móveis
PC-20 - Heterogeneidade	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-21 - Tecnologias de Virtualização	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
PC-22 - Particionamento de Aplicações	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-1 - Políticas e Procedimento de Integridade da Informação	Não Possui	Implantada e Disponível	Possuem donos definidos	Revisados e Testados Continuamente
II-2 - Falha e Remediação	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-3 - Proteção de Códigos Maliciosos e SPAM	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-4 - Ferramentas e Técnicas de Monitoramento	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-5 - Restrições e Alertar de Segurança	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-6 - Integridade de Software e Informações	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica
II-7 - Validação de Entrada de Informações	Não Possui	Possui controle isolado	Possui controle centralizado	Possui política e solução específica