GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

METODOLOGIA PARA AVALIAÇÃO DE RISCO CIBERNÉTICO EM MICROGRIDS

EDMAR CANDEIA GURJÃO(1);RAFAEL GOMES BENTO(2);UBIRATAN ALVES DO CARMO(1);LUIZ ANTONIO DE SOUZA RIBEIRO(3)
IATI(1);CPFL PAULISTA(2);FUNDACAO UNIVERSIDADE FEDERAL DO MARANHAO(3)

RESUMO

Micro e nano redes tem riscos cibernéticos relacionados aos sistemas de potência e acrescentam novos. Neste trabalho propomos uma metodologia que se baseia em análise em várias dimensões (Físico, Cibernético, Comunicação e Interdependência entre Sistema) quantificando o risco. O processo proposto parte de uma análise inicial (risco absoluto), atribuí probabilidade da ameaça, e vulnerabilidade associadas e ao final do processo, tem-se o valor para o Risco, e em paralelo o custo para a implementação das contramedidas. São apresentados dois estudos de caso, em ambos observa-se que a metodologia proposta permite analisar o impacto técnico e econômico das contramedidas propostas para diminuir o risco da microrede.

PALAVRAS-CHAVE

1.0 INTRODUÇÃO

Risco é uma ameaça que explora alguma vulnerabilidade que pode causar prejuízo a um ativo [1]. O gerenciamento de risco é o processo de identificar, controlar e minimizar o impacto de eventos incertos, e é dividido em análise de risco, avaliação de risco, minimização e avaliação de vulnerabilidades e controles. O objetivo é permitir o balanço operacional e econômico eficiente no custo das ações protetivas necessárias para garantir que se atinja a efetividade do projeto.

A análise de risco identifica e avalia fatores que podem comprometer um projeto de atingir seus objetivos, ajudando a definir medidas preventivas para reduzir a probabilidade de ocorrência desses fatores, e identificar contramedidas para tratar as consequências quando esses fatores ocorrem. A avaliação de risco calcula o risco como uma função dos ativos, ameaças e vulnerabilidades. A mitigação de risco é a implementação de proteções e controles para prevenir a ocorrência dos riscos identificados e de meios de recuperação quando o risco se torna realidade.

Neste trabalho é proposta uma metodologia para a avaliação de risco considerando os aspectos de segurança cibernética de redes elétricas de médio e pequeno porte denominadas de microrredes e nanorredes, e doravante citadas apenas como microrredes, que segundo a definição do Departamento de Energia (DOE) dos Estados Unidos, consistem de um grupo de cargas e fontes de energia distribuídos com limites elétricos claros que agem como uma única entidade controlável em relação ao sistema elétrico [2].

A metodologia proposta permite a partir da mensuração do risco, avaliar as opções de redução desse valor considerando os aspectos técnico e financeiro.

2.0 AVALIAÇÃO DE RISCO

Ameaça (*Threats*) é aquilo que pode prejudicar, destruir ou interromper a operação da microrrede, e é do que se deseja proteger. Vulnerabilidade são fragilidades na infraestrutura ou nos processos, que quando exploradas se tornam ameaças. Risco é uma função das ameaças pela exploração das vulnerabilidades, e no caso das microrredes tanto podem ser influenciados pelos componentes individuais como pela sua interligação em um sistema. Ameaças e vulnerabilidades são quantificadas pela possibilidade de ocorrência usando uma escala qualitativa (alto, médio ou baixo) ou quantitativa (1 a 10, sendo 1 pouco provável e 10 muito provável). Os valores podem ser obtidos de dados históricos ou indicados por um especialista no sistema. A quantificação do risco é feita pela multiplicação entre a possibilidade da ameaça pela probabilidade do risco e o impacto, ou seja

Fator de Risco = Probabilidade de ameaça *x* Probabilidade da vulnerabilidade *x* Impacto da vulnerabilidade

2.1 Análise de riscos em micro e nanorredes

Considerando que as microrredes são em essência sistemas elétricos de potência em escala reduzida e com dinâmicas distintas dos grandes sistemas, tem-se que essas redes herdam os riscos relacionados a esses sistemas e acrescentam novos. No caso das microrredes há características que não necessariamente estão presentes nos sistemas de potência tradicionais, que são discutidas a seguir.

Uma microrrede pode conter geradores de energia renováveis (solar, eólico, etc.) ou não renováveis (gerador a Diesel, Hidrogênio, Gás, etc.), armazenamento de energia (baterias, células de carga, etc.), um sistema supervisório e integração em rede, todos nas mais diversas escalas. Além disso pode haver cargas críticas ou não críticas.

Há ainda a possibilidade de a microrrede funcionar desconectada do sistema elétrico (modo ilhado) ou conectada ao sistema elétrico da distribuidora de energia local, podendo consumir ou fornecer energia ao sistema. Essas redes usam tecnologias diversas, e embora obedeçam a regulamentação de instalação da concessionária são operadas e gerenciadas por proprietários particulares. Mostra-se que as microrredes são sistemas Ciber-Físicos muito sensíveis, pois a parte física é influenciada pela parte cibernética devido aos múltiplos pontos de conexão interna e externa [3], e por esse motivo os intrusos têm mais chances de causar problemas [4].

Pode-se dividir a preocupação com a segurança cibernética das microrredes em duas categorias, uma relacionada ao funcionamento da microrrede como unidade autônoma (estando ou não no modo ilhado), e outra quando se tem um conjunto de microrredes que devem ser coordenadas conjuntamente para atender uma determinada demanda. Essas categorias têm sido estudadas, sendo a primeira mais bem explorada [5], e a segunda com estudos recentes [6].

2.2 Ameaças e vulnerabilidades

O primeiro passo para a análise de risco de um sistema é a definição de sua arquitetura, para em seguida identificar os pontos de falha, e assim determinar as estratégias de mitigação.

Embora o objetivo deste trabalho seja a segurança cibernética, é importante que os aspectos físicos e de comunicação sejam analisados para a análise de risco mais completa. Muitos trabalhos a segurança cibernética consideram que ao analisar os aspectos de comunicação de dados englobam os efeitos das demais ameaças, , neste trabalho os diversos aspectos estão separados para o melhor detalhamento das ameaças, vulnerabilidades e, principalmente, das contra medidas.

a) Ameaças Físicas: são aquelas relacionadas à estrutura física da microrrede, e podem ser naturais quando ocasionadas pelos eventos advindos do ambiente em que a microrrede está instalada, tais como inundações, terremotos, raios, incêndios e mudanças climáticas, ou induzidas pelo ser humano, podendo ser desde ação física como roubo, vandalismo, ou até mesmo via indução de ondas eletromagnéticas para interferir no funcionamento (jamming) dos equipamentos.

b) Ameaças Cibernéticas: Estão relacionadas às estruturas lógicas na microrrede, e normalmente são relacionados com Disponibilidade, Integridade e Confidencialidade, ou tríade CIA como é como é conhecida. Um exemplo de um ataque contra a disponibilidade é Negação de Serviço (DoS – Denial of Service). Contra a integridade um atacante pode alterar o Sistema de Nomes de Domínios (DNS – Domain Name Service) para que os elementos da microrrede acessem sites falsos, e contra a confidencialidade tem-se o acesso às informações de consumo do usuário.

c) Ameaças à Comunicação: Estão relacionadas aos meios de comunicação usados pelos componentes da microrrede, ou entre microrredes. A utilização cada vez maior de redes de comunicação tem tornado as microrredes cada vez mais vulneráveis. Nesse ponto deve-se considerar que a microrrede deve ter a habilidade de se ilhar quando houver problemas de comunicação.

d) Ameaças a Interdependência entre sistemas: Em conjunto com os segmentos de óleo, gás natural, transporte, telecomunicações e água, a eletricidade forma a infraestrutura crítica cujos elementos são interdependentes. Assim, o risco em um desses sistema pode se transportar para os demais.

2.3 - Contramedidas

Definidas as ameaças e vulnerabilidades pode-se identificar contramedidas para mitigá-los. Nesse ponto deve-se ter em mente que implementar formas de mitigação a ponto de não haver riscos, embora seja possível, é

contraproducente pois pode impor um conjunto tão grande de restrições e com um custo tão alto que inviabiliza o propósito do negócio sendo protegido [7]. Portanto, o objetivo das contramedidas é reduzir o risco a um nível aceitável.

Como já afirmado, cada microrrede tem configuração particular, e por esse motivo os riscos e contramedidas devem ser avaliados caso a caso. Porém é possível estabelecer regrais gerais que podem ser adaptadas às particularidades. Na Tabela 1 estão listados alguns exemplos de ações para aumentar a resiliência da microrrede.

Atributo	Qualidade	Exemplo
Robustez	- Segurança física - Segurança cibernética - Reforço na infraestrutura - Monitoramento do desempenho	- Monitoramento ativo e passivo - Manutenção e uso de checklists - Proteção física contra acessos não autorizados - Controles de acesso as instalações e à elementos da rede
Redundância	- Eliminar pontos únicos da falha	- Modularização das unidades para facilitar o gerenciamento e manutenção - Linhas de alimentação e comunicação redundantes - Backup de dados e de pessoal
Reforço	- Disponibilidade de geradores de energia - Armazenamento	- Diversidade de fontes de geração de energia e armazenamento - Desconexão de cargas para priorizar as mais críticas - Uso de UPS – Uninterruptable power supply
Resposta	- Automação - Auto ajuste - Previsão - Indicadores de desempenho - Treinamento e exercícios	- Treinamento contínuo das pessoas envolvidas - Coleta de dados e análise preditiva - Tolerância a falhas - Sistema de controle inteligentes - Procedimentos documentados
Recuperação	- Componentes padronizados - Inventário de componentes extras - Priorização no religamento	- Atualização contínua dos inventários de componentes extras, preferencialmente usando componentes de prateleira - Sequência de religamento bem definida

Tabela 1 – Princípios e exemplos para aumento da resiliência em microrredes

As técnicas de mitigação podem ser, de forma genérica, classificadas em planejamento pré-desastre, medição durante o desastre, e recuperação e restauração pós desastre.

Na fase de planejamento um conjunto de estratégias de mitigação devem ser consideradas para primordialmente tornar os ativos físico e lógicos menos vulneráveis, e podem ser categorizadas como reforço no sistema e nos procedimentos operacionais.

As contramedidas devem estar disponíveis e serem tecnicamente fáceis de implementar, pois além da parte técnica, deve-se considerar o aspecto financeiro. Dependendo do que for especificado, pode ser difícil justificar o investimento, principalmente se não houver uma medida objetiva, além do valor financeiro, que permita demonstrar o ganho em termos de risco.

3 Metodologia para Gerenciamento de Risco em Microrredes

Como já discutido, o gerenciamento de risco é realizado em etapas, e no caso específico das microrredes há particularidades que aumentam a complexidade da tarefa. Na busca de uniformizar a análise, nesta seção é proposta uma metodologia que permite, além do gerenciamento, quantificar em termos monetários a utilização de contramedidas para diminuir o risco em uma microrrede.

A metodologia proposta está representada na Figura 1, e se baseia no princípio de analisar os fatores de risco (Físico, Cibernético, Comunicação e Interdependência entre Sistema) e em seguida obter um valor para o risco. Como ainda não há contramedidas, o valor obtido representa o maior risco e é absoluto, ou seja, não há, a priori, como compará-lo com um valor de outra microrrede pois foi calculado para a uma configuração específica.

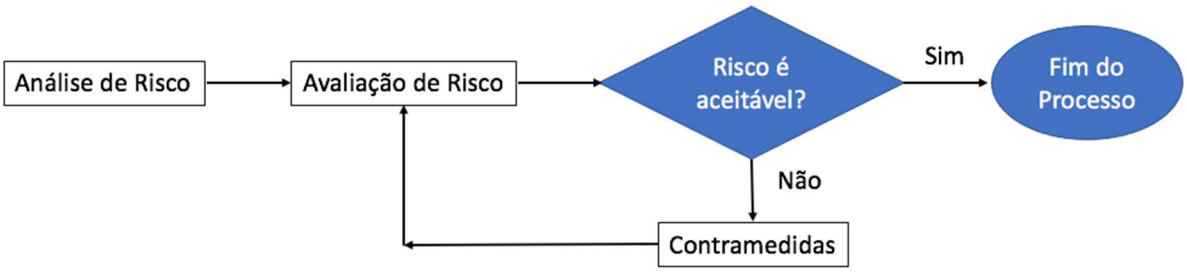

Figura 1 – Fluxograma da metodologia proposta para avaliação de risco em microrredes.

Para cada ameaça são atribuídas a probabilidade da ameaça, a probabilidade de a vulnerabilidade ocorrer e o seu impacto. Esse valor é um número inteiro, numa escala de 0 a 9, sendo o valor 0 quando não se aplica e 9 o maior valor de risco. A escala procura refletir um valor de probabilidade, sendo 0 improvável e 9 muito provável. No contexto de análise de risco não faz sentido 100% de probabilidade. Também como já discutido, a quantificação de algumas vulnerabilidades é difícil, e nesses casos usa-se os atributos Alto, Médio e Baixo, para os quais foram associados os valores 9, 5 e 1, respectivamente.

Caso o Risco obtido seja aceitável, o processo termina. Caso contrário, são estabelecidas contramedidas explicitando as suas ações, como podem reduzir as ameaças e os respectivos custos. Em seguida, a avaliação do risco é revisitada, e o novo risco calculado, e segue-se o ciclo até que o risco seja aceitável. Ao final do processo, tem-se o valor para o Risco, e em paralelo o custo para a implementação das contramedidas. Neste ponto pode-se fazer a avaliação da prioridade de implementação das contramedidas, com base no impacto do risco e no custo associado.

O termo aceitável, em destaque no parágrafo anterior, deve ser entendido como um valor indicativo do risco que se aceita conviver, ou o valor do risco cujo custo para atingir está dentro do orçamento.

Os procedimentos apresentados na Seção 2.3 devem ser fortemente considerados quando da atribuição de contramedidas, tanto por estarem bem estabelecidos quanto por facilitarem a quantificação do risco aqui proposta.

A metodologia apresentada pode ser adaptada, por exemplo pelo estabelecimento de um conjunto mínimo de vulnerabilidades que devem servir de referência para obter o valor de risco inicial comparável entre microrredes.

Na próxima seção são apresentados alguns estudos de caso utilizando a metodologia proposta.

4 RESULTADOS

Nesta seção são apresentados estudos de caso aplicando a metodologia proposta. Cabe salientar que em todos os exemplos, tanto as topologias quanto a atribuição de valores foram criados com intuito de exemplificação, e que o estudo de risco em microrredes, como já salientado, precisa ser feito caso a caso e tomando proveito dos dados históricos e da experiência sobre o sistema.

4.1 Caso 1

Seja a microrrede representada na Figura 2, na qual há geração local por painéis fotovoltaicos, unidade de armazenamento de energia e duas cargas, tendo a Carga 1 maior prioridade que a Carga 2. A microrrede funciona no modo ilhado, porém compartilha a rede de dados com a do local onde está instalada, que por sua vez tem conexão com a Internet. Esse local por sua vez se localiza em uma avenida com pouco movimento.

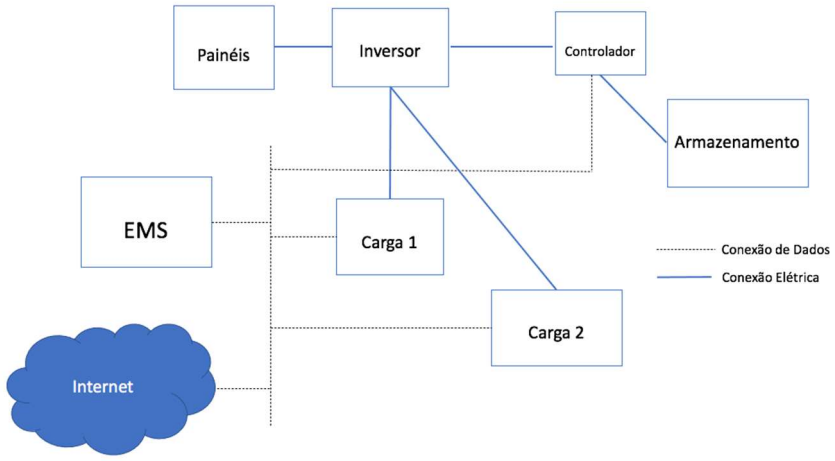

Figura 2 – Diagrama microrrede para Estudo de Caso 1. (EMS – Energy Management System)

Análise de risco:

1) Físico:

F1: Ameaça: Inundação;
Vulnerabilidade: a localidade onde a microrrede está instalada é uma área de alagamento;
F2: Ameaça: Vandalismo;
Vulnerabilidade: os equipamentos da microrrede ficam visíveis às pessoas externas;

2) Cibernético

CS1: Ameaça: Quebra de senha de acesso à rede;
Vulnerabilidade: uso de senhas fracas;

CS2: Ameaça: Ataque de negação de serviço;
Vulnerabilidade: a rede interna não tem proteção de acessos externo;

3) Comunicação

Com1: Ameaça: perda de comunicação entre os nós da rede interna;
Vulnerabilidade: a rede interna é sem fio, e pode ser desconectada;

4) Interdependência entre sistemas

IS: Não se aplica (NSA), a microrrede funciona somente no modo ilhado.

Avaliação do risco:

Ameaça	Probabilidade de ameaça (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Probabilidade da vulnerabilidade ocorrer (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Impacto da Vulnerabilidade (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Descrição	Contribuição para o Risco
F1	H	H	H	As inundações ocorrem anualmente.	= 9*9*9 = 729
F2	H	M	H	Há histórico de roubos de equipamentos.	= 9*5*9 = 405
CS1	H	M	H	Pode dar acesso interno à rede.	= 9*5*9 = 405
CS2	H	L	M	A rede não representa grande atrativo para agentes externos	= 9*1*5= 45

Com1	M	M	M	A rede interna não oferece atrativos	=5*5*5= 75
IS	NSA	NSA	NSA	A rede não tem conexão com outros sistemas	0
Risco total					1.695

Tabela 2 – Valoração inicial do risco.

Os valores atribuídos a cada um dos itens na Tabela 2 não precisam se resumir aos associados a H, M e L, podem ser atribuídos outros valores na escala de 0 a 9, e isso pode ser feito com base em dados históricos ou pela experiência da equipe.

O valor do Risco Total de 1.695 não tem um significado absoluto, nem unidade. Servirá como referência para avaliar o quanto as ações propostas reduzem o risco. Por exemplo, consideremos que as contramedidas abaixo descritas sejam adotadas, e o reflexo na matriz de risco e no risco total.

1) Físico:

F1: Ameaça: Inundação;
Vulnerabilidade: a localidade onde a microrrede está instalada é uma área de alagamento;
Contramedida: Reforço na estrutura de contenção de águas.
Custo: R$ 10.000,00

F2: Ameaça: Vandalismo;

Vulnerabilidade: os equipamentos da microrrede ficam visíveis às pessoas externas;
Contramedida: uso de cerca elétrica e telas para proteção;
Custo: R$ 3.000,00

2) Cibernético

CS1: Ameaça: Quebra de senha de acesso à rede;
Vulnerabilidade: uso de senhas fracas;
Contramedida: Nenhuma.
Custo: 0

CS2: Ameaça: Ataque de negação de serviço;
Vulnerabilidade: a rede interna não tem proteção de acessos externo;
Contramedida: Uso de Firewall na entrada da rede;
Custo: R$ 2.500,00

3) Comunicação

Com1: Ameaça: perda de comunicação entre os nós da rede interna;
Vulnerabilidade: a rede interna é sem fio, e pode ser desconectada;
Contramedida: Nenhuma;
Custo: 0

4) Interdependência entre sistemas

IS: Não se aplica, a microrrede funciona somente no modo ilhado.

Após aplicadas as contramedidas, pode-se reavaliar o risco, como mostrado na Tabela 3.

Ameaça	Probabilidade de ameaça (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Probabilidade da vulnerabilidade ocorrer (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Impacto da Vulnerabilidade (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Contribuição para o Risco	Custo da Contramedida (R$)
F1	H	L	H	= 9*1*9 = 81	10.000,00
F2	H	2	H	= 9*2*9 = 162	3.000,00

CS1	H	M	H	= 9*5*9 = 405	-
CS2	H	0	M	= 9*0*5= 0	2.500,00
Com1	M	M	M	=5*5*5= 75	-
IS	NSA	NSA	NSA	0	-
Risco total				723	
Custo					15.500,00

Tabela 3 – Valoração da aplicação das contramedidas.

Cada um dos fatores de risco pode ser detalhado pelos especialistas na área, por exemplo, os riscos cibernéticos podem ser analisados em mais detalhes usando o modelo DREAD, como exemplificado na Tabela 4.

Categoria	Valor	Justificativa
Damage	5	Neste campo deve-se colocar as justificativas para a atribuição dos valores.
Reproducibility	5	
Exploitability	5	
Affected Users	10	
Discoverability	10	
Score do Risco	= (5+5+5+5+5)/5 = 5	

Tabela 4 – Atribuição de valores para o impacto do ataque de negação de servi no contexto do estudo de caso.

4. 2 Caso 2

Tomemos proveito da microrrede analisada no Caso 1, porém agora acrescentando o fato que pode haver conexão com a rede da distribuidora. Nesse cenário os riscos já descritos na seção anterior se mantêm, porém deve ser acrescentado tanto o risco de Interconexão com outros sistemas quanto a injeção de dados falsos. Ou seja, devem ser acrescentados:

CS3: Ameaça: Injeção de dados falsos de geração ;
Vulnerabilidade: a rede interna não tem proteção de acessos externos, um atacante pode injetar dados falsos de geração;

CS4: Ameaça: Injeção de dados falsos de geração ;
Vulnerabilidade: Não há mecanismo para validar os dados de geração de energia que são registrados pelo inversor;

E deve ser modificado:

IS: Não se aplica, a microrrede funciona somente no modo ilhado.

Para IS1: Ameaça: Conexão com a rede quando não há geração extra;
Vulnerabilidade: Sistema pode ser enganado pelos dados falsos injetados;

Que devem ser acrescentadas à matriz de avaliação do risco, gerando a Tabela 5.

Ameaça	Probabilidade de ameaça (0 a 9) ou (H – 9, M – 5, L - 1, NSA – 0)	Probabilidade da vulnerabilidade ocorrer (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Impacto da Vulnerabilidade (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Descrição	Contribuição para o Risco
F1	H	H	H	As inundações ocorrer anualmente.	= 9*9*9 = 729
F2	H	M	H	Há histórico de roubos de equipamentos.	= 9*5*9 = 405
CS1	H	M	H	Pode dar acesso interno à rede.	= 9*5*9 = 405
CS2	H	L	M	A rede não representa	= 9*1*5= 45

				grande atrativo para agentes externos	
CS3	M	L	H	A rede não representa grande atrativo para agentes externos	= 5*1*9 = 45
CS4	M	L	H	A rede não representa grande atrativo para agentes externos	= 5*1*9 = 45
Com1	M	M	M	A rede interna não oferece atrativos	=5*5*5= 75
IS1	M	L	H	A rede não tem conexão com outros sistemas	= 5*1*9 = 45
Risco total					1.830

Tabela 5 - Valoração da aplicação das contramedidas para o segundo caso.

Pode-se utilizar as contramedidas

CS3: Ameaça: Injeção de dados falsos de geração ;
Vulnerabilidade: a rede interna não tem proteção de acessos externo, um atacante pode injetar dados falsos de geração;
Contramedida: Uso de Firewall na entrada da rede;
Custo: R$ 2.500,00
Contramedida: Sistema de detecção de intrusos;
Custo: R$ 1.500,00

CS4: Ameaça: Injeção de dados falsos de geração ;
Vulnerabilidade: Não há mecanismo para validar os dados de geração de energia que são registrados pelo inversor;
Contramedida: Exigência de geradores calibrados;
Custo: R$ 1.000,00

IS1: Ameaça: Conexão com a rede quando não há geração extra;
Vulnerabilidade: Sistema pode ser enganado pelos dados falsos injetados;
Contramedida: Utilização de equipamento para validar a possibilidade de conexão;
Custo: R$ 1.000,00

Ameaça	Probabilidade de ameaça (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Probabilidade da vulnerabilidade ocorrer (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Impacto da Vulnerabilidade (0 a 9) ou (H – 9, M – 5, L -1, NSA – 0)	Contribuição para o Risco	Custo da Contramedida (R$)
F1	H	L	H	= 9*1*9 = 81	10.000,00
F2	H	2	H	= 9*2*9 = 162	3.000,00
CS1	H	M	H	= 9*5*9 = 405	-
CS2	H	0	M	= 9*0*5= 0	2.500,00
CS3	L	L	H	= 1*1*9 = 9	= 0 + 1.500,00 = 1.500,00
CS4	L	L	H	= 1*1*9 = 9	1.00,00
Com1	M	M	M	=5*5*5= 75	-
IS1	L	L	H	=1*1*9 = 9	1.000,00
Risco total				750	
Custo					19.000,00

Tabela 6 – Custo total associado à inclusão das contramedidas.

Vale observar que em CS3 o custo de utilizar Firewall não foi considerado, visto que já foi adicionado em CS2.

5.0 CONCLUSÔES

A avaliação de risco é a etapa em que se quantifica o Risco, e nela devem ser levados em conta os diversos aspectos que influenciam no funcionamento da entidade sob análise. Devido à diversidade de variáveis, realizar a avaliação de risco pode ser uma tarefa complexa.

Neste trabalho foi proposta uma metodologia para avaliação de risco cibernético em microrredes, considerando várias dimensões (física, comunicação, cibernética e interdependência entre sistemas) de tal forma que partindo de dados históricos, ou do conhecimento sobre o sistema, é possível obter um valor de referência para o risco, e em seguida avaliar a influência das contramedidas nesse valor, obtendo-se simultaneamente o custo das medidas adotadas.

Utilizando dois exemplos como estudo de caso foi possível demonstrar a utilização da metodologia, e observar que esse uso permite que contramedidas possam ser priorizadas. A metodologia proposta pode ser adaptada ao caso específico de uma microrrede, como também evoluir para incluir outros fatores não considerados nesse trabalho.

6.0 Bibliografia

[1] T. R. Peltier, Information Security Risk Analysis, Aurbach Publications, 2005.

[2] Executive Office of the President, “Economic Benefits of Increasin Electrical Grid Resilience to Waether Outages,” 2013.

[3] M. Rekik, Z. Chtourou, C. Gransart e A. Atieh, “A Cyber-Physical Threat Analysis for Microgrids,” em 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Hammamet, 2108.

[4] M. M. Rana, L. Li e S. W. Su, “Cyber attack protection and control of microgrids,” IEEE/CAA Journal of Automatica Sinica, vol. 5, pp. 602-609, Março 2018.

[5] J. Stamp, C. K. Veitch, J. Henry e D. H. Hart, “Microgrid Cyber Security Reference Architecture (V2),” New Mexico, 2015.

[6] “Cybersecurity of Networked MIcrogrids: Challenges, Potential Solutions, and Future Directions,” Albuquerque, New Mexico, USA, 2020.

[7] T. R. Peltier, Information Security Risk Analysis, Auerbach Publicaitions, 2005.

[8] S. Mishra, K. Anderson, B. Miller, K. Boyer e A. Warren, “Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies,” Applied Energy, vol. 264, Abril 2020.

[9] D. O. Duggan, S. R. Thomas e C. K. e. a. Veitch, “Cathegorzing Threat: Building and Using a Generic Threat Model,” Sando National Laboratories, Albuquerque, 2007.

[10] D. o. D. (DOD), “Information Assurance (IA) Implementation,” 2003.

[11] N. I. o. S. a. T. (NIST), “Guidelines for Smart Grid Cyber Security,” 2010.

7.0 Agradecimentos

Os autores agradem ao programa P&D&I ANEEL através do projeto PD-00063-3058/2019, à Companhia Paulista de Força e Luz (CPFL), Universidade Estadual de Campinas (UNICAMP), Universidade Federal do Maranhão (UFMA) e ao Instituto Avançado de Tecnologia e Inovação (IATI).

DADOS BIOGRÁFICOS

Doutor em Engenharia Elétrica pela Universidade Federal de Campina Grande - UFCG (2003). Atualmente é professor Associado do Departamento de Engenharia Elétrica da UFCG e professor colaborador do Mestrado Profissional em Ciência e Tecnologia em Saúde da Universidade Estadual da Paraíba. Tem experiência na área de Engenharia Elétrica, com ênfase em Amostragem Compressiva (Compressed Sensing), Rádio Definido por Software, Processamento de Sinais e Aplicações de Álgebra Linear. Senior Member do IEEE, membro da Sociedade Brasileira de Telecomunicações (SBrT) e do CIGRÉ. Co-autor dos livros Introdução à Análise de Sinais e Sistemas, Elsevier, 2015, e Digital Signal Processing, Momentum Press, 2018.

(2) RAFAEL GOMES BENTO
Analista de Projetos de Inovação na CPFL - Companhia Paulista de Força e Luz. Possui formação técnica em eletroeletrônica pelo Colégio Técnico de Campinas (2008) e graduação em Engenharia Elétrica com ênfase em Telecomunicações pelo Centro Universitário Salesiano de São Paulo (2015). Atua na prospecção, formatação e gerenciamento de projetos de inovação tecnológica no âmbito do Programa de P&D do Setor de Energia Elétrica, regulado pela ANEEL, com foco em projetos voltados ao segmento de distribuição de energia.

(3) UBIRATAN ALVES DO CARMO
UBIRATAN ALVES DO CARMO - Doutor em Ciências da Computação pela Universidade Federal de Pernambuco (2017), mestre em Ciências da Computação pela Universidade Federal de Pernambuco (2003), especialização em Telecomunicações pela Universidade Federal Fluminense (2006) e graduado em Engenharia Elétrica pela Universidade Federal de Pernambuco (1979). Atua na área de P&D, como pesquisador associado, do Instituto Avançado de Tecnologia e Inovação (IATI) com ênfase em segurança cibernética em sistemas de automação industriais (ICS). Membro do Cigré com participações nos SC-B5/D2. Atuação em redes de computadores, sistemas de automação de subestação, protocolos industriais, segurança cibernética e sistemas SCADA

(4) LUIZ ANTONIO DE SOUZA RIBEIRO
Doutor (1998) e mestre (1994) em Engenharia Elétrica pela Universidade Federal da Paraíba (1994), graduação em Engenharia Elétrica pela Universidade Federal do Maranhão (1990). De 1991 a 2008 trabalhou no departamento de engenharia Elétrica do CEFET. Durante o período de 2004 a 2006 foi pesquisador na Universidade de Wisconsin, Madison, Estados Unidos. Durante o ano de 2015 foi pesquisador na Universidade de Aalborg, Dinamarca. Desde 2008 é professor adjunto no Departamento de Engenharia Elétrica da Universidade Federal do Maranhão. Suas áreas de interesse são sistemas de controle, conversores de potência, microrredes, acionamentos de máquinas elétricas e fontes renováveis de energia.