| Resultado da aplicação do Método de Identificação de Riscos Ciberfísicos (MIRC) | | | |
|---|---|---|---|
| **Ativo** | Planta de Energia Fotovoltaica | | |
| **Sistema** | Sistema fotovoltaico composto por paineis fotovoltaicos, inversores e gateway ModBus TCP. | | |
| **ID** | **Método** | **Componente** | **Lista de Risco** |
| 1. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A presença de rachaduras e fissuras nos painéis solares pode gerar hot spots (pontos quentes) , resultando na redução na eficiência de geração de energia na área afetada e aumentando o risco de incêndios. |
| 2. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A presença de sombras por sujeira acumulada nas placas solares pode impedir a captação da luz solar, resultando na reduçaõ da produção de energia elétrica. |
| 3. | Diagnóstico de risco por fatores | Painel fotovoltaicos | Paineis fabricados com materiais inadequados ou de baixa qualidade pode levar à corrosão interna dos painéis solares, resultando na deterioração das células solares rapidamente e, or sua vez, a diminuição da capacidade de conversão de luz solar em eletricidade. |
| 4. | Diagnóstico de risco por fatores | Painel fotovoltaicos | O furto de placas solares ou suas peças resulta em perdas financeiras, mal funcionamento do sistema, e prejudica a eficiência na geração de energia. |
| 5. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A exposição dos painéis solares a condições climáticas adversas, como chuvas de granizo, nevascas, tempestades de vento e furacões, pode resultar em danos físicos aos componentes do sistema, incluindo a criação de novos caminhos de circuito, curtos-circuitos, incêndios, perda parcial ou total da funcionalidade do dispositivo e redução na eficiência na geração de energia. |
| 7. | Diagnóstico de risco por fatores | Painel fotovoltaicos | Condições climáticas adversas ou extremas, como nevascas, chuvas de granizo, tempestades de vento e furacões, podem causar danos físicos aos painéis solares, resultando em danos físicos (perda parcial ou total da funcionalidade do dispositivo). |
| 8. | Diagnóstico de risco por fatores | Painel fotovoltaicos | Defeitos de fabricação podem causar contato elétrico entre as células fotovoltaicas, modificando a curva característica de corrente e tensão do módulo, resultando em impactos negativos no seu desempenho do painel. |
| 9. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A utilização de materiais de baixa qualidade na fabricação dos módulos fotovoltaicos pode facilmente afetar a superfície do painel, gerando camadas de óxido que desgastam a superfície, resultando na diminuição da vida útil do painel. |
| 11. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A exposição do painel fotovoltaico a locais com alta umidade (>0,85%) pode causar danos às células, como perda de aderência do encapsulamento, permitindo maior penetração da umidade no interior do módulo, resultando no aceleramento da corrosão nos conectores e caixa de junção, aumentando o risco de curto-circuito no sistema. |
| 12. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A manutenção inadequada, realizada com o uso de ferramentas e materiais inadequados ou por profissionais inexperientes, pode resultar na quebra das conexões dos cabos, danos físicos à superfície da placa (rachaduras ou fissuras) e danos aos componentes elétricos, levando à redução da eficiência de geração de energia. |
| 13. | Diagnóstico de risco por fatores | Painel fotovoltaicos | O posicionamento da placa em áreas sombreadas pode reduzir a produção de corrente, diminuindo a produção de energia elétrica. |
| 14. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A falha na soldagem dos componentes do módulo fotovoltaico pode gerar um aumento da resistência de contato, resultando na redução na eficiência da geração de energia. |
| 15. | Diagnóstico de risco por fatores | Painel fotovoltaicos | O dimensionamento inadequado do sistema fotovoltaico, incluindo o superdimensionamento da corrente contínua ou alternada, pode causar sobrecarga no painel solar, resultando na queima dos componentes conectados ao painel, redução da vida útil do sistema, além de reduzir a eficiência na geração de energia. |
| 16. | Diagnóstico de risco por fatores | Painel fotovoltaicos | Módulos fotovoltaicos com materiais de baixa qualidade pode gerar áreas sombreadas na superfície do painel, resultando na redução da quantidade de energia gerada e na diminuição da vida útil do painel. |

| | | | |
|---|---|---|---|
| 17. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A instalação incorreta dos inversores pode levar a uma sobretensão na corrente alternada (CA), prejudicando o funcionamento dos painéis solares e reduzindo a eficiência na geração de energia. |
| 18. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A falha nos conectores e na caixa de junção dos painéis solares pode permitir a entrada de umidade, acelerando a corrosão e aumentando o risco de curto-circuito nos componentes do sistema. |
| 19. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A falta de manutenção periódica dos painéis pode levar à acumulação de sujeira, resultando em hot spots que reduzem a geração de energia local e degradam a placa |
| 20. | Diagnóstico de risco por fatores | Painel fotovoltaicos | O uso de materiais inadequados durante a manutenção, como abrasivos, pode causar danos físicos à superfície da placa, resultando em rachaduras ou fissuras que comprometem a geração de energia. |
| 23. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A sabotagem à rede elétrica pode desequilibrar a produção e distribuição de energia dos painéis fotovoltaicos, resultando em perdas financeiras, furto de energia e danos aos painéis. |
| 27 | Diagnóstico de risco por fatores | Inversor | A queima do inversor pode impedir a conversão da energia armazenada pela placa em corrente contínua (CC), resultando na ausência de geração e armazenamento de energia. |
| 29. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A manutenção preventiva realizada por profissionais inexperientes pode danificar os componentes elétricos e mecânicos do painel, resultando na redução da eficiência e a segurança do sistema de geração de energia. |
| 30. | Diagnóstico de risco por fatores | Painel fotovoltaicos | O diagnóstico ineficiente de falhas nos painéis fotovoltaicos pode levar à interrupção da geração de energia, reduzindo a eficiência do sistema e aumentando os custos de manutenção corretiva. |
| 32. | Diagnóstico de risco por fatores | Painel fotovoltaicos | A exposição dos módulos solares a temperaturas elevadas e níveis altos de tensão pode resultar na Degradação Potencial Induzida (DPI), resultando em defeitos nos materiais semicondutores e diminuindo a eficiência dos painéis. |
| 34. | Diagnóstico de risco por fatores | Inversor | A quebra do inversor pode interromper a transferência de energia para a rede e os equipamentos, resultando na redução da eficiência do sistema. |
| 35. | Diagnóstico de risco por fatores | Inversor | O superaquecimento do inversor, por falha, pode levar à deterioração rápida dos seus componentes, resultando em incêndios e necessidade de substituição frequente do equipamento. |
| 36. | Diagnóstico de risco por fatores | Inversor | Instalar o inversor em local inadequado, com exposição direta aos raios solares, pode aumentar a temperatura do inversor, resultando em sua degradação acelerada e, em casos extremos, em sua queima por sobreaquecimento. |
| 37. | Diagnóstico de risco por fatores | Inversor | Uma conexão inadequada entre os cabos de string e o inversor, juntamente com o dimensionamento de corrente inadequado, pode ocasionar falhas nas ligações elétricas, resultando no desligamento do equipamento, abertura não intencional do disjuntor e interrupção do fornecimento de energia. |
| 38. | Diagnóstico de risco por fatores | Inversor | Os leds sinalizadores do RS485 com defeito podem causar falhas de operação, resultando na má interpretação do status do equipamento, o que, por sua vez, pode levar à outras falhas. |
| 39. | Diagnóstico de risco por fatores | Inversor | O roubo do inversor pode interromper a transferência de energia para os demais dispositivos, devido à falta do equipamento, resultando na redução da eficiência do sistema e perdas financeiras. |
| 40. | Diagnóstico de risco por fatores | Inversor | A distância excessiva entre a rede de comunicação e o inversor pode causar uma grande diferença de potencial entre os locais, resultando na degração do sinal de comunicação. |
| 41. | Diagnóstico de risco por fatores | Inversor | O subdimensionamento da velocidade de comunicação do inversor e a rede pode gerar mais retransmissões, resultando no o aumento da latência no sistema de comunicação. |
| 42. | Diagnóstico de risco por fatores | Inversor | A falta de medidas de segurança adequadas, como a ausência de alteração das senhas padrão e a utilização de chaves criptográficas padrão do fabricante, pode aumentar a probabilidade de violação não autorizada, possibilitando o acesso a informações confidenciais e o possível roubo de informações sensíveis. |

| | | | |
|---|---|---|---|
| 44. | Diagnóstico de risco por fatores | Inversor | A falta de um sistema de detecção de intrusão, como alarmes e sensores, pode impedir a identificação e monitoramento de violações no inversor, permitindo acesso silencioso aos dados. |
| 45. | Diagnóstico de risco por fatores | Inversor | A sobretensão que ultrapassa o limite estabelecido na especificação técnica pode causar danos nos componentes do inversor, resultando em mau funcionamento ou até mesmo na queima do equipamento. |
| 46. | Diagnóstico de risco por fatores | Inversor | A ausência de verificação da integridade e falhas nos processos de carregamento de software sem padronização podem possibilitar a manipulação ou exclusão de dados, resultando na perda de precisão, consistência e confiabilidade da atualização realizada. |
| 47. | Diagnóstico de risco por fatores | Inversor | A ausência de chaves criptográficas ou a utilização de chaves padrões do fabricante podem comprometer seriamente a segurança dos dados, resultando no acesso não autorizado e o roubo de informações sensíveis. |
| 48. | Diagnóstico de risco por fatores | Inversor | Problemas nas conexões e prensas de cabos podem causar resistência elétrica, resultando em perdas de energia e diminuição da eficiência do sistema. |
| 49. | Diagnóstico de risco por fatores | Inversor | A falta de manutenção nas proteções elétricas, como disjuntores e fusíveis, pode diminuir a eficiência desses dispositivos em proteger o sistema elétrico em caso de fuga de corrente elétrica ou falhas de isolamento, aumentando a vulnerabilidade do sistema elétrico a problemas de segurança elétrica. |
| 50. | Diagnóstico de risco por fatores | Inversor | A falta de manutenção adequada nos componentes do inversor, como o ventilador, grade, trocador de calor e filtro, pode interferir na dissipação de calor adequada e gerar acúmulo de poeira no equipamento que aumenta a temperatura interna do equipamento, resultando em desligamentos automáticos frequentes e aumento dos gastos com manutenção corretiva. |
| 51. | Diagnóstico de risco por fatores | Inversor | A falta de manutenção geral do inversor fotovoltaico, incluindo a detecção de danos ou rompimentos em componentes, pode interferir na conversão de energia e no funcionamento geral do equipamento, resultando em desligamento, redução no desempenho, perda de potência ou, em casos extremos, gerar incêndios. |
| 52. | Diagnóstico de risco por fatores | Inversor | O grampeamento da rede de comunicação pode permitir o controle de vários inversores conectados ao barramento, resultando em possíveis manipulações dos sinais de controle enviados aos inversores. |
| 53. | Diagnóstico de risco por fatores | Inversor | A ausência de verificação da autenticidade da carga de software pelo inversor pode permitir a instalação de versões adulteradas do firmware, resultando no acesso indevido e malicioso a informações privadas e possibilita a transmissão e recebimento de dados não autorizados. |
| 54. | Diagnóstico de risco por fatores | Inversor | A instalação ou reposicionamento inadequado do inversor fotovoltaico pode resultar em risco de choque elétrico para quem realiza a instalação e a perda da funcionalidade dos componentes elétricos. |
| 55. | Diagnóstico de risco por fatores | Inversor | O diâmetro inadequado dos cabos pode gerar à queda de tensão e reduzir a eficiência da conversão de corrente, resultando na perda de potência do sistema. |
| 57. | Diagnóstico de risco por fatores | Inversor | A presença de um arquivo malicioso na carga de software pode comprometer o funcionamento dos softwares gerenciadores responsáveis pelos comandos do inversor, como o Aurora Manager, resultando no controle e gerenciamento indevido das informações do inversor. |
| 58. | Diagnóstico de risco por fatores | Inversor | A instalação inadequada da comunicação de rede, como a instalação de dois RS485/Modbus-RTU mestres na mesma rede, pode levar a intermitencia de rede, resultando em parada de funcionamento do inversor e interrupção do fornecimento de energia. |
| 59. | Diagnóstico de risco por fatores | Inversor | A instalação incorreta de cabos de comunicação junto aos cabos de energia pode resultar em interferência no cabos, resultando em mal funcionamento da rede como um todo. |

| | | | |
|---|---|---|---|
| 60. | Diagnóstico de risco por fatores | Inversor | Não seguir as orientações do fabricante e normas técnicas pode levar ao dimensionamento inadequado de corrente elétrica do inversor, resultando no risco de descargas elétricas e incêndios. |
| 61. | Diagnóstico de risco por fatores | Inversor | O dimensionamento de corrente inadequado pode provocar a abertura não intencional do disjuntor, resultando na interrupção do fornecimento de energia, danos ao equipamento e riscos elétricos para os profissionais responsáveis pela manutenção do sistema fotovoltaico. |
| 62. | Diagnóstico de risco por fatores | Inversor | Dimensionamento inadequado do inversor (inclinação superior a 5º na vertical) pode reduzir a capacidade de geração de energia do sistema fotovoltaico, resultando em menor eficiência na conversão de energia, consequentemente, na geração de energia elétrica. |
| 63. | Diagnóstico de risco por fatores | Inversor | A instalação de inversores na vertical com inclinação superior a 5° pode dificultar a dissipação adequada de calor dos componentes, levando ao superaquecimento do equipamento e aumentando o risco de incêndio. |
| 65. | Diagnóstico de risco por fatores | Inversor | A instalação do inversor em locais com alta umidade e vedação inadequada dos cabos pode permitir a fuga de corrente elétrica, resultando em baixa resistência de isolamento do equipamento, risco de choque elétrico, além de acelerar a corrosão dos componentes elétricos, reduzindo a vida útil do equipamento. |
| 66. | Diagnóstico de risco por fatores | Inversor | Arcos elétricos elevam a temperatura dos componentes, excedendo limites técnicos, causando desgaste prematuro, falhas, e reduzindo a eficiência e vida útil do equipamento. |
| 67. | Diagnóstico de risco por fatores | Inversor | O envelhecimento dos inversores e seus componentes ao longo do tempo pode gerar desgastes decorrente do tempo de uso do equipamento, resultando falhas de funcionamento e custo com manutenções corretivas. |
| 68. | Diagnóstico de risco por fatores | Inversor | A falta de manutenção regular nos componentes do inversor, como o ventilador, grade, trocador de calor e filtro, pode gerar acúmulo de poeira no equipamento, resultando na redução da eficiência de resfriamento que reduzem a vida útil do inversor e aumenta os gastos com manutenção corretiva. |
| 69. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | O superaquecimento do gateway acima dos limites da especificação técnica pode levar à degradação acelerada dos componentes eletrônicos, resultando na redução na eficiência do equipamento e aumentando o risco de incêndios. |
| 70. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A instalação inadequada do inversor e do gateway, além de configurações errôneas de rede, drivers e configurações específicas, pode comprometer as funcionalidades e integridades do sistema fotovoltaico, prejudicando o controle, monitoramento e comunicação entre dispositivos, resultando em baixo desempenho geral e perda de dados. |
| 71. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Um defeito nos LEDs sinalizadores do gateway pode levar a indicações incorretas sobre seu funcionamento, resultando em falhas que comprometem tanto a eficiência quanto a integridade do hardware. |
| 72. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | O furto do hardware do gateway pode desabilitar a conversão do protocolo ModBus TCP para RTU, essencial para a integração de equipamentos que usam diferentes protocolos, prejudicando a comunicação e a segurança da planta. |
| 73. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A ausência de medidas de segurança adequadas, como a falta de um firewall com proxy e a falta de proteção de rede cabeada, pode permitir o acesso não autorizado a informações do sistema supervisório e da rede, resultando em risco à integridade e disponibilidade da informação, facilitando a instalação de malware e softwares mal-intencionados. |
| 74. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Problemas na conexão de cabos, como danos ou desconexões, podem comprometer a comunicação entre o sistema supervisório, os inversores e o gateway, resultando na perda de dados importantes, na impossibilidade de atualização do software e no controle e monitoramento inadequado dos inversores. |

| | | | |
|---|---|---|---|
| 75. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de senha para autorizar alterações de firmware pode facilitar a ação de hackers, comprometendo a segurança e privacidade das informações, além de permitir o roubo de dados. |
| 76. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Uma intrusão em uma rede cabeada pode permitir acesso não autorizado e imediato a todas as informações do gateway, resultando na facilitação da instalação de malware e software mal-intencionado. |
| 77. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de mecanismos de autenticação de origem, como o IP Spoofing, pode permitir a falsificação dos endereços IP de origem de outros hosts, resultando no acesso não autorizado a dados confidenciais associados a esses endereços IP. |
| 78. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Autenticação e criptografia frágeis podem levar a ataques de desincronização na comunicação TCP, permitindo a captura e controle de conexões de terceiros, comprometendo informações sensíveis e colocando em risco a segurança da rede. |
| 79. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A utilização de números iniciais de sequência previsíveis pode levar ao TCP Sequence Number Prediction, permitindo a geração de pacotes maliciosos direcionados a um determinado host, resultando na manipulação do tráfego de rede, roubo de informações, injeção de pacotes falsos ou até mesmo negação de serviço (DoS). |
| 81. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de criptografia na comunicação pode possibilitar o Source Routing attack, permitindo que um atacante monitore e intercepte as comunicações na rede, obtendo acesso a informações confidenciais e comprometendo a segurança da rede como um todo. |
| 83. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Uma ação de ataque DoS ou a transmissão em grande escala de pacotes SYN com endereço IP falsificado pode ocasionar o consumo excessivo de recursos, resultando em sua inoperância. |
| 85. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Manutenções inadequadas no gateway podem alterar suas configurações, resultando em falhas operacionais e possíveis violações de segurança. |
| 86. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A desconexão ou dano de cabos ou conexões durante a manutenção pode interromper a comunicação do gateway com outros dispositivos de rede, resultando na perda de dados ou informações importantes armazenadas no gateway. |
| 87. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de habilidades técnicas e a utilização de ferramentas inadequadas durante a manutenção do gateway pode agravar as falhas já existentes no dispositivo, resultando no aceleramento da deterioração da integridade do sistema. |
| 88. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A perda de dados armazenados no gateway durante a manutenção pode comprometer a integridade das informações, afetar a produtividade e segurança do sistema, além de resultar em prejuízos financeiros e paralisação de processos. |
| 91. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Um acesso físico ao gateway por agentes maliciosos pode permitir a substituição do dispositivo por um hardware adulterado, resultando em perdas financeiras, comportamento anômalo e acesso não autorizado aos dados do proprietário original. |
| 93. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de verificação da autenticidade e integridade da carga de software pode possibilitar a instalação de um software malicioso no gateway, acarretando na vulnerabilidade e comprometimento da segurança. |
| 94. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Falhas durante a carga de software podem causar interrupções no serviço ou vulnerabilidades de segurança no gateway. |
| 95. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de padronização nos processos de carga de software pode levar a um aumento de custos e tempo de manutenção, resultando em uma diminuição da eficiência, segurança e confiabilidade do sistema. |
| 96. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A falta de atualização de software e firmware pode deixar o gateway vulnerável a ataques conhecidos, que poderiam ser evitados por meio da aplicação de patches de segurança. |

| | | | |
|---|---|---|---|
| 97. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | A instalação inadequada do gateway e a configuração errônea de rede, drivers e configurações específicas podem gerar problemas na comunicação entre dispositivos, resultando em perda de dados, atrasos na transmissão de informações e falhas ou interrupções na comunicação. |
| 98. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | Redes RS485 com endereços Modbus diferentes configurados incorretamente podem levar a problemas de comunicação, como interrupções e falhas na comunicação entre dispositivos. |
| 99. | Diagnóstico de risco por fatores | Gateway (ModBus TCP) | O envelhecimento natural do hardware, incluindo cabos, pode resultar em falhas na comunicação do protocolo Modbus TCP para RTU, resultando na interrupção da comunicação ou à perda de pacotes de dados. |
| 100. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | O aumento da temperatura ambiente acima dos limites especificados pode causar estresse térmico na placa fotovoltaica, resultando em danos físicos e maiores custos com manutenção e substituição. |
| 101. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | Condições climáticas extremas, como nevascas, podem causar a redução da temperatura ambiente abaixo dos limites especificados, resultando no resfriamento excessivo das células fotovoltaicas e na quebra ou fissuração das placas, impactando negativamente a eficiência da geração de energia do painel. |
| 103. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | A redução da temperatura ambiente abaixo dos limites especificados pode causar o resfriamento excessivo das células fotovoltaicas, resultando na quebra ou fissuração das placas e, por consequência, reduz a eficiência da geração de energia do painel. |
| 104. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | Zonas com alta umidade relativa do ar (>0,85%) podem causar condensação de água no interior das células fotovoltaicas, reduzindo o isolamento térmico e aumentando o risco de choques elétricos. |
| 105. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | Zonas com alta umidade relativa do ar pode levar à oxidação e corrosão dos cabos na planta de energia fotovoltaica. |
| 106. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | Tensões acima do limite especificado podem causar sobretensões no sistema de energia fotovoltaica, resultando em danos irreparáveis às células solares e levando a curtos-circuitos e incêndios. |
| 107. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | A velocidade de impacto de pedras de granizo acima de 50 mph pode causar micro trincas ou fissuras nas células fotovoltaicas, reduzindo sua resistência mecânica e aumentando o risco de curtos-circuitos no sistema. |
| 108. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | O acúmulo excessivo de neve nos painéis fotovoltaicos pode danificar as células fotovoltaicas, reduzindo a capacidade do sistema de gerar energia. |
| 109. | Estratégia bottom-up do Hazop | Painel fotovoltaicos | Condições climáticas extremas, como ventos fortes acima do limite especificado, podem levar à perda de fixação dos painéis e danos internos nas células fotovoltaicas, resultando em perda de eficiência na geração de energia. |
| 110. | Estratégia bottom-up do Hazop | Inversor | O aumento da corrente contínua além dos limites técnicos especificados pode causar sobretensão, resultando no desligamento do inversor e possíveis curtos-circuitos. |
| 111. | Estratégia bottom-up do Hazop | Inversor | Presença de defeitos nos circuitos elétricos do inversor pode ocasionar uma subtensão na corrente contínua, resultando numa tensão de entrada insuficiente para alimentar o sistema de armazenamento de energia. |
| 112. | Estratégia bottom-up do Hazop | Inversor | A falta de aterramento elétrico pode comprometer a proteção contra correntes de fuga e descargas atmosféricas, resultando em danos aos equipamentos e riscos de acidentes elétricos. |
| 113. | Estratégia bottom-up do Hazop | Inversor | Sobredimensionamento da potência pode gerar uma potência de saída menor do que a potência de entrada, resultando no maior tempo de operação prolongado do inversor com menor eficiência e perda de energia elétrica. |
| 114. | Estratégia bottom-up do Hazop | Inversor | A elevação da corrente alternada acima dos limites técnicos especificados e infraestrutura inadequada podem gerar sobretensão de corrente alternada, resultando no desligamento do inversor fotovoltaico ou na queima de equipamentos eletrônicos conectados à rede. |

| | | | |
|---|---|---|---|
| 115. | Estratégia bottom-up do Hazop | Inversor | A redução da tensão de alimentação dos equipamentos pode gerar subtensão de corrente alternada, o que pode resultar na interrupção do funcionamento ou na queima de equipamentos conectados. |
| 116. | Estratégia bottom-up do Hazop | Inversor | O aumento da frequência acima do limite da especificação técnica, geralmente causado por um excesso de oferta de energia em relação à demanda, pode causar desconexões de rede, resultando no desligamentos em massa do inversor fotovoltaico e dos equipamentos conectados a ele. |
| 117. | Estratégia bottom-up do Hazop | Inversor | Mudanças climáticas, instalação inadequada e dimensionamento inadequado podem causar superaquecimento do inversor, resultando em uma redução na potência gerada pelo sistema, além de, em casos extremos, provocar o desligamento total do inversor. |
| 118. | Estratégia bottom-up do Hazop | Inversor | O resfriamento excessivo do inversor, geralmente por mudanças climáticas como nevascas, pode ocasionar falhas nos sensores de temperatura e corrosão nos componentes metálicos, comprometendo o funcionamento adequado do equipamento e acarretando perdas econômicas para o sistema fotovoltaico. |
| 119. | Estratégia top-down do NIST CSF | Inversor | A falta de um inventário de ativos, papéis e responsabilidades definidos pode comprometer o gerenciamento de ativos, autorização de acesso, identificação de responsáveis, mapeamento, documentação e tratamento de incidentes de segurança cibernética. |
| 120. | Estratégia top-down do NIST CSF | Inversor | Ausência de inventário dos softwares podem comprometer o gerenciamento de softwares e identificação de proprietários. |
| 121. | Estratégia top-down do NIST CSF | Inversor | A falta de mapeamento da comunicação organizacional e do fluxo de dados pode dificultar o processo de gerenciamento dos dispositivos, resultando em menor proteção contra ataques aos serviços de rede. |
| 122. | Estratégia top-down do NIST CSF | Inversor | Ausência de processos e ferramente de monitoramente de ameaças e a falta classificação da informação, podem dificultar a detecção de ameaças à segurança da rede e a gestão eficaz da informação. |
| 123. | Estratégia top-down do NIST CSF | Inversor | Ausência de requisitos de segurança e controles para gestão, podem dificultar o gerenciamento e controle da segurança da informação |
| 124. | Estratégia top-down do NIST CSF | Inversor | Ausência de padrões para relatar incidentes e procedimentos de resposta a eles, podem comprometer a resposta e gestão de incidentes |
| 125. | Estratégia top-down do NIST CSF | Inversor | Ausência de papeis e responsabilidade definidos, podem dificultar o mapemanto, documentação e tratamento de incidentes de segurança cibernética |
| 126. | Estratégia top-down do NIST CSF | Inversor | Ausência de requisitos de identificação, avaliação e plano de tratamento de riscos, podem dificultar o gerenciamento de riscos de segurança cibernética |
| 127. | Estratégia top-down do NIST CSF | Inversor | Ausência de informações de vulnerabilidades e ferramentas para análise de conformidade de sistemas e redes, podem dificultar o gerenciamento de vuneralidades e a análise de conformidade |
| 128. | Estratégia top-down do NIST CSF | Inversor | Ausência de fóruns especializados para mapeamento de ameaças cibernéticas podem dificultar a genciamento dessas ameaças |
| 129. | Estratégia top-down do NIST CSF | Inversor | Ausência de indentificação e documentação de ameaças internas podem reduzir a integridade do ativo |
| 130. | Estratégia top-down do NIST CSF | Inversor | Ausência de gestão de vulnerabilidades técnicas e restrições quanto à instalação de softwares podem dificultar a coleta de informações sobre essas vulnerabilidades e dificultar a definição de critérios para instalação de softwares |
| 131. | Estratégia top-down do NIST CSF | Inversor | Ausência do plano de tratamento de risco podem dificultar a definição sobre a forma, processo e controles para tratamento dos riscos de segurança da informação |
| 132. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | A falta de um inventário de ativos, papéis e responsabilidades definidos pode comprometer o gerenciamento de ativos, autorização de acesso, identificação de responsáveis, mapeamento, documentação e tratamento de incidentes de segurança cibernética. |

| | | | |
|---|---|---|---|
| 133. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de inventário dos softwares podem comprometer o gerenciamento de softwares e identificação de proprietários |
| 134. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência do mapeamento de comunicação organizacional e fluxo de dados podem dificultar o amplo gerenciamento dos dispositivos e ataques contra serviços de rede. |
| 135. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de processos e ferramente de monitoramente de ameaças e a falta classificação da informação, podem dificultar a detecção de ameaças à segurança da rede e a gestão eficaz da informação. |
| 136. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de requisitos de segurança e controles para gestão, podem dificultar o gerenciamento e controle da segurança da informação |
| 137. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de padrões para relatar incidentes e procedimentos de resposta a eles, podem comprometer a resposta e gestão de incidentes |
| 138. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de papeis e responsabilidade definidos, podem dificultar o mapemanto, documentação e tratamento de incidentes de segurança cibernética |
| 139. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de requisitos de identificação, avaliação e plano de tratamento de riscos, podem dificultar o gerenciamento de riscos de segurança cibernética |
| 140. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de informações de vulnerabilidades e ferramentas para análise de conformidade de sistemas e redes, podem dificultar o gerenciamento de vuneralidades e a análise de conformidade |
| 141. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de fóruns especializados para mapeamento de ameaças cibernéticas podem dificultar a genciamento dessas ameaças |
| 142. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de indentificação e documentação de ameaças internas podem reduzir a integridade do ativo |
| 143. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência de gestão de vulnerabilidades técnicas e restrições quanto à instalação de softwares podem dificultar a coleta de informações sobre essas vulnerabilidades e dificultar a definição de critérios para instalação de softwares |
| 144. | Estratégia top-down do NIST CSF | Gateway (ModBus TCP) | Ausência do plano de tratamento de risco podem dificultar a definição sobre a forma, processo e controles para tratamento dos riscos de segurança da informação |