# ANÁLISE DOS SISTEMAS DE INFORMAÇÃO DE UMA INSTALAÇÃO NUCLEAR: Um foco na segurança cibernética*

FRANÇOA **TAFFAREL** ROSÁRIO CORRÊA**
Primeiro-Tenente

**SUMÁRIO**



## INTRODUÇÃO

A evolução tecnológica dos Sistemas de Informação (SI) apresentou inovações cada vez mais importantes e de fácil compreensão para uso de computadores e dispositivos móveis. Entretanto, mesmo com os vários ganhos de flexibilidade e eficiência em diversas áreas da sociedade, esta evolução tem sido acompanhada de novos riscos devido à crescente conectividade entre os computadores, visto que a exposição de vulnerabilidades cresceu de forma proporcional em várias organizações públicas e privadas na internet, aumentando o número de ataques cibernéticos.

---

* Artigo adaptado da dissertação apresentada ao Centro de Instrução Almirante Wandenkolk como trabalho de conclusão do Curso de Aperfeiçoamento Avançado em Tecnologia Nuclear (C-ApA-TN-2020). Orientador: Capitão-Tenente (EN) Fernando Lage Araújo Schweizer, mestre em Ciências Técnicas Nucleares pela Universidade Federal de Minas Gerais.

** Formado em Ciências Navais pela Escola Naval e graduado em Sistema de Computação pela Universidade Federal Fluminense. Especialista em Segurança da Informação pela Universidade Estácio de Sá e tecnólogo nuclear formado no C-ApA-TN. Atualmente, é aluno do Curso de Pós-Graduação em Guerra Cibernética para Oficiais do Exército Brasileiro.

Com isso, a atenção à segurança da informação digital intensificou-se de forma clara e tornou-se o desafio mais importante no desenvolvimento do setor tecnologia da informação (TI). A Guerra Cibernética tem sido motivo de inquietação dos líderes de diversos países ao redor do mundo, pois o posicionamento destes é referenciado não apenas para que suas Forças Armadas estejam preparadas para uma luta bélica ou para aplicações de táticas em defesa, mas também para que detenham o conhecimento no setor de TI aplicado à segurança cibernética.

Segundo a ABNT NBR ISO/IEC 27002:

> O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos. (ABNT, 2013, p. 4)

Impende ressaltar que a informação é o ativo mais valioso possuído por uma organização, pois o valor dos documentos físicos ou digitais não é mais subavaliado por executivos sem uma análise formal e abrangente. Atualmente, esses gestores reconhecem que seus negócios são dependentes desses ativos, sejam na forma de dados brutos, sejam expostos de forma refinada.

Acresce-se a isso o fato de que, segundo Freire (2003), a sociedade utiliza a informação como um recurso estratégico para o seu desenvolvimento econômico e social, gerenciando sua influência por intermédio dos avanços tecnológicos desenvolvidos pelo setor de TI.

Neste contexto de desenvolvimento, conforme previsto em estratégias de defesa de diversos países, existe um conjunto de Infraestruturas Críticas (IC) pertencentes a setores estratégicos, como energia, transporte, abastecimento de água, telecomunicações e finanças, os quais são importantes para a estabilidade socioeconômica de um país, devendo ser defendidos e constantemente analisados no que tange à segurança dos seus sistemas para prognosticar vulnerabilidades.

**A elevação do índice de geração de energia das termonucleares ocorreu de forma diretamente proporcional ao aperfeiçoamento e à inserção de novas tecnologias da Informação em instalações nucleares**

Por conseguinte, conforme o relatório anual da empresa British Petroleum (2019) sobre as estatísticas de produção da energia, as usinas termonucleares respondem por aproximadamente 15% da geração de energia elétrica mundial e, concomitantes com outras Instalações Nucleares (IN), são consideradas as IC mais sensíveis a ataques cibernéticos, pois, segundo Sklyar (2012), um ataque bem-sucedido aos SI pode causar indisponibilidade da geração de energia ou iniciar um incidente nuclear que eleva a probabilidade de fatalidade à população e de danos ao meio ambiente em suas proximidades.

Cumpre destacar que, conforme a Associação Nuclear Mundial (WNA, 2018), a elevação do índice de geração de energia proveniente de usinas termonucleares ocorreu de forma diretamente proporcional ao aperfeiçoamento e à inserção de novas tecnologias do setor de TI em IN. Somado a isso, WNA (2019) afirma que esse índice de produção tem sido elevado devido ao fato de que estas usinas geram baixas emissões de dióxido de carbono e possuem um custo de produção menor quando comparadas às outras matrizes geradoras, devido ao alto nível de monitoramento e automação por meio de sistemas SCADA[1].

Contudo, ainda que os sistemas SCADA ofereçam aos gestores das IN menor custo e maior eficiência, gradua-se também de forma exponencial a insegurança dos sistemas devido à presença de diversos controladores lógicos programáveis, os quais podem sofrer alterações devido a uma inserção bem-sucedida de um código malicioso nos sistemas de informação.

Dessa forma, ressalta-se que órgãos reguladores internacionais de segurança nuclear e de segurança cibernética, juntamente com as agências nacionais desses setores, estão implementando regulamentações e inspeções mais rigorosas nos sistemas de informação em IN, pois, segundo a Agência Internacional de Energia Atômica (IAEA, 2013), as normas regulatórias dos principais órgãos devem ser mantidas atualizadas, a fim de diminuir os índices de incidentes cibernéticos expostos no Gráfico 1, pois é significativo e de elevada preocupação que a dependência dessas infraestruturas críticas aos SI possam elevar a probabilidade de incidentes.

Conforme afirmado pela Comissão Reguladora Nuclear (NRC, 2019), o uso de sistemas digitais em IN e radiológicas continua a aumentar. Sendo assim, é de vital importância que todos esses sistemas estejam adequadamente protegidos contra ações maliciosas em SI. Deste modo, impende ressaltar que o tema

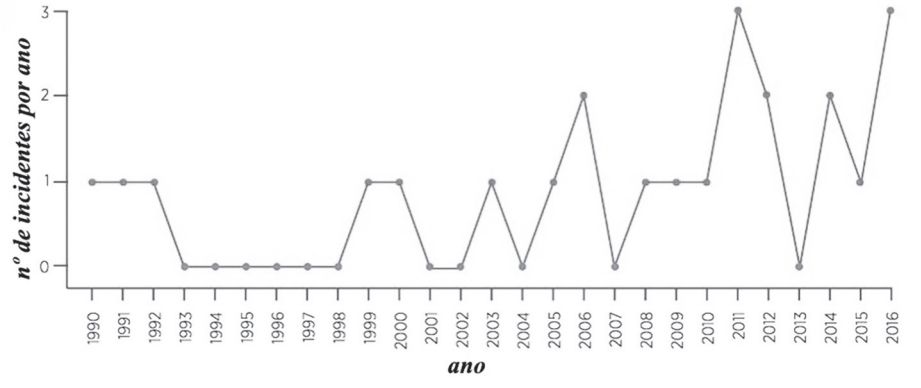



Gráfico 1 − Frequência de incidentes cibernéticos em instalações nucleares[2]
Fonte: Nixu (2017)

1 O Supervisory Control and Data Acquisition (SCADA) é um sistema que permite às organizações industriais controlar e monitorar remotamente os equipamentos vitais em tempo real.

2 Os incidentes cibernéticos em IN mostrados acima foram divulgados publicamente desde 1990. É possível que tenham ocorrido outros incidentes que não foram divulgados.

alvo deste artigo é analisar a ocorrência da indisponibilidade de uma IN a partir de um ataque cibernético, por meio do estudo dos instrumentos normativos dos principais órgãos reguladores do setor nuclear no que tange à segurança cibernética, a fim de apresentar possíveis cenários de ataque cibernético em uma instalação nuclear.

Nessa assertiva, justifica-se o tema tendo em vista o elevado número de informações, tais como os conhecimentos operacionais e tecnológicos e os direitos de propriedade científica ou intelectual encontrados nos programas, bancos de dados e sequências lógicas programáveis, os quais circulam no âmbito das IN e as tornam alvos potenciais para ataques cibernéticos.

## CONTEXTUALIZAÇÃO HISTÓRICA NORMATIVA

### *Conceituação de infraestrutura crítica*

Segundo o Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR, 2019), o termo IC refere-se a instalações físicas ou sistemas digitais que são essenciais para as operações mínimas do governo. Conforme o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (GSICI):

> As Infraestruturas Críticas (IC) são instalações, serviços, bens e sistemas que exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não. (BRASIL, 2010)

De acordo com a GSICI (2010), as áreas prioritárias das IC são: energia, transporte, água, telecomunicações e finanças. Essas áreas, nas últimas décadas, foram privilegiadas com os avanços tecnológicos que elevaram a eficiência de suas operações industriais. Assim, as IC estão se tornando cada vez mais automatizadas e interconectadas. Contudo essas melhorias introduziram vulnerabilidades adicionais novas, relacionadas a falhas nos equipamentos, erros humanos e também ameaças físicas ou digitais.

Segundo Clarke e Olcott (2012), o governo americano, por meio do Departamento de Segurança Interna (DHS), considera as IC como sistemas ou ativos vitais ao país, designando cerca de 15 setores como críticos, dos quais os principais são centrais nucleares geradoras de energia, pois a indisponibilidade dessas IN gerará um impacto negativo na segurança e na economia nacional.

Nesse sentido, é válido ressaltar também que a Comissão Europeia (2008) definiu as IC como os ativos principais da sociedade europeia, pois sua não-estabilidade pode afetar setores como energia, transporte, comunicação e serviços de emergência, prejudicando o desenvolvimento socioeconômico da Europa.

Segundo Kelly (2001), uma IC é composta de um ou mais sistemas, os quais possuem diversas funções a fim de prestar um serviço à sociedade. Conforme citado anteriormente, a sociedade depende dessas instalações, as quais, de acordo com Clemente (2013), dependem entre si umas das outras para seu próprio funcionamento, criando assim uma forte interdependência bidirecional, que pode

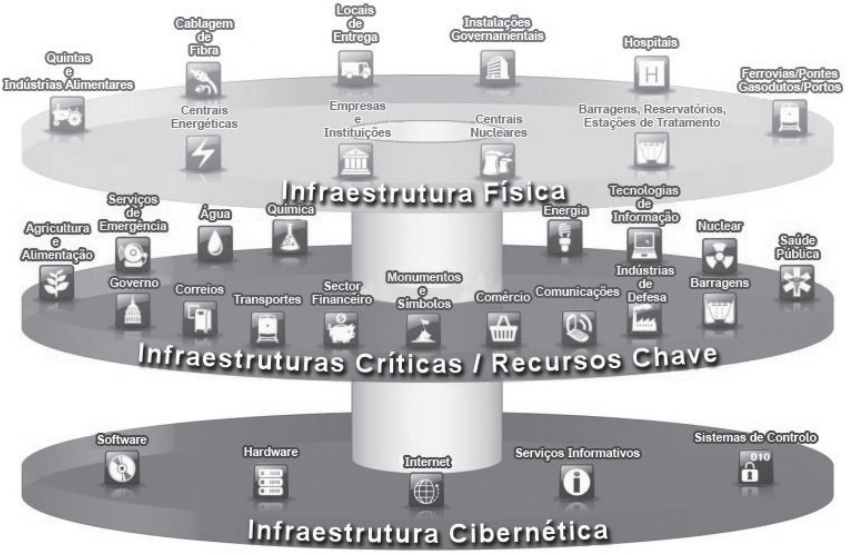



Figura 1 – As infraestruturas críticas
Fonte: Beggs (2010)

desencadear eventos significativos em uma simples falha.

Nesse contexto, segundo Pederson (2006), é indiscutível que as IC não estão isoladas e que as suas interações estão intrinsecamente ligadas em múltiplos níveis, conforme ilustrado na Figura 1, pois um impacto na disponibilidade ou integridade de uma delas levará a sérias consequências para outras IC, sejam estruturas físicas ou digitais, ocasionando efeitos dramáticos, como instabilidades sociais devido a cortes na distribuição de energia.

A asserção acima permitiu que Natário e Nunes (2014, p. 248) afirmassem que a infraestrutura cibernética é estrutura basal das interdependências das IC, influenciando "todos os setores do Estado, do domínio público ao privado, e do âmbito regional à escala global".

Dessa forma, corroborando com o exposto acima, as IN são as infraestruturas críticas de maior relevância no que tange a um ataque por meio de uma arma cibernética, pois seus sistemas de informação desempenham cada vez mais um papel fundamental relacionado às três principais funções de segurança de uma IN, que, segundo Perrota (2017), são: realizar o controle da reatividade neutrônica, manter o resfriamento do elemento combustível e garantir o confinamento de todo o material radioativo. Caso estas não sejam asseguradas, eleva-se a probabilidade de perda de vidas, destruição de propriedades e instabilidade econômica.

### *As normas da segurança da informação importantes no setor nuclear*

Na década de 90, de acordo com Fernandes e Abreu (2014), o governo britânico originou o primeiro código de prática para a gestão da segurança da informação, que foi aperfeiçoado no British Standard 7799, a fim de suprir a necessidade de proteção de informações, o qual evoluiu para o atual conjunto ISO/

EIC 27000. É válido ressaltar que, dentre as normas deste conjunto, evidenciam-se a ABNT NBR ISO/IEC 27001:2013 e a ABNT NBR ISO/IEC 27002:2013, ambas relacionadas à segurança da informação e criadas pela Organização Internacional de Normalização (ISO).

Segundo Oliveira (2015), a ABNT NBR ISO/IEC 27001 foi desenvolvida com o propósito de prover um modelo para implementar, monitorar e evoluir de forma positiva um Sistema de Gestão de Segurança da Informação. A ABNT NBR ISO/IEC 27002 atua como guia para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança.

No entanto, conforme Symonov (2018), somente a implementação dessas duas normas da série ISO/EIC 27000 na estrutura de um plano organizacional de uma IN não atendia às necessidades de proteção dos sistemas nucleares, em particular no que diz respeito à sua operação e às suas regulamentações.

Sendo assim, o setor que coordena a regulação em IN iniciou um esforço de normalização internacional em 2008, por meio do apoio em conjunto da IAEA e da International Electrotechnical Commission (IEC), com o intuito de desenvolver um conjunto de referências documentais sobre segurança cibernética para os sistemas de informação das IN. Foram emitidos diversos documentos relacionados à segurança da informação dos sistemas de controle em IN, entre os quais:

− IEC 62645 - centrais de energia nuclear, instrumentação e sistemas de controle, requisitos para programas de segurança para sistemas baseados em computador;

− IEC 60880 - centrais de energia nuclear, sistemas de instrumentação e controle importantes para a segurança, aspectos de *software* para sistemas baseados em computador executando funções de categoria A;

− IEC 61226 - centrais de energia nuclear, instrumentação e controle importantes para a segurança, classificação das funções de instrumentação e controle; e

− IEC 62859 - centrais de energia nuclear, sistemas de instrumentação e controle, requisitos para a coordenação de segurança nuclear e segurança cibernética.

Cumpre destacar que a IEC 62645 foi o primeiro documento da IAEA/IEC visando principalmente à segurança cibernética, sendo desenvolvido com base nos padrões exigidos da Norma ISO/IEC 27001, tendo como função estabelecer requisitos e fornecer orientação para o desenvolvimento e o gerenciamento de programas eficazes de segurança dos computadores nas IN.

É válido salientar que o documento mais recente, a IEC 62859, datado de 2016 e que trata da coordenação entre segurança nuclear e segurança cibernética para sistemas de controle, foi elaborado de forma a maximizar a segurança nuclear, bem como difundir ações e procedimentos organizacionais para garantir proteção dos sistemas de controle, incluindo prevenção, detecção e reação a ataques digitais durante todo o ciclo de vida da IN. Segundo esta norma, os principais requisitos e recomendações são:

> Com base na segurança nuclear, deve-se: (i) integrar a segurança cibernética na estrutura organizacional e nos sistemas de controle das IN; (ii) evitar possíveis conflitos entre disposições de segurança nuclear das instalações e a segurança cibernética; e (iii) auxiliar na identificação e no aproveitamento das sinergias potenciais entre segurança e segurança cibernética. (IEC 62859, 2016, p. 5)

Segundo a IEC 62859 (2016), o binômio segurança da informação e segurança nuclear tende a contribuir com os esforços globais para alcançar uma segurança efetiva, fornecendo modelo de gerenciamento das interações do binômio.

Dessa forma, a intenção da IAEA/IEC é garantir que as normas norteadoras facilitem a coordenação entre a segurança cibernética e recursos de sistemas de controle, de forma que a implementação da segurança não impacte negativamente no desempenho, na confiabilidade, na operação e na segurança nuclear.

Em consonância com o acatado, o desenvolvimento dessas diretrizes de segurança cibernética específicas do setor nuclear influenciou na criação de outras orientações regulatórias e estruturas modelos de políticas de segurança da informação, as quais podem ser agrupadas em três categorias organizacionais em geral: IAEA, NRC e DHS.

A IAEA publicou três documentos que norteiam a segurança nos sistemas de informação no setor nuclear; seu propósito principal é elevar o nível qualitativo das orientações técnicas, das recomendações e dos guias de implementação no que tange à segurança cibernética.

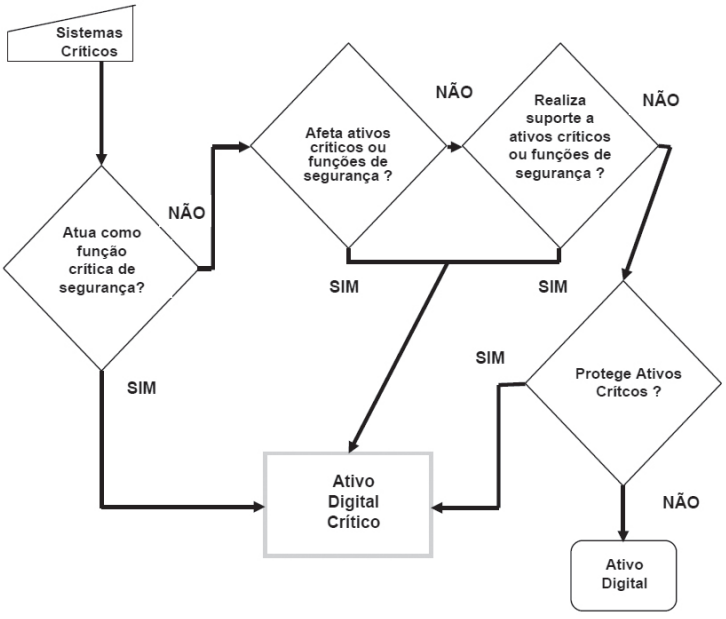
Assim, destaca-se a publicação chamada Série de Segurança Nuclear nº 17 da IAEA, que trata da segurança de sistemas de informação em IN, sendo fundamentada na série ISO/IEC 27000 e nas contribuições de um grande número de especialistas dos Estados membros da IAEA, em virtude de suas experiências e práticas nas áreas de segurança cibernética e segurança nuclear.

Cumpre destacar também o Plano de Resposta a Incidentes de Segurança Computacional em Instalações Nucleares, cujo propósito é auxiliar os Estados membros da agência no desenvolvimento de planos de contingência para incidentes de segurança cibernética com potencial de afetar a segurança nuclear. Nesta publicação existem recomendações para estabelecer uma resposta a incidentes de segurança considerando não apenas as atitudes a serem tomadas, mas também as funções e responsabilidades do operador, da autoridade competente e da autoridade técnica nacional.

Em adição a essas publicações, a IAEA divulgou uma outra, chamada de Condução de Avaliações de Segurança de Computadores em Instalações Nucleares, que é um conjunto de metodologias não pertencente à Série de Segurança Nuclear nº 17 da agência, criado para a realização de avaliações de segurança de computadores em IN. Deste modo, os gestores das IN podem estabelecer, em seus calendários administrativos, avaliações periódicas ou de execução imediata para encontrar as melhores medidas corretivas no que tange à proteção dos sistemas de informação.

A NRC publicou o *Guia de Regulamentação 5.71*, desenvolvido especificamente para ajudar as IN a cumprir o regulamento da 10 CFR 73.54, o qual exige aos interessados em licenças para construção de IN verificarem se seus computadores, sistemas de comunicação digital e redes estão protegidos contra ataques cibernéticos. Segundo a NRC (2010), este guia fornece detalhes sobre o desenvolvimento de um planejamento robusto de segurança cibernética, apresentando um programa eficaz e dinâmico, que deve ser mantido por meio de monitoramento contínuo de seus requisitos básicos, tais como a implementação de uma metodologia de identificação de ativos digitais críticos, ilustrada no Fluxograma 1.

O DHS publicou o *Guia de Implementação (GI) do Modelo de Cibersegurança para Reatores de Energia Nuclear dos*




Fluxograma 1 − Determinação ativos críticos digitais
Fonte: Adaptado de NRC (2010)

*EUA*, que tem o propósito de melhorar a segurança cibernética em uma IN, sendo fundamentado no modelo Estrutura de Segurança Cibernética do Instituto Nacional de Padrões e Tecnologia (NIST). Cabe destacar que o DHS procura, por meio desse guia, simplificar o processo de implementação de uma política de segurança da informação para todas as organizações do setor nuclear.

## SISTEMAS DE INFORMAÇÃO EM USINAS NUCLEARES

O sistema de instrumentação e controle (I&C) é o principal subsistema que atua em funções de controle e monitoramento das usinas nucleares (UN), provendo também informações importantes para o desligamento seguro do reator em resposta a eventos operacionais adversos.

Vale ratificar que os reatores mais modernos estão equipados com sistemas I&C integrados aos sistemas SCADA para coordenar a produção de energia com as demandas de transmissão e distribuição para determinadas regiões. Conforme citado anteriormente, a utilização dos sistemas digitais de I&C e a crescente conectividade entre redes internas e externas expõem as UN a ataques cibernéticos.

Segundo Pengfei (2016), a arquitetura do sistema de I&C tem três funções principais, que são responsáveis pela medição, detecção, regulação e proteção das funções críticas de segurança de uma IN. A primeira função tem como propósito fornecer os recursos sensoriais de medição e detecção a fim de apoiar o monitoramento e controle, permitindo que os operadores atuem em caso de necessidade. Esses sensores e detectores atuam diretamente nos equipamentos das UN, enviando seus sinais através de sistemas computacionais até ao operador, facilitando sua tomada de decisão.

A segunda função é responsável por fornecer controle automático com o propósito de reduzir a carga de trabalho dos operadores, permitindo que estes observem o comportamento da planta e monitorem as condições em evolução. Cumpre destacar que a atuação manual pode ser reservada como ação corretiva, sendo realizada, conforme necessário, com base em treinamentos qualificados. A terceira função é auxiliar os sistemas de segurança, que exigem maior confiabilidade, funcionalidade e disponibilidade, na tarefa de proteção da planta.

Conforme exposto na Figura 2, um sistema moderno de I&C consiste em componentes de controle, como Controladores Lógicos Programáveis (CLP) que interagem com equipamentos físicos e estações de trabalho, a fim de enviar informações aos sistemas de segurança, que estão colocados na metade esquerda, ou aos sistemas que não exigem elevado nível de segurança, expostos na metade direita da Figura 2.

Insta salientar que, segundo Pengfei (2016), a funcionalidade do I&C em uma central nuclear é composta por uma variedade de elementos tecnológicos que constituem sua arquitetura, resultando em uma complexa abordagem devido à profundidade e amplitude dos siste-

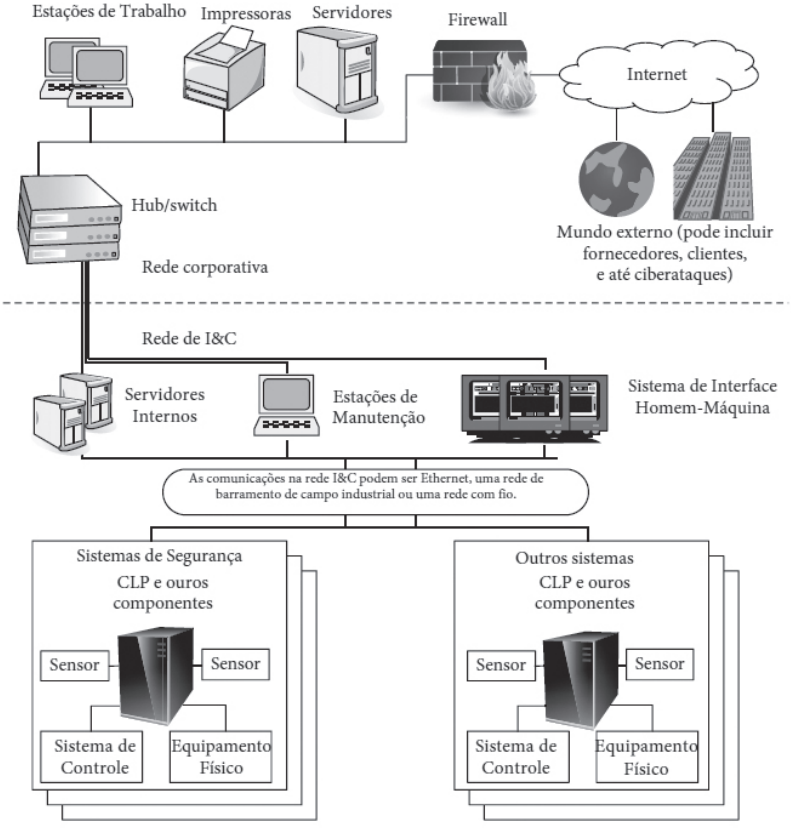



Figura 2 - Sistemas e redes típicos em uma central nuclear
Fonte: Adaptada do DHS (2012)

mas, os quais também incluem campos técnicos, como fatores humanos, gerenciamento de informações, simulações, engenharia de *software*, integração de sistemas e prognósticos.

Em geral, os sistemas de I&C em UN são fisicamente isolados de redes externas e têm um ambiente operacional diferente daquele dos sistemas de TI convencionais. Entretanto, segundo Tellabi *et al*. (2018), diante dos avanços tecnológicos e da tendência da diminuição da mentalidade de segurança, algumas vulnerabilidades foram constatadas nos sistemas de I&C. A Tabela 1 expõe as categorias de vulnerabilidades que podem ocorrer em uma UN, juntamente com os componentes vulneráveis.

De forma a elevar a mentalidade de segurança, diminuindo as vulnerabilidades acima expostas, os diversos setores lógicos ou físicos, funcionários ativos ou passivos são aperfeiçoados para atuarem com conceito de defesa em profundidade. A publicação *Série de Segurança Nuclear nº 17* da IAEA (2013) afirma que o princípio básico de segurança em instalações nucleares é a implementação desse conceito, que consiste na introdução de múltiplas camadas e níveis de proteção consecutivos e independentes, os quais precisariam falhar para comprometer as funções críticas de segurança da IN. Essas camadas são divididas em cinco níveis, abaixo expostos:

− O primeiro nível de defesa tem como propósito evitar os desvios da operação normal e a falha de itens importantes para a segurança.

− O propósito do segundo nível de defesa é detectar e controlar os desvios da operação normal, a fim de evitar que ocorrências operacionais previstas se tornem condições de acidentes.

− O terceiro nível de defesa é responsável por evitar danos ao núcleo do reator e liberações de material radioativo que exijam ações de proteção externas, bem como retornar a usina a um estado seguro por meio de recursos de segurança prévios.

− O quarto nível de defesa tem como propósito impedir o progresso e mitigar as consequências de acidentes resultantes da falha do terceiro nível de defesa, impossibilitando sequências de acidentes que levam a grandes liberações radioativas.

− O propósito do quinto e último nível de defesa é mitigar as consequências radiológicas de uma grande liberação de material radioativo que pode resultar potencialmente de um acidente.

É valido ressaltar que a concepção de níveis de segurança é uma definição que

| Categoria de Vulnerabilidade | Componentes vulneráveis |
|---|---|
| Falta ou validação incorreta de entrada | Estações de trabalho na sala de controle |
| Autorização inadequada | Estações de trabalho na sala de controle |
| Autenticação inadequada | Todos os sistemas de I&C |
| Dados sensíveis não criptografados | Todos os sistemas de I&C |
| Gerenciamento de *software* incorreto | Estações de trabalho na sala de controle |
| Falta de atualizações e *backups* | Sistema de proteção da UN e Sensores |
| Ausência de auditoria | Todos os sistemas de I&C |

Tabela 1 − Categorias de vulnerabilidade e componentes vulneráveis em IN
Fonte: Adaptado de Tellabi (2018)

permite dividir os ativos digitais críticos em diversos graus de proteção de segurança contra qualquer ataque cibernético. Essa abordagem, segundo o *Guia de Regulamentação 5.71* da NRC (2010), divide a arquitetura do sistema de I&C de um IN em quatro níveis, abaixo citados:

Nível 1 - Rede corporativa de longa distância (WAN);

Nível 2 - Rede de área local;

Nível 3 - Rede de aquisição de dados; e

Nível 4 - Sistema de Controle e Segurança.

Cada nível possui diferentes conjuntos de medidas de proteção e requisitos de segurança para garantir atuação contra possíveis ameaças. Cabe ressaltar que algumas medidas de proteção se aplicam a todos os computadores e sistemas em todos os níveis, enquanto outras são específicas para determinados níveis. Destaca-se que as áreas de acesso são um agrupamento lógico e físico de sistemas de informação, enquanto os níveis representam o grau de proteção exigido. A Figura 3 expõe e correlaciona os níveis de segurança e áreas de acesso.

## ANÁLISE DOS CENÁRIOS DE ATAQUE CIBERNÉTICO EM UMA USINA NUCLEAR

Para identificar cenários de ameaças não é suficiente elencar somente as vulnerabilidades citadas anteriormente; faz-se necessário citar requisitos de segurança das instalações nucleares. Esses requisitos foram fundamentados no *Guia de Regulamentação 5.71* da NRC (2010). São eles:

- autenticação mútua;
- confidencialidade;
- autorização;
- integridade dos dados;
- irretratabilidade;
- monitoramento de capacidade de segurança de sistemas;
- auditoria; e
- disponibilidade.

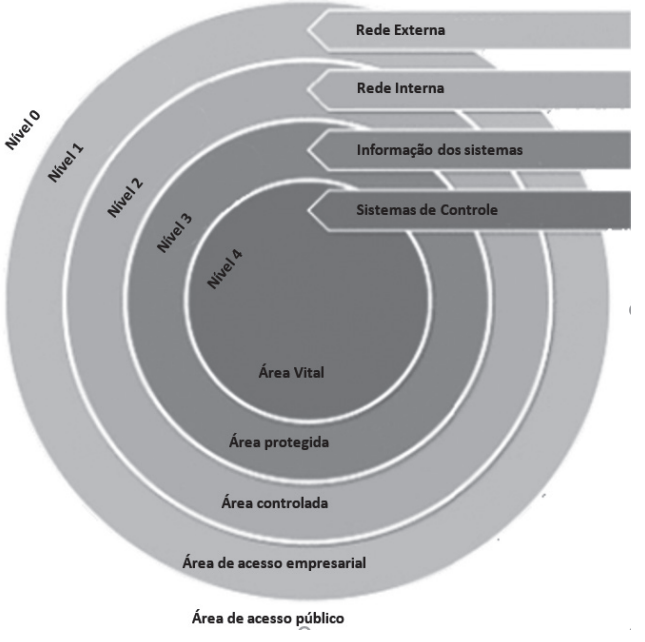



Figura 3 − Correlação entre níveis de segurança e áreas de acesso
Fonte: Adaptado do Congresso Cooperação Índia-EUA (GUENTHER, 2013)

Isso exposto, afirma-se que a análise probabilística de segurança, amplamente utilizada na indústria nuclear para considerar o impacto da falha do equipamento na segurança das instalações, é insuficiente para a análise de ataques cibernéticos. Isso porque esses ataques são iniciados por seres humanos e sua progressão pode ser alterada durante sua realização, em resposta a medidas defensivas da UN.

Entretanto a consideração de falha de causa co-

mum é uma ferramenta útil para ser usada como parte da análise de segurança cibernética de uma IN, pois, ainda que componentes redundantes sejam aparentemente independentes, podem ser individualmente atacados por um invasor, para concluir o propósito de causar a indisponibilidade de uma instalação por uma simples falha.

As diretrizes regulatórias de segurança cibernética anteriormente expostas exigem que sejam desenvolvidos cenários de ataque em IN. Nesse contexto, o NRC (2010), por meio de seu *Guia de Regulamentação 5.71*, expõe cenários de ataque padrões para tornar os treinamentos eficazes, estimulando o estabelecimento e a elaboração de tais cenários como meio de avaliações de gestão e riscos. Esses cenários são essenciais para elevar o nível de segurança das UN, podendo também ser utilizados nos seguintes casos: entender a natureza dos ataques, compreender os potenciais locais de um ataque, definição de contramedidas, gerenciamento de riscos, teste de penetração e implementação de planos e programas de segurança cibernética.

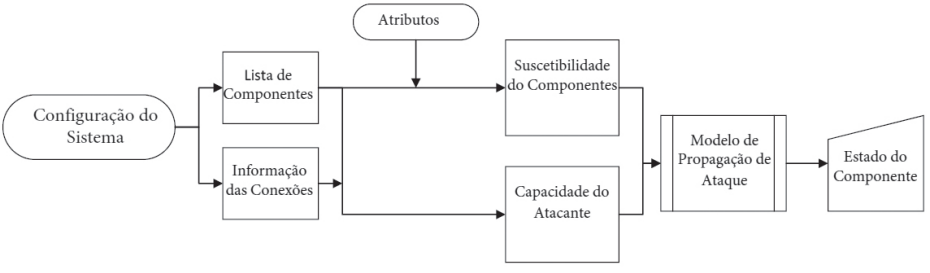
De forma a fundamentar a elaboração de cenários de ataque, este artigo utilizou os seguintes conceitos previstos no *Guia de Regulamentação 5.71* da NRC:

- identificação do alvo;
- reconhecimento;
- acesso / comprometimento do sistema;
- execução de ataques; e
- cobertura de faixas para manter a negação.

No que tange à geração de cenários de ataque, exposta no Fluxograma 2, segundo o *Guia de Regulamentação 5.71* (2010), a configuração do sistema é usada para gerar as regras sobre como os ataques podem se propagar sobre a arquitetura de rede e as informações dos componentes.

Conforme a Tabela 2, cada componente do sistema possui um conjunto associado a alguns atributos, os quais determinam a suscetibilidade de um componente a um ataque e a capacidade do invasor em obter controle completo do componente. Por exemplo, um componente com capacidade de gerar tráfego de rede pode ser comprometido e causar degradação no desempenho dos componentes vizinhos que são vulneráveis ao tráfego malicioso. Da mesma forma, um componente que possui *firmware*[3] atualizável pelo usuário ficará vulnerável a *firmware* malicioso introduzido durante a atualização.

Conforme citado pela NRC (2010) no *Guia de Regulamentação 5.71*, depois que o conjunto de atributos é anexado a




Fluxograma 2 − Geração de cenários de ataque
Fonte: Adaptado do no *Guia de Regulamentação 5.71* (NRC, 2010)

3 *Firmware* é um programa de *software* ou conjunto de instruções programadas em um dispositivo de *hardware*.

| Atributo do Componente | Capacidade de | Atacante atua | Suscetibilidade de |
|---|---|---|---|
| Interface de programação local | Alterar código e dados | Inserindo sub-rotina maliciosa | - |
| Interface de programação remota | Alterar código e dados | Inserindo sub-rotina maliciosa | - |
| Interface de rede - saída | Gerar pacotes de rede arbitrários | Negando serviço a rede | - |
| Interface de rede - entrada | Capturar pacotes de rede arbitrários | Coletando informação | Aumentar uso de memória |
| *Firmware* | Controlar *hardware* | Alterando mecanismo de segurança | Alterar o controle ou acesso ao *hardware* |
| Sistema operacional | Controlar *hardware* | Alterando mecanismo de segurança | Gerar corrupção de memória |

Tabela 2 − Relação entre atributos, capacidades de atuação do atacante e suscetibilidade
Fonte: Adaptado da NRC (2010)

cada componente, as possíveis interações entre os componentes permitem modelar a propagação do ataque. Um cenário de ataque completo contém informações desde o vetor de ataque inicial até o estado final do componente, somado a uma retroalimentação que pode utilizar informações a partir de análises adicionais sobre a resposta de defesa do sistema a cada ataque. Essa análise pode ser feita no pior cenário possível, permitindo avaliar possíveis e reais vetores de ataque.

Assim, nas seguintes subseções serão apresentados dois cenários de ataques fundamentados a partir dos conceitos acima expostos, pautados em uma abordagem que caracteriza um componente inicialmente comprometido sendo utilizado para iniciar um ataque cibernético em UN.

### *Ataque no sistema de controle de pressão do pressurizador*

Segundo Sotoma (1973), o pressurizador é um dispositivo do circuito primário de reatores a água pressurizada, o qual recebe as variações da pressão que o líquido refrigerante (água) sofre no decorrer da operação do reator. Ele possui elementos aquecedores, que conservam a água na temperatura de saturação, garantindo a pressurização. O primeiro cenário de ataque consiste na indisponibilidade da IN por meio da ativação do sistema de proteção do reator, que foi acionado devido a uma falha de causa comum no pressurizador.

Segundo a IAEA (2004) em sua publicação que versa sobre projeto dos sistemas de refrigeração do reator em usinas nucleares, o sistema de controle do pressurizador em uma concepção genérica, porém, comumente utilizada em UN consiste em três sensores de pressão dos aquecedores conectados a dois CLP. Esses CLP são interconectados através de uma interface de rede com a sala de controle do reator. O sistema de controle do pressurizador contém ainda um *backbone*[4] de rede que possui uma estação de trabalho e roteadores unidirecionais que são usa-

4 *Backbone* é a maior linha de transmissão que carrega dados coletados de linhas menores interconectadas; é uma parte da rede de computadores que interconecta várias partes da rede. (DEAN, 2010)

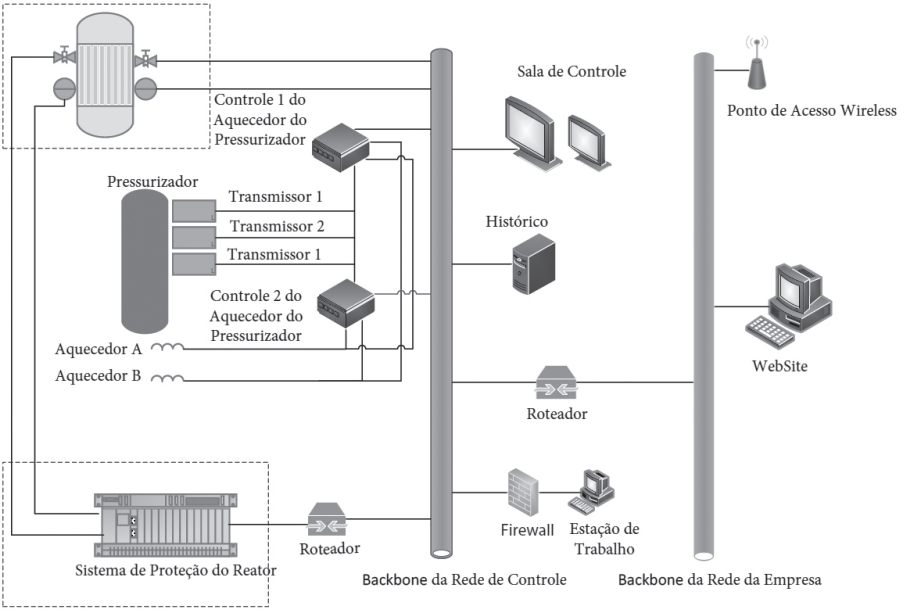



Figura 4 − Sistema I&C do pressurizador de uma usina nuclear
Fonte: Adaptado de Torres (2014)

dos para segmentar a rede de controle da rede corporativa e da rede do sistema de proteção de reatores.

O sistema descrito anteriormente está ilustrado na Figura 4. Um ato malicioso poderia ser iniciado a partir de uma injeção de código malicioso no *software* atualização do *firmware* do CLP, que inicialmente aumentaria a latência para comunicação na rede de controle, comprometendo o envio de informações entre os sensores e os CLP. Em seguida, esse *firmware* alterado faz com que o *hardware* de rede do CLP mude o ponto de atuação do aquecedor, que será ação suficiente para o sistema de proteção do reator entrar em ação, desligando o reator e tornando a UN indisponível.

### *Ataque a um relé de proteção da subestação de energia elétrica de uma IN*

Segundo Morimoto (2005), os relés de proteção fornecem funções de controle, proteção, medição e automação para sistemas ou subestações de energia elétrica. Os relés de proteção digital oferecem um nível mais alto de confiabilidade, funcionalidade e de capacidade de fornecer integração direta a vários outros sistemas, incluindo o SCADA, em comparação com os relés de proteção mecânicos mais antigos.

Conforme Zhang e Dong (2017), quando esses dispositivos são encontrados como elementos digitais ligados em rede, um invasor pode realizar um ataque, afetando os sistemas de I&C e impedindo o envio de informações. Supondo que o invasor conheça a topologia de um sistema de energia e suas áreas de proteção, ele pode selecionar relés com base na importância dessas áreas. Assumindo que o invasor possui conhecimento completo sobre o estado do sistema e suas vulnerabilidades, o primeiro nível da defesa em profundidade da instalação pode ser violado, indisponibilizando o relé de proteção

da rede de recebimento de energia da IN, o que automaticamente iniciará a atuação do sistema de proteção do reator, desligando o reator e tornando a UN indisponível.

### *Incidentes cibernéticos em IN*

Ainda que com frequência reduzida, sempre são divulgadas notícias de incidentes relacionados a ameaças cibernéticas em IN pela IAEA. Dentre essas notícias, expostas na Tabela 3, destaca-se o incidente com a IN iraniana em 2010, a fim de elevar o nível da mentalidade de segurança.

### *Atuação do vírus Stuxnet na instalação nuclear de urânio em Natanz, Irã*

Segundo Marr (2019), no ano de 2005, o aumento do desenvolvimento em pesquisas no setor nuclear pelo Irã acarretou em um grande impasse desse país com o Conselho de Segurança das Nações Unidas (CSNU), tendo em vista que o alto nível de enriquecimento poderia representar a capacidade de produção para construção de um artefato bélico nuclear, o que foi motivo de preocupação da maioria dos países pertencentes ao CSNU, principalmente do governo americano.

Dessa forma, conforme explanado por Marr (2019), em 2007 iniciou-se uma operação de guerra cibernética, chamada Jogos Olímpicos, com o propósito de sabotar as crescentes atividades de enriquecimento do Irã por meio de ataques cibernéticos contra a IN na cidade iraniana de Natanz, interrompendo a capacidade daquele país em desenvolver seu programa de enriquecimento de combustível.

Os ataques cibernéticos direcionados a IN em Natanz obtiveram sucesso devido à utilização do código malicioso chamado

| Mês/Ano | Nome | País | Descrição | Categoria |
|---|---|---|---|---|
| junho de 2010 | IN de Natanz | Irã | Vírus Stuxnet usado para destruir centrífugas | Intencional |
| abril de 2011 | Laboratório Nacional Oak Ridge | Estados Unidos | Roubo de dados via *spear-phishing* | Intencional |
| setembro de 2011 | Areva | França | Intrusões de rede | Desconhecido |
| maio de 2012 | Programa Nuclear Iraniano | Irã | Vírus Duqu usado para realizar espionagem | Intencional |
| janeiro de 2014 | Usina Nuclear de Monju | Japão | Liberação de dados | Desconhecido |
| dezembro de 2014 | Korea Nuclear Power | Coreia do Sul | Roubo e liberação de dados | Intencional |
| fevereiro de 2016 | Comissão Reguladora Nuclear/Departamento de Energia dos EUA | Estados Unidos | Vírus distribuídos através de *e-mails* de *spear-phishing* | Intencional |
| abril de 2016 | Planos de energia nuclear de Gundremmingen | Alemanha | Sistema de monitoramento do elemento combustível | Desconhecido |
| junho de 2016 | Universidade de Toyama, Centro de Pesquisa de Isótopos de Hidrogênio | Japão | Roubo de dados via *spear-phishing* | Intencional |

Tabela 3 − Incidentes cibernéticos em IN

Stuxnet, o qual foi inserido na instalação iraniana para administrar os sistemas de controle, permanecendo indetectável durante todo o processo e inviabilizando a operação da usina.

Segundo Marr (2019), o vírus[5] Stuxnet foi desenvolvido pelas agências de inteligência israelense e americana. Sua principal ação era reprogramar sistemas da instalação, modificando o código de controle nos CLP que eram responsáveis pelo funcionamento das centrífugas utilizadas no processo de enriquecimento de urânio nas IN de Natanz.

Destaca-se que, ao ser inserido na rede, conforme a Figura 5, o Stuxnet pesquisava o programa Simatic, da empresa Siemens, em computadores com sistema operacional Windows, que gerenciava os CLP. Em seguida, o Stuxnet modificava o perfil operacional das centrífugas, fazendo com que seus rotores girassem de forma acelerada, e esse aumento substancial na velocidade resultava no aumento de pressão do rotor nas paredes do equipamento, causando danos catastróficos à IN iraniana.

Segundo relatórios divulgados pela empresa Nixu (2017), estima-se que, entre o final de 2009 e o início de 2010, o Irã desativou e substituiu aproximadamente mil centrífugas em Natanz devido a danos causados pelo vírus Stuxnet. No final do ano de 2010, conforme Marr (2019) elencou, o Irã suspendeu tempora-

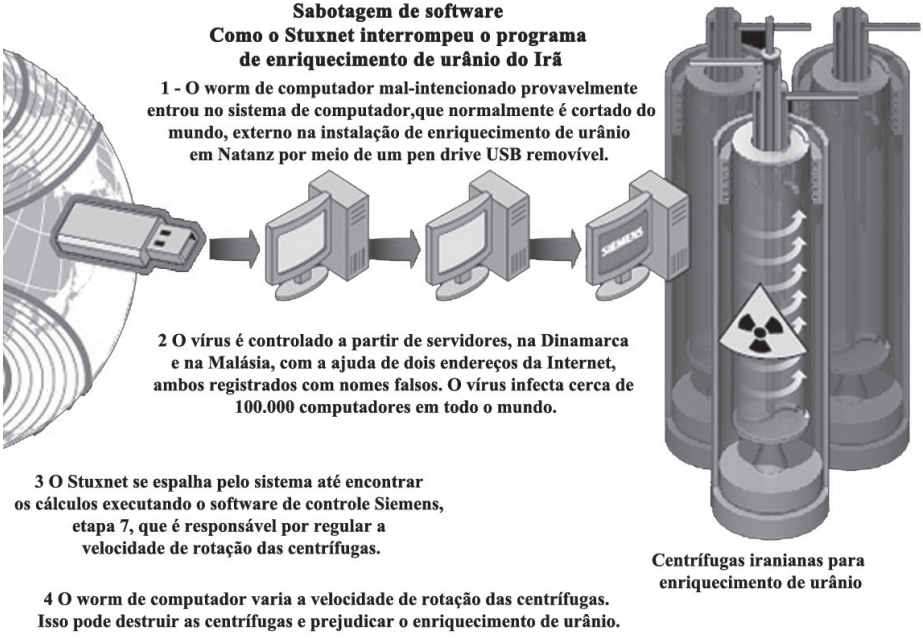



Figura 5 – Atuação do Vírus Stuxnet
Fonte: Adaptado da WNA (2019)

5 O vírus de computador é um programa malicioso que se propaga inserindo cópias de si mesmo.

riamente as atividades de enriquecimento em meio a problemas crescentes nas operações de centrifugação.

## CONSIDERAÇÕES FINAIS

Em coadunância com o exposto anteriormente, impende afirmar que o contínuo avanço tecnológico no âmbito das IN as torna alvos potenciais para ataques cibernéticos. Dessa forma, este artigo expôs uma análise de segurança diante da ocorrência da indisponibilidade de uma IN, a partir de um ataque cibernético, por meio de um estudo da interação entre os sistemas de I&C presentes nessas instalações.

De forma a atingir o propósito principal delineado, constatou-se que a base de normatização de diversos órgãos reguladores, tais como IAEA, ISO, NIST e NRC, sobre o tema de segurança da informação no setor nuclear possui diversas semelhanças entre seus conteúdos, com destaque para:

- categorização dos sistemas de segurança de computadores;
- medidas para proteção contra ameaças cibernéticas;
- criação, implementação e suporte do plano de segurança dos sistemas;
- realização de avaliação e gerenciamento de riscos; e
- exposição do ciclo de vida da segurança dos SI.

Todavia, ainda são evidenciadas diferenças entre essas normas em aspectos como o treinamento e manutenção da cultura de segurança cibernética do pessoal diretamente envolvido com a operação de uma IN. Assim, cada vez mais é necessária uma rigorosa estrutura normativa para lidar com essa questão desafiadora.

É válido ressaltar também que, em um cenário onde a importância da segurança cibernética para uma IC é de elevada preocupação, este artigo depreendeu que alguns procedimentos devem ser observados nessas IC, tais como:

- estabelecimento de políticas e programas de segurança cibernética;
- incorporação de uma política de segurança cibernética no programa de proteção física;
- uso de CLP com menor grau de vulnerabilidade;
- estabelecer o controle de acesso para ferramentas de desenvolvimento e programação; e
- análise de ameaças e cenários de ataques cibernético em diferentes tipos de componentes.

Nesse contexto, o artigo também abordou o tema relacionado a cenários de ataques cibernéticos em UN, expondo exemplos de vulnerabilidades dos componentes que afetam os sistemas de I&C.

Assim, é possível afirmar que não há panaceia contra ataques cibernéticos. No entanto, uma segurança com a metodologia de defesa em profundidade incorporada ao projeto de uma IN pode fornecer uma camada de defesa contra ameaças cibernéticas atuais e emergentes, limitando vetores de ataque e novas vulnerabilidades.

Como trabalho futuro, a intenção é quantificar e simular modelo de geração de cenários de ataque com base nas diretrizes preconizadas pelas agências reguladoras, a fim de aumentar o nível de conscientização dos gestores e funcionários de uma instalação nuclear quanto à segurança cibernética.

CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<SISTEMAS>; Sistema de Segurança;

## REFERÊNCIAS BIBLIOGRÁFICAS


ABNT. ABNT NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013.

ABNT. ABNT NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2013.

BEGGS, P. *Securing the Nation's Critical Cyber Infrastructure.* DHS, Washington, 2010. Disponível em: https://www.dhs.gov/. Acesso em: 4 set. 2019.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Portaria nº 93. *Glossário de Segurança da Informação*. Brasília, DF: Gabinete de Segurança Institucional da Presidência da República, set. 2019. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 28 out. 2019.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. *Guia de referência para a segurança das infraestruturas críticas da informação.* Brasília, DF: Gabinete de Segurança Institucional da Presidência da República, nov. 2010. Disponível em: http://dsic.planalto.gov.br/legislacao/2_Guia_SICI.pdf. Acesso em: 4 nov. 2019.

BRITISH PETROLEUM. *British Petroleum BP Statistical Review of World Energy*. British Petroleum, London, 2019. Disponível em: https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-nuclear-energy.pdf. Acesso em: 11 out. 2019.

CLARKE, R. A.; OLCOTT, J. *Confronting Cyber Risk in Critical Infrastructure: The National and Economic Benefits of Security Development Processes*. Good Harbor, Washington, 2012. Disponível em: https://www.semanticscholar.org/paper/Confronting-Cyber-Risk-in-Critical-Infrastructure/45bb69ba1f7e5286f951bd3a. Acesso em: 29 out. 2019.

CLEMENTE, D. *Cyber Security and Global Interdependence: What is Critical?*. Chatham House, London, 2013. Disponível em: http://bit.ly/2V70bh6. Acesso em: 16 set. 2019.

COMISSÃO EUROPEIA. *Proteção das infraestruturas críticas*. Comissão Europeia, Bruxelas, 2008. Disponível em: http://publications.europa.eu/resource/cellar/15306167-9a7e-4022-9f02-ce742f9d7850.0020.02/DOC_1. Acesso em: 30 out. 2019.

DHS. *Office of Infrastructure Protection Strategic Plan: 2012-2016*. DHS, Washington, 2012. Disponível em: https://www.cisa.gov/sites/default/files/publications/IP-Strategic-Plan-FINAL-508.pdf. Acesso em: 20 dez. 2019.

DHS. *Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power Reactors.* DHS, Washington, 2015. Disponível em: https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/nuclear-framework-implementation-guide-2015-508.pdf. Acesso em: 15 dez. 2019.

FERNANDES, A. A.; ABREU, V. F. *Implantando a Governança de TI: da Estratégia à Gestão de Processos e Serviços*. 4. ed. Rio de Janeiro: Brasport, 2014.

FREIRE, I. M. "O futuro é agora". Revista *Você S/A*, Rio de Janeiro, v. 63, p. 58, 2003. Disponível em: http://www.isafreire.pro.br/site/documentos/outrostextos/O%20futuro.pdf/. Acesso em: 30 set. 2019.

GUENTHER, R. et al. *Committee on India-United States Cooperation on Technical Aspects of Civilian Nuclear Materials Security*. Washington: National Academy of Sciences, 2013.

IAEA. *Power Reactor Information System*. IAEA, Vienna, 2017. Disponível em: https://pris.IAEA.org/pris/. Acesso em: 11 dez. 2019.

IAEA. *Computer Security at Nuclear Facilities*. IAEA, Vienna, 2011. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf. Acesso em: 12 dez. 2019.

IAEA. *Computer Security of Instrumentation and Control Systems at Nuclear Facilities*. IAEA, Vienna, 2018. Disponível em: https://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf. Acesso em: 14 dez. 2019.

IAEA. *Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants*. IAEA, Vienna, 2004. Disponível em: https://www.iaea.org/publications/7020/design-of--the-reactor-coolant-system-and-associated-systems-in-nuclear-power-plants. Acesso em: 14 jan. 2019.

IAEA. *Safety of Nuclear Power Plants: Design*. IAEA, Vienna, 2016. Disponível em: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1715web-46541668.pdf. Acesso em: 23 dez. 2019.

IEC. IEC 62859:2016 - Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity. Geneva: IEC, 2016. Disponível em: https://webstore.iec.ch/publication/26131. Acesso em: 12 dez. 2019.

KELLY, T. K. *Infrastructure Interdependencies. A Workshop on Electricity Security and Survivability*. Carnegie Mellon University, Pennsylvania, 2001. Disponível em: https://www.cmu.edu/. Acesso em: 30 out. 2019.

KKG. *Detecção de* malware *de escritório em vários computadores.* KKG, Gundremmingen, 2016. Disponível em: https://www.kkw-gundremmingen.de/presse.php?id=571. Acesso em: 16 set. 2019.

MARCONI, M. A.; LAKATOS, E. M. *Metodologia do trabalho científico*. 8. ed. São Paulo: Atlas, 2017.

MARR, C. *Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello*. University of Pennsylvania, Pennsylvania, 2019. Disponível em: https://repository.upenn.edu/spice/vol14/iss1/2/. Acesso em: 25 jan. 2019.

MORIMOTO, C. E. "Relê (Relay)". *Guia do* hardware, São Paulo, 2005. Disponível em: https://www.hardware.com.br/termos/rele-relay. Acesso em: 15 jan. 2020.

NATÁRIO, R. M. P.; NUNES, P. F. V. "Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas". *Revista Militar*, Lisboa, n. 2.547, p. 249, abr. 2014. Disponível em: https://www.revistamilitar.pt/artigo/913. Acesso em: 2 nov. 2019.

NIXU. *Cybersecurity is an inseparable part of nuclear safety*. Helsinki: Nixu, fev. 2017. Disponível em: https://www.nixu.com/whitepaper/publication-cybersecurity-nuclear-safety. Acesso em: 23 out. 2019.

NRC. NUREG 7007 - Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems. NRC, Washington, 2008. Disponível em: https://www.nrc.gov/docs/ML1005/ML100541256.pdf. Acesso em: 23 dez. 2019.

NRC. Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities. NRC, Washington, 2010. Disponível em: https://www.nrc.gov/docs/ML0903/ML090340159.pdf. Acesso em: 15 dez. 2019.

OLIVEIRA. M. S *et al*. *Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa*. Centro Universitário Municipal de Franca, Franca, 2019. Disponível em: http://periodicos.unifacef.com.br/index.php/resiget/article/view/1065. Acesso em: 30 dez. 2019.

PEDERSON, P. *et al*. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory, Idaho, 2006. Disponível em: http://cip.management.dal.ca/publications/Critical%20Infrastructure%20Interdependency%20Modeling.pdf. Acesso em: 1º nov. 2019.

PENGFEI, G. *A Study About Safety I&C System Software V&V in Nuclear Power Plant*. Pensilvânia, 2019. Disponível em: https://doi.org/10.1115/ICONE24-60125. Acesso em: 16 dez. 2019.

PERROTA. J. A. *Reatores Nucleares − Conceitos*. Instituto de Pesquisas Energéticas e Nucleares, São Paulo, 2017. Disponível em: https://www.institutodeengenharia.org.br/. Acesso em: 2 nov. 2019.

SKLYAR, W. “Cyber Security of Safety-Critical Infrastructures: A Case Study for Nuclear Facilities”. *Information & Security Journal*, [s. l.], 2012. Disponível em: http://it4sec.org/bg/system/files/28.08Sklyar.pdf. Acesso em: 12 out. 2019.

SOTOMA, H. *Estudo transiente de um pressurizador de um Reator a água pressurizada (PWR)*. 1973. Dissertação (Mestrado em Ciência), Escola Politécnica, Universidade de São Paulo, São Paulo, 1973. Disponível em: http://carpedien.ien.gov.br:8080/handle/ien/1997. Acesso em: 7 jan. 2019.

SYMONOV, A.; KLEVTSOV, A. *About the Problem of Regulatory Activity for Computer Security of NPP Instrumentation and Control Systems in Ukraine*. IEEE, Kyiv, 2018. Disponível em: http://bit.ly/2T0MEoG. Acesso em: 10 dez. 2019.

TELLABI, A. et al. *International Standards as Precondition for Prevention of Cyber Attacks on Nuclear Power Plants*. AMNT, Berlim, 2018. Disponível em: http://bit.ly/38Fw5oU. Acesso em: 21 dez. 2019.

TORRES, R. *Modelagem de pressurizador para reator nuclear compacto: abordagem de duas regiões*. 2014. Dissertação (Mestrado em Ciência e Tecnologia Nucleares), Instituto de Engenharia Nuclear, Rio de Janeiro, 2014.

WNA. *Nuclear Energy and Sustainable Development*. WNA, London, 2018. Disponível em: https://www.world-nuclear.org/information-library/energy-and-the-environment/nuclear-energy-and-sustainable-development.aspx. Acesso em: 13 out. 2019.

WNA. *Nuclear Power in Iran*. WNA, London, 2019. Disponível em: https://www.world-nuclear.org/information-library/country-profiles/countries-g-n/iran.aspx. Acesso em: 14 jan. 2020.

ZHANG, J.; DONG, Y. *Cyber attacks on remote relays in smart grid.* In: 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, 2017. Disponível em: https://doi.org/10.1109/CNS.2017.8228637. Acesso em: 20 jan. 2019.