FACULDADE DE TECNOLOGIA DE SÃO BERNARDO DO CAMPO

“ADIB MOISÉS DIB”

ARTUR MARTINS PEREIRA
PAULA DE MATOS SILVA
ULISSES RAFAEL FAVARIS
VICTOR ANDREOLI CUSTÓDIO

CIBERSEGURANÇA NA INDÚSTRIA 4.0: CRIAÇÃO DE WEBSITE INFORMATIVO

São Bernardo do Campo - SP
Junho/2021

ARTUR MARTINS PEREIRA
PAULA DE MATOS SILVA
ULISSES RAFAEL FAVARIS
VICTOR ANDREOLI CUSTÓDIO

CIBERSEGURANÇA NA INDÚSTRIA 4.0: CRIAÇÃO DE WEBSITE INFORMATIVO

Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de São Bernardo do Campo “Adib Moisés Dib” como requisito parcial para a obtenção do título de tecnólogo em Tecnologia em Informática para Negócios.

Orientador: Prof. Esp. Ismael Moura Parede.

São Bernardo do Campo - SP
Junho/2021

RESUMO

A chegada da Quarta Revolução Industrial trouxe novas tecnologias aos meios de produção, como a Internet of Things, o que consequentemente elevou o número de ameaças à cibersegurança. Esse crescimento tecnológico também possibilitou uma maior facilidade no acesso à informação, haja visto que os smartphones são uma das tecnologias mais utilizadas no mundo atual. Nesse contexto, o objetivo deste projeto é construir um website informativo que instrua os colaboradores da indústria 4.0, reunindo os principais tópicos relacionados à cibersegurança, permitindo a prevenção de possíveis ciberataques. Trata-se de uma pesquisa aplicada, composta por pesquisa bibliográfica para a discussão das contribuições de autores da área e pesquisa experimental, com vistas ao desenvolvimento do produto tecnológico. A princípio, as linguagens HTML, CSS e JavaScript foram escolhidas para construção do portal web, porém o WordPress oferece mais vantagens no desenvolvimento, já que reúne essas tecnologias em um mesmo ambiente, e de forma mais simplificada. O produto final do trabalho é uma plataforma web que reúne as informações coletadas ao longo da pesquisa, englobando a cibersegurança, os meios de prevenção de ciberataques e a indústria 4.0.

Palavras-chave: Cibersegurança. Indústria 4.0. Ciberataques. Internet das Coisas.

ABSTRACT

The arrival of the Fourth Industrial Revolution brought new technologies to the means of production, such as the Internet of Things, which consequently increased the number of threats to cybersecurity. This technological growth has also made it easier to access information, given that smartphones are one of the most used technologies in the world today. In this context, the objective of this project is to develop an informative website that instructs employees in Industry 4.0, gathering the main topics related to cybersecurity, and allowing the prevention of possible cyber-attacks. It is an applied research, consisting of both bibliographic study for later discussion concerning the contributions from different authors in the field, and an experimental research, aimed at the development of a technological product. At first, the languages HTML, CSS and JavaScript were chosen to build the web page. However, WordPress offers more advantages in development, since it brings these technologies together in the same environment, and in a more simplified way. The final product of the work is a website which gathers the information collected during this research, encompassing themes such as cybersecurity, the prevention of cyber-attacks, and other Industry 4.0 related topics.

Keywords: Cybersecurity. Industry 4.0. Cyberattacks. Internet of Things.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Este trabalho aborda os principais tópicos relacionados à cibersegurança na indústria 4.0, com foco nas vulnerabilidades encontradas nas redes industriais. Seu desenvolvimento visa o público inserido na parcela dos colaboradores envolvidos na indústria 4.0, desde o nível estratégico, da alta administração, até o operacional, da mão de obra.

A fim de atender a esse segmento, a proposta deste trabalho trata-se da elaboração de um informativo sobre os principais tópicos de cibersegurança, bem como maneiras de se prevenir, em forma de um website. O portal contém um menu, que leva para páginas dedicadas a cada tópico, como conceitos gerais, notícias dos ciberataques mais recentes, e métodos de prevenir riscos à cibersegurança. Cada página aborda os conteúdos de forma simples e objetiva, com o auxílio de recursos, como imagens e gráficos.

O objetivo deste projeto foi a criação de um informativo em uma plataforma web, com a finalidade de instruir e auxiliar aos colaboradores da indústria 4.0 com as principais informações sobre temas relacionados à cibersegurança. É interessante saber que, até o momento, não existia um portal informativo em língua portuguesa dedicado exclusivamente para a cibersegurança no contexto da indústria 4.0, o que ressalta ainda mais a importância deste projeto.

Diversas empresas ao redor do mundo estão vulneráveis a ciberataques, como por exemplo a invasão a uma usina nuclear no Irã pelo vírus Stuxnet, em 2010. Além disso, é conhecido que uma das tecnologias mais utilizadas no mundo atual são os smartphones, e conforme indicado pela 31ª Pesquisa Anual do FGV (2020), no Brasil existem dois smartphones ativos por pessoa, em média. Também vale ressaltar que, conforme a pesquisa Digital 2020 feita pelo DataReportal (2020), o brasileiro passa, em média, 9 horas por dia conectado à Internet. Esses dados foram fundamentais para a escolha do tema deste projeto, no caso, o desenvolvimento de um website informativo. Nesse contexto, foi muito importante a criação de um portal que ajude a informar sobre a cibersegurança na indústria 4.0, aprofunde a

compreensão das estruturas de segurança mais recentes, desenvolva o pensamento crítico em relação ao assunto, e induza todos os envolvidos a inserirem novas práticas em suas atividades. Também vale notar que ter uma fonte de informação que aborde os últimos incidentes de segurança ocorridos pelo mundo pode auxiliar as empresas a não cometerem os mesmos erros dos alvos desses ataques.

O presente trabalho se divide nas partes: Capítulo 1 - Fundamentação Teórica, em que são discutidos e comparados os principais autores e teorias que fundamentam o projeto; Capítulo 2 - Metodologia, em que são exploradas as questões relacionadas ao planejamento do desenvolvimento do projeto, com as etapas para sua realização e as ferramentas necessárias; Capítulo 3 - Desenvolvimento, em que efetivamente se descreve o passo a passo da construção do projeto, ou seja, a parte prática; e finalmente, Considerações Finais, com discussões referentes a todo o processo e à conclusão a partir delas.

1 FUNDAMENTAÇÃO TEÓRICA

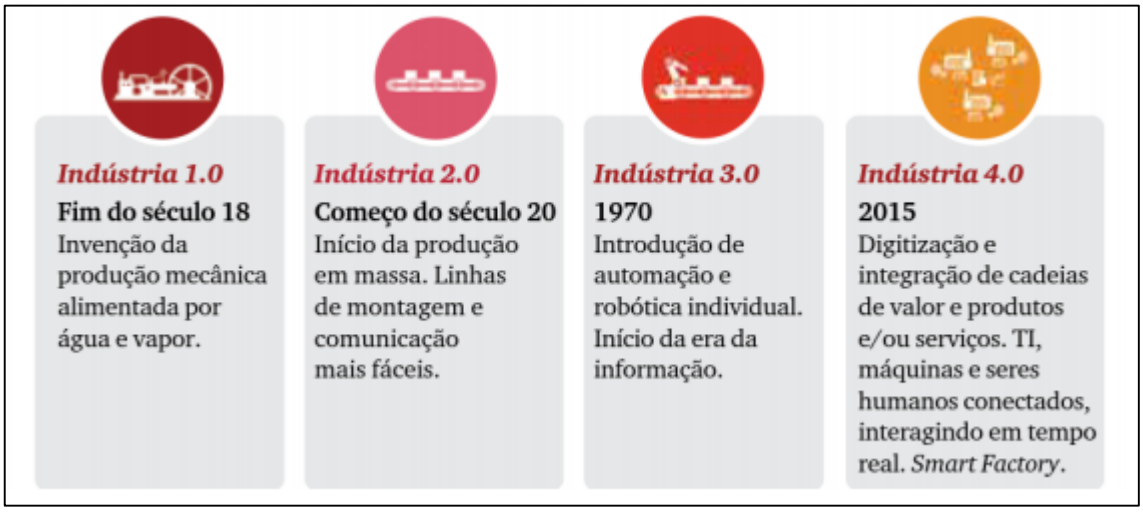
Neste capítulo são apresentados os autores e as discussões que norteiam este projeto de pesquisa.

1.1 As Revoluções Industriais

O surgimento da indústria foi de grande importância para a evolução da humanidade. As inovações em constante mudança serviram para o desenvolvimento de toda uma sociedade, que hoje passa por uma gigante transformação tecnológica, e que se encontra na situação de se adaptar ao novo mundo (SAKURAI; ZUCHI, 2018).

A imagem a seguir representa um panorama das principais descobertas tecnológicas ao longo de quatro Revoluções Industriais, desde o fim do século 18 até os dias atuais:

Figura 1.1 - Mostra a evolução e mudanças nos padrões tecnológicos com as Revoluções Industriais



Fonte: PWC BRASIL (2016)

Antes da revolução industrial, tudo era produzido manualmente em pequenas quantidades, mas por conta do aumento descontrolado da população, se tornou inviável esse método de produção. Como principal objetivo do capitalismo é a

obtenção de lucros, a produção em maior escala passou a ser cada vez mais necessária (CAVALCANTE; SILVA, 2011).

Os autores Sakurai e Zuchi indicam com mais precisão o período em que se iniciou a Primeira Revolução Industrial, bem como suas ramificações entre países a partir da Inglaterra:

> Conforme Boettcher, a primeira Revolução Industrial ocorreu na Inglaterra, final do século XVIII e início do século XIX, entre 1760 e 1860, e depois se estendeu para outros países como: França, Bélgica, Holanda, Rússia Alemanha e Estados Unidos (SAKURAI; ZUCHI, 2018, p. 482).

A Primeira Revolução Industrial foi marcada pela evolução do setor produtivo, primeiramente no setor de transportes, quando a ciência havia permitido a descoberta do carvão enquanto fonte de energia, e também a criação das primeiras máquinas a vapor (VENTURELLI, 2017).

A figura a seguir ilustra a principal tecnologia da Primeira Revolução Industrial - as máquinas a vapor:

Figura 1.2 - É uma ilustração da locomotiva movida a vapor

Fonte: TODO ESTUDO (2020)

Segundo Boettcher, as novas tecnologias foram fatores essenciais no processo da Revolução Industrial, pois elas proporcionaram a modernização e o

crescimento da produção, assim garantindo maior obtenção de lucros (BOETTCHER, 2015).

Silva e Gasparin explicam que nesse período houveram várias descobertas tecnológicas, como a eletricidade, transformação de ferro em aço, meios de transporte mais modernos, e também o desenvolvimento de vários setores industriais. A Revolução 2.0 teve notoriedade pela maior busca dos lucros, trabalho e desenvolvimento da produção (SILVA; GASPARIN, 2013).

Nessa Revolução iniciou-se o Fordismo, sistema de produção em massa criado por Henry Ford em 1914 (BOETTCHER, 2015). Com esse novo sistema, Ford criou a automatização da linha de montagem utilizando esteiras automáticas, assim revolucionando a indústria automobilística.

O autor aponta, entre as principais características da indústria 2.0, o maior controle de gastos, a geração de lucros cada vez maiores, e maior qualidade dos processos envolvidos desde a obtenção de matéria prima até a aquisição pelo consumidor final.

A figura a seguir mostra uma linha de produção em uma fábrica automobilística, a fim de representar a produção em massa, característica da Segunda Revolução:

Figura 1.3 - Mostra trabalhadores na linha de produção de uma fábrica automobilística

Fonte: ESCOLA EDUCAÇÃO (2020)

A Terceira Revolução Industrial é marcada pelas grandes descobertas tecnológicas e científicas, trazendo uma renovação nos processos econômicos, políticos e sociais. As áreas de maiores avanços são da informática, robótica, telecomunicações, transportes, biotecnologia, química e nanotecnologia (BOETTCHER, 2015).

A indústria 3.0 teve diversos atributos relevantes, com o surgimento de novos potenciais industriais, a tecnologia em massa, a percepção ambiental, maquinário moderno, ampliação dos direitos dos trabalhadores, entre outros. Em meio à globalização, ao avanço tecnológico contínuo, e às mudanças de comportamento sociais e culturais, nasce a indústria 4.0 (SILVA et al., 2002).

A figura a seguir apresenta a robótica, uma das tecnologias que caracterizam a Terceira Revolução Industrial:

Figura 1.4 - Mostra robôs em uma fábrica produzindo automóveis

Fonte: BRASIL ESCOLA (2013)

1.2 Indústria 4.0

O progresso tecnológico marcou as três últimas revoluções industriais, e trouxe grandes avanços ao desenvolvimento humano. A quarta revolução industrial, conhecida como indústria 4.0, é um conceito novo e desafiador, muito relevante para o Brasil e para o mundo, com grande impacto na tecnologia, principalmente no setor de manufatura (FROTA, 2019, p. 10).

Frota et al. (2019, p. 10) informa que “a definição do dicionário da palavra evolução, quando aplicada à indústria, reflete o progresso sistemático que vem ocorrendo nos últimos séculos”.

As Revoluções Industriais trouxeram muitos efeitos positivos para a sociedade, como o desenvolvimento industrial e de tecnologias de produção, o oferecimento de maior renda, produtos e serviços sociais, mas ainda existem muitos desafios a serem superados. A indústria 4.0, conhecida como a Nova Revolução Industrial, foi concebida para impulsionar o crescimento econômico, incorporar novas tecnologias e fornecer melhor controle sobre os mecanismos de produção. Essa nova revolução procura introduzir fábricas inteligentes, com modelos de produção mais eficientes, autônomos e personalizáveis (BRETTEL et al., 2014).

SILVEIRA et al. (2017) descrevem que a Nova Revolução Industrial surgiu dos projetos estratégicos do governo alemão, visando utilizar novas tecnologias na indústria. A indústria 4.0 foi apresentada na Feira de Hannover de 2011. Em outubro do ano seguinte, foi elaborado um relatório recomendando a sua implantação em vários setores da Alemanha. Em abril do ano seguinte, o projeto final foi apresentado, com o objetivo de obter maior autonomia e eficiência de produção nos setores manufatureiros.

O foco da indústria 4.0 é o desenvolvimento de produtos e processos inteligentes para acelerar os meios de produção. Através de novas tecnologias, é possível melhorar a produtividade de novas fábricas inteligentes, além de ser um meio para facilitar o processo de desenvolvimento de novos produtos (BRETTEL et al., 2014).

Segundo Silveira et al. (2017), os seis princípios que definem os sistemas de produção inteligente na indústria 4.0 são:

- **Capacidade de operação em tempo real:** processamento e tratamento de dados adquiridos em tempo real, para que a tomada de decisões possa ser imediata;
- **Virtualização:** uma cópia virtual de uma fábrica inteligente. Isso torna o monitoramento mais preciso, podendo ser controlado remotamente através de sensores distribuídos pela planta;
- **Descentralização:** aprimoramento dos processos de produção, atualizando em tempo real as necessidades de produção, através de sistemas cyber-físicos. Dessa forma, a máquina não apenas recebe comandos de trabalho, mas também pode fornecer informações sobre todo o ciclo;
- **Orientação a serviços:** utilização de arquitetura de softwares aliado ao conceito de *Internet of Services*, que é o uso do IoT na prestação de serviços;
- **Modularidade:** fabricação conforme demanda, oferecendo a flexibilidade para alterar as tarefas da máquina mais facilmente.

Com base nos princípios acima, a indústria 4.0 é alcançada combinando os mais recentes progressos tecnológicos, com as inovações que estão sendo desenvolvidas nas áreas de TIC (Tecnologia da Informação e Comunicação) e engenharia.

De acordo com os princípios mencionados acima por Silveira et al., a indústria 4.0 tornou-se possível devido ao progresso tecnológico da última década e ao desenvolvimento das áreas de tecnologia da informação e engenharia. Os itens considerados como as bases da indústria 4.0 são:

- **Internet das coisas (Internet of Things - IoT):** A integração de tecnologias digitais, físicas e biológicas por meio de dispositivos eletrônicos que permitem a coleta e a troca de dados;

- **Big Data Analytics:** Estruturas de dados grandes e complexas, que auxiliam na análise e gerenciamento de informações. Quando aplicada na indústria 4.0, utilizam os 6 Cs para rastrear as informações mais importantes: conexão (à rede industrial, sensores e CLPs), cloud (nuvem/dados por demanda), cyber (modelo e memória), conteúdo, comunidade (compartilhamento das informações) e customização (personalização e valores);
- **Segurança:** toda conectividade requer sistemas que protejam o fluxo de informações. É um grande desafio, pois a segurança e a robustez dos sistemas de informação devem se tornar cada vez mais eficientes. A falta de comunicação pode causar problemas sérios a um sistema de produção.

1.3 Conceito de Redes

Hoje, estão todos de alguma forma em contato com as redes. Como observa Torres (2001), as redes de computadores surgiram da necessidade de uma troca de informações que permita o acesso a dados fisicamente distantes.

Para Maya (2020) uma rede de computadores se trata de um grupo de sistemas e dispositivos de hardware de computação que tem a finalidade de facilitar a comunicação e o compartilhamento de recursos entre os usuários.

Soares (1995) esclarece que um conjunto de módulos de processadores e um sistema de comunicação formam uma rede de computadores. Criando os chamados hosts, conexões lógicas (programas e protocolos) e físicas (equipamentos) entre vários computadores. Um computador conectado a uma rede pode ter acesso às informações que chegam diretamente a ele e às informações que chegam nos demais computadores conectados na mesma rede, aumentando o número de informações possíveis em somente um computador.

As redes computacionais e as tecnologias comandam as indústrias de hardware, software e periféricos. Esse crescimento reflete a quantidade de usuários de redes. No momento atual, o centro da comunicação são as redes de computadores.

Os objetivos da comunicação cresceram consideravelmente na década de 1990 e essa expansão não teria ocorrido se não houvesse o avanço progressivo das redes computacionais (FOROUZAN, 2010).

A comunicação de dados e dispositivos é organizada por meio de protocolos, ou seja, um conjunto de regras que organiza a comunicação de dados entre dispositivos, formatando e a ordenando mensagens, controlando o envio e o recebimento de pacotes de informações em uma determinada rede de computadores (GOMES, 2019).

Atualmente, os protocolos TCP/IP (Transmission Control Protocol / Internet Protocol) são os mais comumente utilizados. Isto se deve em grande parte à popularidade da internet, pois é a razão pela qual o conjunto foi criado. De acordo com Torres (2001), uma das vantagens destes protocolos em meio a outros existentes, é a sua capacidade de rotear, o que permite o envio de mensagens ou dados por uma rede de longa distância, podendo haver vários caminhos para o computador receptor. Também vale ressaltar que esse conjunto de protocolos é adotado por muitos fabricantes, pois eles podem utilizar suas próprias versões do TCP/IP em seus sistemas operacionais, já que se tratam de protocolos de arquitetura aberta.

O TCP/IP trata-se de um conjunto de protocolos. É um grupo dividido em quatro camadas: aplicação, transporte, rede e enlace de dados. Cada camada executa uma tarefa diferente. A divisão em camadas busca garantir a integridade dos dados que trafegam pela rede (REIS, 2017).

As principais características do TCP/IP são:

- Pode ser usado e desenvolvido gratuitamente, independentemente do hardware ou sistema operacional do computador, pois possui padrão aberto;
- É independente de hardware de rede específico;

- Seu esquema de endereçamento comum que permite que cada dispositivo se comunique com outro dispositivo pela rede, independentemente do tamanho;
- Consiste em protocolos de alto nível padronizados para serviços amplamente disponíveis.

1.4 Cibersegurança

Segundo Leite (2016), o ciberespaço surge como uma plataforma mundial sem limites, que pode ser acessada e sofrer manipulação por qualquer pessoa. E com isso, surgem diversas possibilidades de ataques tecnológicos que possam prejudicar pessoas e instituições, então há a necessidade de configurar estruturas nacionais e internacionais para monitorar e prevenir a segurança.

Um novo espaço foi criado com a invenção da internet e sua rede mundial, tal espaço não é físico; apenas virtual, e atende pelo nome de ciberespaço. Esse novo espaço afeta o modo como se vive, a forma de socializar ganhou uma nova forma, estudar, comunicar e conhecer o mundo através da internet. Porém, com toda essa interligação, surgiram novos desafios para a segurança, pois conforme foi constatado a partir da identificação das vulnerabilidades da tecnologia e a sua exploração através de agentes de ameaça (LEITE, 2016).

A cibersegurança, na área da TIC, é definida como a proteção de redes, dispositivos e dados contra acesso não autorizado ou uso criminoso (CISA, 2009). Uma definição mais adequada para a área industrial de Tecnologia Operacional é a proteção de redes, dispositivos, processos operacionais e pessoas contra acesso não autorizado ou uso criminoso, e a garantir operações seguras, contínuas (VERVE, 2020).

Goes (2019) indica que a automatização adotada por diversas indústrias na era 4.0 tem como consequência uma relação de dependência entre grande parte dos processos industriais, e o grande número de dados gerados, coletados e processados pelos sistemas inteligentes de informação. Desse modo, os impactos de possíveis

ataques que possam interferir nesses dados são motivo de grande preocupação por parte das organizações. Ele ressalta três características que são consideradas os pilares ao se trabalhar com segurança de informações:

- **Confidencialidade:** proteger o conteúdo da informação, permitindo o acesso apenas por pessoas autorizadas;
- **Integridade:** garantir que a informação permaneceu inalterada desde sua origem até o seu destino;
- **Disponibilidade:** fazer com que as pessoas tenham acesso à informação no mesmo momento que desejarem fazê-lo.

O autor também descreve as vulnerabilidades, que são as fragilidades em sistemas passíveis de serem exploradas para a realização de ataques, que geralmente visam atingir os pilares da segurança. A obtenção de informações sobre vulnerabilidades é particularmente facilitada em organizações que não priorizam as questões de cibersegurança, sendo essas comumente divulgadas em meios midiáticos ou em plataformas públicas de transparência.

Goes (2019) apresenta algumas medidas necessárias para se evitarem surgimento de ameaças:

- **Gestão da Segurança**: O item mais crucial para a cibersegurança industrial é o plano de segurança: um documento em que todos os cenários de possíveis ciberataques devem estar rigorosamente documentados, incluindo os seus impactos na organização, bem como conter planos de resposta já previamente testados. Também é interessante listar todos os equipamentos ligados à rede industrial, e identificar todas as suas vulnerabilidades e configurações de segurança. Os documentos devem ser divulgados entre os funcionários da indústria por meio de publicações internas;
- **Segurança de Periféricos**: Os periféricos de rede requerem muitos cuidados com a segurança. Uma boa medida é fazer um mapeamento detalhado da rede, e fazer sua estratificação entre diferentes grupos e subgrupos. Também é indispensável o uso de controles de acesso, além

de firewalls, que são pontos de conexão entre redes de forma monitorada e segura;

- **Segurança de Dados**: para garantir a estabilidade dos pilares da segurança de dados, é possível utilizar algumas soluções, tais como criptografia, mecanismos de dupla autenticação, hashing e Data Loss Prevention;
- **Atualização de Infraestrutura**: de nada adianta buscar soluções de segurança quando se utilizam máquinas ultrapassadas, então é recomendável que se esteja sempre substituindo equipamentos por versões mais atualizadas. Quando não for possível fazer a substituição de novos componentes, é possível utilizar outros recursos para fazer com que o nível de segurança seja mantido; por exemplo: em vez de efetuar a compra de um novo CLP, é possível adicionar um firewall à rede;
- **Cultura de Segurança**: o mais difícil de se obter a curto prazo; requer todo o processo de informar a todos os colaboradores sobre os possíveis riscos de cibersegurança, apresentando a importância de manter uma preocupação constante com essas questões, e assim, a manutenção da segurança deve se tornar uma rotina na organização. Sugere-se que sejam fornecidos palestras e workshops para os funcionários, para que gradativamente a cultura de segurança seja implementada.

Sobre periféricos, anteriormente mencionados, Laplante (2000, p. 367) os define como “dispositivos físicos ligados a um computador, utilizados para inserir ou extrair informações, ou ambos”.

1.5 Padrões de Segurança

Segundo Donda (2016), o intuito das normas de segurança da informação é o fornecimento e suporte de melhores práticas, diretrizes e princípios gerais, para que qualquer organização possa realizar a sua gestão. Essas normas são criadas por instituições padronizadoras nacionais e internacionais como por exemplo:

- **ISO** - *International Standardization Organization;*
- **IEC** - *International Electrotechnical Commission;*

- **ABNT** - Associação Brasileira de Normas Técnicas.

Para Mendoza (2017), existem vários benefícios quando se trabalha seguindo padrões de segurança:

- Padrões trazem um conjunto de melhores práticas que já foram testadas por especialistas e tiveram um resultado positivo;
- Colaboram com a melhoria contínua pois as atividades como documentar, monitorar, comunicar e medir são automáticas e otimizadas;
- Os padrões dão importância para proteção da informação e administração de riscos

Segundo Paz (2019) as normas ISO são certificações que garantem o cumprimento de exigências pelas empresas ao fornecer um produto, serviço ou sistema, garantindo a qualidade, é uma diretriz a ser seguida.

A seguir, são apresentados e discutidos alguns padrões e normas relativos à questão da cibersegurança:

ISA-99 (2007) é um relatório pertinente aos sistemas de automação e controle industrial, que caso seja ineficiente pode ter várias situações como por exemplo: ameaças à segurança pública ou de funcionários, perda de confiança do público, violação de requisitos regulatórios, perda econômica, perda de informações confidenciais e impacto na segurança nacional. Os padrões ISA auxiliam os profissionais de automação na otimização, melhoria de processos, segurança, eficiência e lucratividade, sendo assim reconhecido como fonte especialista em padrões para sistemas de automação e controle.

Segundo Baumier (2020) IEC 62443 / ISA-99 é o padrão mundial para segurança dos Sistemas de Controle Industriais, que beneficia às organizações com seus procedimentos, que ajuda a melhoria da segurança digital, processos e ambientes que utilizem os sistemas supervisórios SCADA, alavancando o nível de segurança do processo ou nos ambientes de produção.

Já o IEC 17799 é definido pela ABNT (2005) como um guia, que nele contém regras gerais para melhorar toda a gestão da segurança da informação passando pelas fases de iniciação, implementação e por manter a gestão, onde seus objetivos de controle atendem aos requisitos na análise de riscos,

A ABNT (2013) define que a norma ISO/IEC 27002, antiga IEC 17799, é o código de prática para a gestão de segurança da Informação, e tem como objetivo definir e criar um ciclo de princípios gerais que são: iniciar, implementar, manter e melhorar a gestão de segurança da informação, pois as informações são consideradas importantes para a continuidade e manutenção dos objetivos de negócio da organização.

Por outro lado, a ABNT (2015) diz que a ISO/IEC 27032 fornece as diretrizes para melhorar o estado de segurança cibernética e engloba: a segurança de informação; a segurança de rede; a segurança da internet; e a proteção da infraestrutura crítica de informação (CIIP). Essa norma fornece: uma visão geral de segurança cibernética; uma explicação da relação entre segurança cibernética e outros tipos de segurança; uma definição de parte interessada e descrição de seus papéis na segurança cibernética; orientação para abordar as questões comuns de segurança cibernética; e uma estrutura para qualificar os interessados a colaborar na resolução de questões de segurança cibernética.

A IEC 62443 divide as práticas de garantia de cibersegurança entre quatro categorias distintas, conforme o nível de cada uma:

- **Nível de Segurança 1**: são ocorrências não-intencionais, geralmente causadas por indivíduos que, por não possuírem conhecimento específico no assunto, cometeram alguma falha;

- **Nível de Segurança 2**: são os cibercrimes, que são todos aqueles crimes realizados em ambiente virtual, com uso de recursos da TIC. Geralmente cometidos por um único indivíduo, o *hacker*, que possui conhecimentos genéricos em cibersegurança;

- **Nível de Segurança 3**: entram nessa categoria as ações de terrorismo e ativismo, que são ciberataques realizados com intenções políticas ou ideológicas. Geralmente requerem uma equipe dedicada a esse propósito, com conhecimentos específicos a respeito de sistema de controles industriais;

- **Nível de Segurança 4**: nessa categoria se enquadram os ciberataques cometidos a nível de Estado, ou seja, possuem motivações geopolíticas, econômicas ou estratégicas em conflitos entre nações. Requerem equipes com profundos conhecimentos em diversas áreas, geralmente contando com o apoio militar.

Uma tabela com os padrões mais importantes da IEC 62443, para todos os níveis de segurança, pode ser consultada no Anexo A desta monografia.

1.6 Histórico de Ciberataques

McMillan (2010) descreveu a ação do Stuxnet, tido como o “vírus mais sofisticado já criado”, quando ele atingiu dezenas de computadores pessoais em uma usina nuclear no Irã. O vírus, que na realidade é um *worm* (um vírus auto replicante), tinha como objetivo interromper operações, além de roubar informações industriais confidenciais, e foi desenvolvido para atacar sistemas de controle da empresa Siemens. Inclusive acredita-se que os responsáveis por criar o vírus foram as inteligências dos EUA e Israel, a fim de sabotar o desenvolvimento do programa nuclear iraniano, visto que o Stuxnet tornava as centrífugas e tanques de enriquecimento de Urânio inoperáveis ao acelerá-las em até 40%. Por muito pouco não se deu início à Terceira Guerra Mundial.

O'Flaherty (2018) relatou um ataque ocorrido em agosto de 2017 em uma companhia petrolífera na Arábia Saudita. Por meio de um malware denominado “Triton”, os hackers - pessoas que realizam invasões intencionais a computadores - conseguiram invadir o sistema com intenções de sabotar as operações e, apenas por uma falha de código, por pouco não causaram uma explosão. O malware - software de caráter malicioso e prejudicial a um sistema - foi designado para atacar

especialmente os sistemas da empresa Schneider Electric, utilizados em mais de 18.000 usinas pelo mundo.

Mais recentemente, Sobczak (2019) contou sobre um ataque realizado à companhia de energia sustentável sPower, em Utah, nos EUA. Os hackers se aproveitam de uma brecha em um firewall - espécie de filtro de segurança que analisa e permite, ou bloqueia, determinadas operações em uma rede - de um sistema CISCO para interromper as operações na instalação, bem como romper as comunicações entre os geradores e a rede elétrica central.

Em março de 2020, conforme relatado por Goud (2020), sob o contexto de pandemia global, o Hospital Universitário de Brno, na República Tcheca, teve de enfrentar os vírus em dois planos distintos: biológico, e o virtual. O hospital subitamente perdeu a capacidade de transferir os dados dos pacientes para um banco de dados central, e o impacto foi tamanho que diversas intervenções cirúrgicas foram adiadas, além de novos pacientes terem de ser realocados para outras unidades. Apesar de oficialmente não haverem anúncios sobre a causa real do ataque, suspeita-se que seja um caso de *ransomware*, o que acontece quando alguém baixa algum arquivo infectado, e o vírus criptografa todos os arquivos de um dispositivo, liberando-os apenas mediante ao pagamento de um determinado valor em bitcoins.

1.7 Tipos de Ciberataques e o Mercado de Hackers

Segundo Branquinho et al. (2014), as ameaças cibernéticas exploram as infraestruturas dos sistemas, que são cada vez mais críticas, deixando em risco a segurança das informações. O risco à segurança cibernética pode afetar negativamente organizações, governos e as demais pessoas, podendo causar aumento de preços e falta de recursos para inovação e tecnologia.

Branquinho et al. (2014) também identificam o malware como um macro, por ser algo facilmente programado em muitas linguagens. O malware é definido como software malicioso, inventado para cruzar as barreiras de segurança de sistemas, com intenção de roubar informações ou simplesmente desaparecer com elas.

1.7.1 Tipos de Malware em Redes Industriais

- **Vírus** - Normalmente são ativados pelo usuário, são programas ou links maliciosos, muitas vezes em forma de algo atrativo para o usuário, como promoções, etc. Tem o objetivo de prejudicar sistemas ou inclusive roubar informações, espalhando-se através da rede para outros computadores (POZZEBOM, 2014);

- ***Worm*** - Segundo Barbosa, Costa e Santos (2005), a principal característica dos vírus de espécie *worm* é se auto replicar através da rede, e-mails, e outros tipos de plataformas. Ele não necessita de hospedeiro, como outro vírus comum, pois se propaga sozinho;

- **Cavalo de Troia (Trojan)** - Os trojans possuem esse nome por serem códigos maliciosos, mas que são transferidos para o computador por se passarem por softwares e arquivos legítimos. Podem realizar diversas ações maliciosas nos computadores e sistemas, como apagar arquivos, roubar senhas e dados de cartões de crédito sem o conhecimento do usuário. Eles também têm o poder de incluir *backdoors* (porta dos fundos), deixando o computador vulnerável ao total controle de quem está fazendo o ataque. Contudo, não são auto replicantes, como os vírus (BARBOSA; COSTA; SANTOS, 2005);

- ***Spyware*** - Os *Spywares* normalmente vêm embutidos em softwares e sites pouco confiáveis, não são denominados vírus, mas podem ser bastante perigosos porque monitoram e capturam informações sobre quem está utilizando o computador ou sistema, como dizem Barbosa, Costa e Santos (2005);

- ***Keylogger* e *Screenlogger*** - Segundo Pozzebom (2014) eles são aplicativos que têm o objetivo de capturar o que é digitado no teclado, capturam senhas e logins, ficam alojados na memória do computador, e enviam os dados para seus criadores. Podem vir inseridos em outros softwares e instalados automaticamente;

- ***Backdoor*** - Conforme Pozzebom (2014) ele é utilizado por outros malwares para conseguir acesso aos sistemas e redes que sejam infectadas. Os backdoors podem identificar falhas críticas em programas, e no firewall do sistema operacional, conseguindo abrir portas do roteador entre outros. A identificação dessas falhas garante o acesso irrestrito do cracker para roubo de dados;

- **Stuxnet** - Pozzebom (2014) defende que o Stuxnet foi programado para atacar um sistema específico SCADA, criado pela empresa Siemens em 2010, para que provocasse rachaduras nas centrífugas de enriquecimento de urânio do Irã. Considerado um dos vírus mais complexos, por ter dados muito específicos, não pode ter sido desenvolvido por qualquer pessoa, sua programação é beneficiada de informações distintivas da usina, acredita-se que algum governo quisesse adiar a produção da bomba atômica, e que tenha mandado criar o programa para esse objetivo.

1.7.2 Mercado do cibercrime

Existe uma parcela crescente no mercado ilegal exclusivamente dedicada ao oferecimento de cibercrimes. “Serviços de *hacking*, aluguel de *botnets*, ataques DDoS, lavagem de criptomoedas, bem como a venda de *exploits*, servidores e informações, são alguns dos produtos e serviços oferecidos por cibercriminosos na *dark web*” (WELIVE, 2020).

Atualmente o cibercrime está cada vez mais complexo, e é um setor em crescente escala. Segundo a Accenture 2018, os ataques cibernéticos custam US $13 milhões em prejuízos para uma organização, e esses números só tendem a aumentar (WELIVE, 2020).

Normalmente um grupo de cibercriminosos possui 10 integrantes, cada qual com uma série de funções específicas. Citando alguns “cargos”: existem os desenvolvedores de programas maliciosos; os *spammers* que lidam com a distribuição dos malwares, links e e-mails falsos; os responsáveis pela infraestrutura que mantém

o grupo anônimo; o setor operacional e o suporte; e por fim o financeiro, que cuida do dinheiro arrecadado com os ataques (WELIVE, 2020).

Existe também o recrutamento de “mulas” - na maioria das vezes, são pessoas comuns que acessam e-mails ou links tendenciosos, a fim de ganhar dinheiro fácil através da internet, sem muitos esforços. Deve-se sempre ter cuidado com anúncios na rede, e desconfiar de qualquer oferta de dinheiro oferecida por estranhos na internet (WELIVE, 2020).

1.7.3 Dispositivos USB como Fontes de Malware

Conforme Perekalin (2019), os pen drives e dispositivos USB são as formas mais comuns de ataques a sistemas industriais. Na maioria dos casos de ataques de malware, é comum estarem relacionados com o aparecimento de um desses dispositivos na planta industrial sem qualquer explicação. Um cenário real, e totalmente evitável caso a segurança ideal fosse aplicada, é quando um funcionário usa um *pen drive* para baixar um filme em seu horário de descanso, e acaba infectando o sistema de uma usina nuclear (PEREKALIN, 2019).

Segundo Perekalin (2019), qualquer tipo de dispositivo USB é facilmente manipulado, podendo se tornar uma arma à base de trojans designada para realizar ataques a redes e sistemas de indústrias. Com a criação dos dispositivos USB em 2010, os hackers identificaram que criar uma versão desse instrumento programada para inserir malwares seria relativamente fácil, pois os dispositivos eram capazes de se tornar discos rígidos dos computadores nos quais eram inseridos. A partir daí começam ser produzidas as versões modificadas dos *pen drives* cada vez mais poderosas, entre elas a Kautilya, Rubberducky, e Bunny, que foi utilizada em ataques a caixas eletrônicos (PEREKALIN, 2019).

A maioria das pessoas não se preocupam ao conectar periféricos como mouses e teclados em seus computadores, e esse foi o motivo que impulsionou o hacker criador do PHUKD a inventar um mouse infectado com *trojans*, tornando ainda mais fácil a invasão de redes e sistemas. A segunda geração das versões programadas entre os anos de 2014 e 2015 se tornaram ainda menores, cabiam

dentro de um cabo USB, a rumores que os dispositivos TURNIPSCHOOL e o Cottonmouth foram criados pela Agência de Segurança Nacional dos Estados Unidos (PEREKALIN, 2019).

Os dispositivos manipuláveis mais modernos, agora em sua terceira geração, funcionam através de conexão Wi-Fi. O hacker pode manipular e atacar de onde estiver, tudo através de acesso remoto, tornando ainda mais fácil a invasão a diversos sistemas. Algumas dessas novas ferramentas são: WHID Injector e P4wnP1. Esses dispositivos pequenos podem ser muito perigosos, sendo capazes de comprometer a rede inteira de uma empresa, roubar dados de segurança, e inserir programas de vigilância de vídeo e áudio (PEREKALIN, 2019).

Algumas formas de proteger os sistemas e infraestruturas das ameaças via dispositivos USB, é usar abordagem multicamadas, começando pela parte física com bloqueio de portas USB, para que não seja possível o acesso de qualquer pessoa. Também é recomendável evitar a troca de dispositivos periféricos como mouse e teclado, que normalmente já são analisados pela equipe de segurança. Além disso, é importante capacitar os colaboradores, ensinando-os sobre as formas de ataques, sobre a segmentação correta da rede com níveis de acesso, e a utilizar soluções para detectar diferentes tipos de ameaças (PEREKALIN, 2019).

1.8 Ferramentas para desenvolvimento web

A seguir são apresentadas as discussões relativas à parte técnica deste projeto, tecnologias que são utilizadas na construção de sites.

1.8.1 HTML

Segundo Longen (2019), HTML é a principal linguagem de marcação da internet, e possibilita a organização e formatação de documentos para páginas web. Ela não é considerada uma linguagem de programação, pois não é utilizada para a criação de funcionalidades, mas sim para a marcação de hipertexto, ou seja, a estrutura a maneira que os documentos são apresentados nas páginas. Vale ressaltar

que apenas o HTML não é suficiente para se criar um website, mas funciona muito bem em conjunto com outras duas linguagens de *front-end*: o CSS e o JavaScript.

1.8.2 CSS

Gonçalves (2019) descreve o CSS como uma linguagem para estilizar os elementos escritos de uma linguagem de marcação, neste caso, o HTML. O CSS é o responsável pelo design da página web, responsável por características como: a cor do texto; fundo; fontes; espaçamentos; tabelas; imagens; e variações de layouts. Não é tecnicamente uma necessidade, porém um site sem CSS tem um aspecto visual desagradável para um usuário.

1.8.3 JavaScript

Segundo Silva (2015) JavaScript é uma linguagem cuja característica principal é permitir rodar programas localmente no dispositivo do usuário, fornecendo às páginas web a possibilidade de programação, transformação e processamento de dados enviados e recebidos. Os *scripts* são uma série de instruções em código para que uma máquina as realize automaticamente. Há alguns deles, por exemplo, que permitem atualizar parte do conteúdo de uma página sem ter que carregá-la totalmente.

1.8.4 WordPress

Conforme Souza (2020), os empreendimentos de tamanhos diversos hoje têm a possibilidade de ter um site eficiente com o apoio do WordPress, criado em 2003, que é a plataforma mais popular de criação e gerenciamento de websites. Esse fenômeno se deve à transformação digital, que mudou a relação entre consumidores e empresas, e que agora se amplificou na internet. Pode-se dizer então que, essencialmente, o WordPress é uma ferramenta que integra as principais tecnologias de desenvolvimento e gerenciamento de páginas web, como HTML, CSS, JavaScript e MySQL.

Souza (2020) mostra os números referentes à plataforma *WordPress*, utilizando uma ferramenta denominada *Built With,* ferramenta que exibe a porcentagem de mercado que é ocupada por determinado sistema. Na lista que indica os sites com maior tráfego na internet, o *WordPress* está colocado:

- Entre 10 mil primeiros colocados - 39.75%;
- Entre 100 mil - 37.73%;
- Entre 1 milhão - 33.39%.

1.8.5 Banco de Dados

Para a manutenção e organização dos dados de arquivos em uma página web, é necessária a criação de um banco de dados, conforme explicado por Souza (2020). Para o desenvolvimento de um banco de dados com aplicação *web*, a melhor linguagem a ser utilizada é a MySQL, pois ela garante a segurança e organização dos dados armazenados, o que leva a uma melhor performance e experiência no website.

E, para que seja realizada a integração do banco de dados com a página em si, bem como sua administração, é necessário o uso do aplicativo phpMyAdmin. Essa ferramenta foi desenvolvida a partir da linguagem PHP, voltada principalmente para o desenvolvimento web, e que realiza o acesso e a gravação no banco por meio de *scripts*.

2 METODOLOGIA

Neste capítulo são apresentadas as considerações relativas à metodologia adotada para o desenvolvimento deste Trabalho de Conclusão de Curso, o projeto intitulado **Cibersegurança na Indústria 4.0: Criação de Website Informativo**. Tais considerações englobam métodos, procedimentos, técnicas e etapas necessárias para o planejamento e consecução do trabalho.

Para o embasamento teórico deste capítulo, foram utilizadas as contribuições de Prodanov e Freitas (2013), e de Flick (2013). Toda a redação desta monografia baseia-se nas normas da ABNT, obtidas a partir do Manual de Normalização de Projeto de Trabalho de Graduação da Fatec SBC (RICCI, CARVALHO e PEREIRA, 2017).

2.1 Classificação da pesquisa

Trata-se de uma pesquisa aplicada, com vistas ao desenvolvimento de um informativo em uma plataforma web para instruir aos colaboradores da indústria 4.0 sobre os temas relacionados à cibersegurança, com caráter explicativo.

Quanto aos procedimentos técnicos (*design* da pesquisa), este trabalho pode ser classificado como:

- Pesquisa bibliográfica, com a discussão das contribuições de autores da área;
- Pesquisa experimental, com vistas ao desenvolvimento de um produto tecnológico.

2.2 Descrição do projeto

Este projeto trata da criação de um informativo em uma plataforma web. O usuário pode encontrar os conceitos de cibersegurança explicados de forma simples, com o auxílio de recursos gráficos. Também é possível encontrar informações sobre os tipos de ciberataques, bem como maneiras de se prevenir deles.

O portal contém um painel com os principais tópicos da cibersegurança, como o seu conceito, exemplos de riscos, maneiras de prevenir e exemplos de ataques mais recentes. O painel também conta com recursos gráficos para auxiliar na abordagem dos assuntos apresentados. A interação com o usuário é feita por meio da rolagem da página (para baixo, para cima).

Para o desenvolvimento do website, foi utilizada a plataforma WordPress, que é responsável por integrar as tecnologias e linguagens de criação e gerenciamento de websites. A construção das páginas foi realizada com base nas linguagens HTML, CSS, PHP e JavaScript.

O banco de dados é modelado através da linguagem MySQL, e sua conexão com o website se dá com a linguagem PHP. Uma vez definido um plano para a hospedagem do site, a conexão pode ser alterada conforme as condições do serviço.

Quanto à hospedagem, foi realizada localmente com o auxílio do software XAMPP, que funciona como um gerenciador de serviços de hospedagem, como o MySQL e PHP. Agora com a estrutura do website finalizada migrado para um servidor de hospedagem, está efetivamente acessível através da internet.

2.3 Etapas para o desenvolvimento do projeto

As seguintes etapas foram realizadas para o trabalho, englobando aspectos teóricos e práticos:

a) Revisão da bibliografia;

b) Fichamento dos dados bibliográficos;

c) Comparação dos autores;

d) Planejamento técnico do projeto (documentação preliminar, materiais, recursos e ferramentas necessários, fases previstas do trabalho);

e) Desenvolvimento - construção do projeto, destacando as fases que o compõem, o passo a passo de sua realização;

f) Análise e discussão dos resultados;

g) Redação final do trabalho e revisão.

2.3.1 Etapas teóricas

A parte da pesquisa bibliográfica (etapas a), b) e c) anteriormente colocadas) foi a primeira atividade desenvolvida depois da delimitação do tema/problema, englobando consultas a sites especializados, manuais, livros, artigos científicos, teses e dissertações universitárias etc., além de livros relativos à metodologia científica.

Todo o material consultado foi fichado e configurou-se como a base para o Capítulo 1 desta monografia (Fundamentação Teórica).

2.3.2 Etapas práticas

As etapas práticas - itens e), f), g) acima - fazem parte do desenvolvimento do projeto (Capítulo 3).

O item d) - Planejamento técnico do trabalho - refere-se à organização do projeto, fazendo parte deste capítulo 2 (Metodologia). Esse planejamento foi feito no quinto semestre.

A seguir é apresentada a previsão das fases metodológicas para o desenvolvimento deste TCC.

Primeira fase - escolha dos instrumentos:

O site foi desenvolvido com o sistema WordPress, com o auxílio de ferramentas estruturais, como o emulador de servidor *web* XAMPP.

Segunda fase - pesquisa de conteúdo:

Foi realizado um trabalho de pesquisa para se escolher todo o conteúdo que é abordado no site, como: histórico de ciberataques; tipos de ciberataques; e boas práticas para sua prevenção. Também foram incluídas as pesquisas por imagens de fundo.

Terceira fase - correção do conteúdo:

O conteúdo coletado para preencher as páginas a respeito dos tópicos tratados neste trabalho, foi devidamente revisto, corrigido e catalogado, para depois ser implementado na página.

Quarta fase - desenvolvimento do *back end* e banco de dados:

Foi feita a instalação das ferramentas necessárias para o desenvolvimento da página web, já definidas anteriormente. O ambiente foi preparado para o desenvolvimento. Aqui também foi criado o banco de dados, para que fosse possível a organização dos arquivos do site inseridos a partir do *front end*, como textos, imagens e documentos.

Quinta fase - importação de conteúdo:

O conteúdo adquirido, como textos e imagens, é efetivamente enviado para o banco de dados, e posteriormente para o *front end.*

Sexta fase - desenvolvimento do *front end*:

No desenvolvimento do website efetivamente foram implementadas as características visuais como: layout; fontes; cores; e imagens. Também foram acrescentados os conteúdos teóricos pesquisados anteriormente referentes à cibersegurança. Os arquivos utilizados na elaboração das páginas foram organizados no banco de dados.

Sétima fase - alocação em servidor web:

O site foi exportado para um servidor web, a partir do uso de um serviço de hospedagem. Assim, ele já está disponível para o acesso através da internet.

Oitava fase - testes:

A versão inicial do website foi finalizada e imediatamente se iniciou a fase de testes. Os voluntários, além de verificar o acesso ao website, relataram as suas impressões e sugeriram pontos de melhoria.

Nona fase - correção das falhas detectadas nos testes:

Após o resultado dos testes, o feedback obtido serviu como um guia para a localização de pontos de melhoria na página.

Décima fase - nova aplicação de testes:

A fim de verificar a efetividade das melhorias feitas na última etapa, os mesmos testes foram repetidos.

3 DESENVOLVIMENTO DO PROJETO

Esse capítulo irá abordar as etapas do projeto no ambiente virtual e suas funcionalidades, separadamente pelos seguintes tópicos, respectivamente: discussão, informações técnicas, histórico do desenvolvimento e resultados.

3.1 Discussão

A abordagem do tema das Revoluções Industriais é algo de grande importância, por serem as responsáveis por trazer para a sociedade o desenvolvimento tecnológico, tanto em produtos quanto em serviços. Além do surgimento e desenvolvimento das tecnologias proporcionado pela indústria 4.0, a necessidade de proteção dos ataques cibernéticos que juntamente surge com elas.

As redes de computadores se tornam aliados necessários para o crescimento e implantação tecnológica dentro das indústrias, o que é refletido pela quantidade de pessoas e processos interconectados por elas. Contudo, proporcional ao crescimento decorrente da expansão das redes de computadores, é o crescimento de suas vulnerabilidades.

Existe uma série de ameaças que podem colocar em risco a confidencialidade, integridade e disponibilidade dos dados e operações de uma indústria. Intencionais ou não, elas sempre irão explorar as diversas fragilidades decorrentes de falhas tecnológicas, de processos ou de pessoas, e por isso existem diversos meios para minimizá-las, como: estabelecer planos de segurança; estratificar as redes e utilizar zonas desmilitarizadas; manter a infraestrutura tecnológica atualizada; e, acima de tudo, cultivar uma cultura de cibersegurança entre os colaboradores da indústria.

Isso tudo exige que seja estabelecido um alto rigor no que diz respeito às normas e padrões de cibersegurança, e por isso existem órgãos internacionais dedicados justamente para essa finalidade. Além disso, é comprovado que há diversas práticas como a gerência com as melhores ferramentas disponíveis no mercado, e a utilização de recursos para documentar, monitorar, comunicar e medir

os processos industriais, são de grande auxílio para administrar melhor os riscos e manter os padrões de cibersegurança.

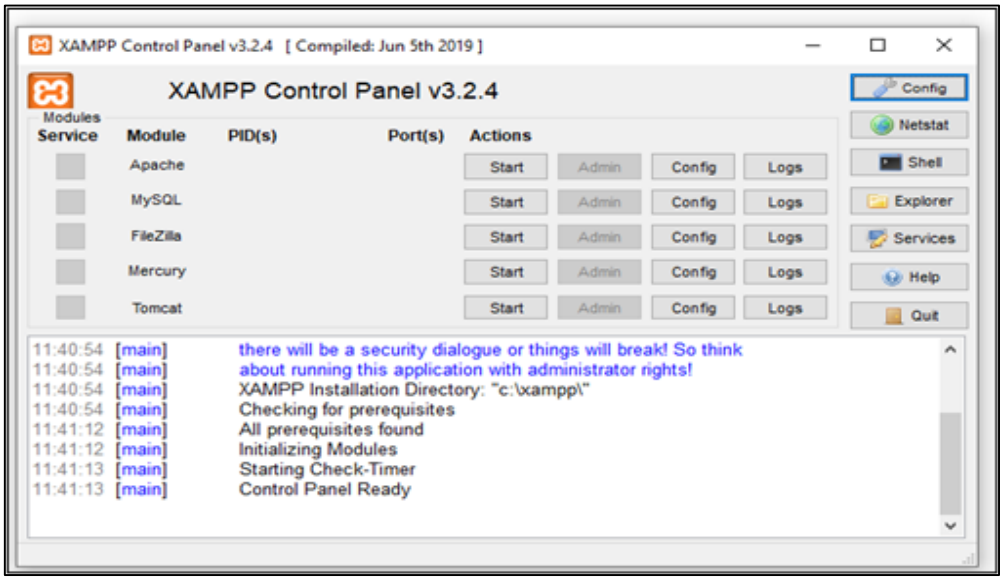
A caracterização do site partiu do princípio de que as empresas brasileiras não têm acesso a ferramentas de informação gratuitas que sejam totalmente voltadas a instruí-las sobre formas de se defender de ameaças cibernéticas, e por isso o informativo web será uma forte arma para essas empresas contra ciberataques.

3.2 Construção da Página Web

No início do desenvolvimento prático do projeto, definiu-se o objetivo do site, o desenvolvimento de um website informativo sobre cibersegurança na indústria 4.0, assim como sua estrutura principal e layout.

Antes da construção do site definitivo, optou-se pela criação de uma página de testes localmente em um computador. Para tanto, foi preciso preparar o ambiente local, o que foi feito através da instalação da ferramenta XAMPP, um emulador de servidor web Apache, com banco de dados MySQL e PHP, conforme pode ser conferido na figura a seguir:

Figura 3.1 - Painel de controle do XAMPP



Fonte: Autoria Própria, 2021

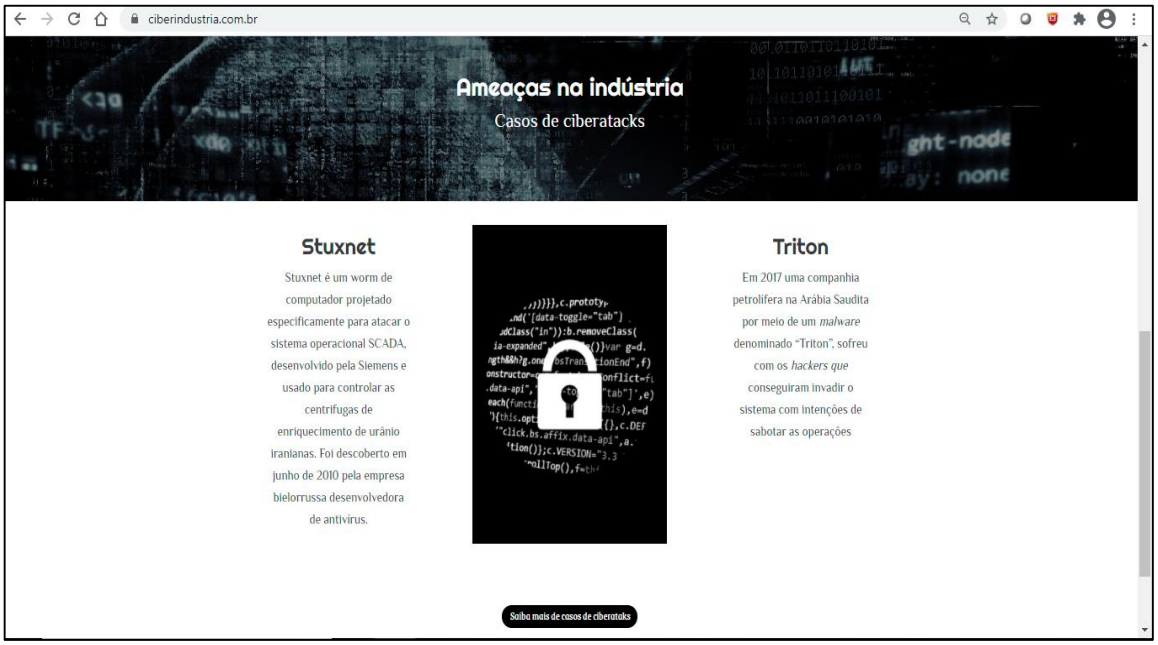
Em seguida, foi necessário baixar e configurar o WordPress, um aplicativo utilizado para facilitar a criação e administração de websites, além disso foi necessária a instalação de plugins para facilitar o trabalho, como: Classic Editor; Microthemer; e Ultimate Addons for Gutenberg. Assim, já estava tudo pronto para iniciar a construção e modelagem da página de testes.

Na página inicial, é possível ver uma barra de menus na parte superior da tela, com links que levam a cada uma das seções do site: “Home”; “Notícias”; “Conceitos Gerais”; “Boas Práticas”; “Padrões de Segurança”, “Tipos de Malware”, e “Quem Somos”, conforme exibido na figura 3.2. Rolando a página para baixo, há uma área “Ameaças na Indústria”, destacando alguns casos importantes de ciberataques, e logo abaixo há um link que leva à página “Histórico de Ciberataques”, que reúne uma listagem mais ampla de incidentes de cibersegurança industriais, o que pode ser visto na figura 3.3.

Figura 3.2 - Tela Inicial do site ciberindustria.com.br

Fonte: Autoria Própria, 2021

Figura 3.3 - Tópico “Ameaças na indústria”



Fonte: Autoria Própria, 2021

Já em “Notícias”, o usuário poderá encontrar quadros com links para as principais notícias envolvendo cibersegurança e indústria 4.0, através do botão “Leia Mais”, bem como as suas respectivas fontes, caso queira ler a notícia completa. A interação do usuário com essa página poderá ser feita por meio da barra de rolagem, e clicando nos botões. A Figura 3.4 mostra a aba “Notícias”:

Figura 3.4 - Aba “Notícias”

Fonte: Autoria Própria, 2021

A aba de “Conceitos Gerais” possui um caráter teórico, pois aborda de maneira informativa os principais conceitos relacionados à cibersegurança e indústria 4.0, como: “Revoluções Industriais”; “Redes”; “Cibersegurança”; “Padrões e Normas de Segurança”; e “Tipos de Malwares”. Nesta página, os conteúdos são dispostos em forma de tópicos, de maneira que o usuário poderá usar a barra de rolagem, e clicar no botão “saiba mais” ao lado do tópico desejado. Assim, ele será redirecionado a uma outra página, a qual explicará sobre o conceito escolhido de maneira mais detalhada. A Figura 3.5 mostra a aba “Conceitos gerais”:

Figura 3.5 - Aba “Conceitos gerais”

Fonte: Autoria Própria, 2021

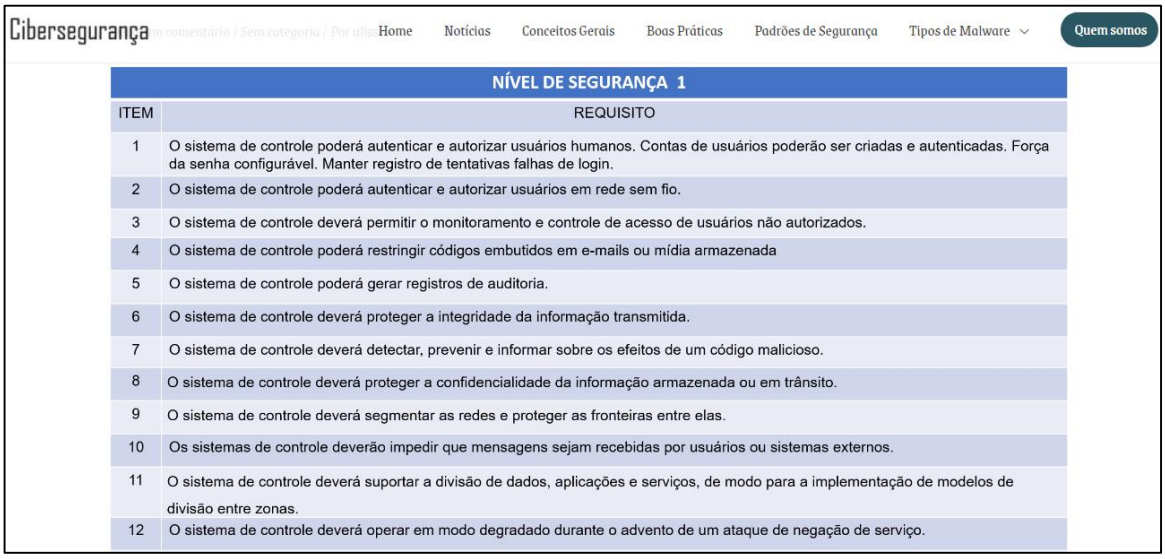
A página “Boas Práticas” reúne uma tabela com algumas das mais importantes e recomendadas práticas para manutenção da segurança cibernética de uma indústria, envolvendo as áreas de dados, redes, operações e pessoas. Para a sua leitura, o usuário deverá apenas realizar a rolagem para baixo. A Figura 3.6 mostra a aba “Boas práticas”:

Figura 3.6 - Aba “Boas práticas”

Fonte: Autoria Própria, 2021

A aba de “Padrões de Segurança” trata a respeito de algumas das normas de cibersegurança conforme definidas por instituições padronizadoras nacionais internacionais, como a ISO e a IEC. Ao final da página, o usuário poderá encontrar um link que o levará a uma tabela em alguns dos padrões de cibersegurança definidos pela IEC 62443, conforme exibido na figura 3.7:

Figura 3.7 - Aba “Padrões de Segurança”

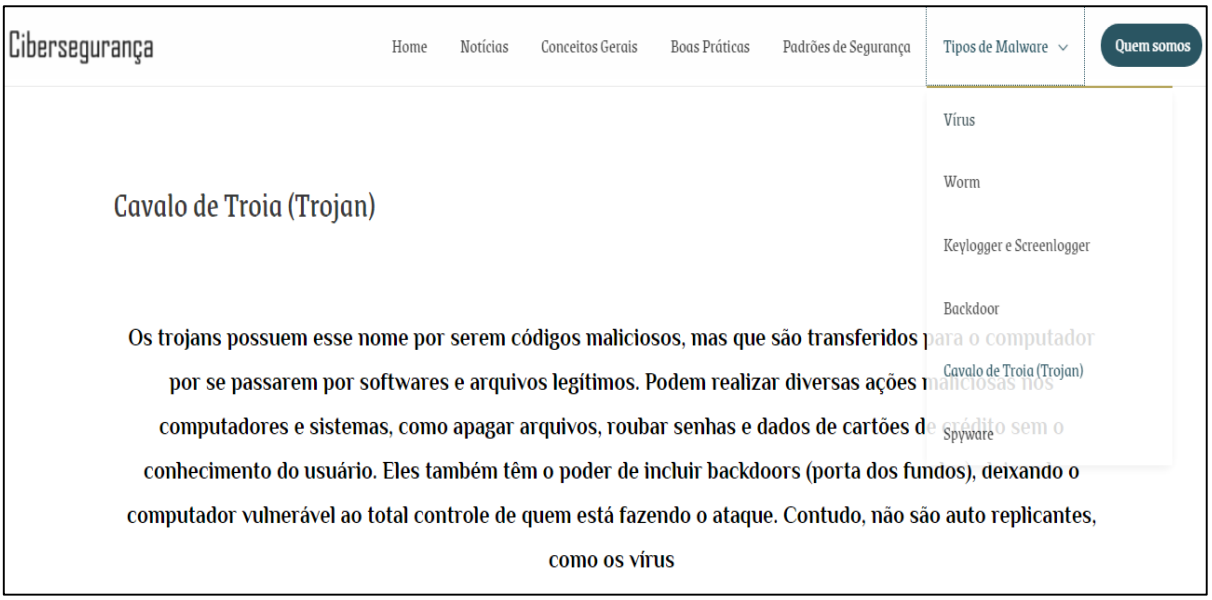


NÍVEL DE SEGURANÇA 1	
ITEM	REQUISITO
1	O sistema de controle poderá autenticar e autorizar usuários humanos. Contas de usuários poderão ser criadas e autenticadas. Força da senha configurável. Manter registro de tentativas falhas de login.
2	O sistema de controle poderá autenticar e autorizar usuários em rede sem fio.
3	O sistema de controle deverá permitir o monitoramento e controle de acesso de usuários não autorizados.
4	O sistema de controle poderá restringir códigos embutidos em e-mails ou mídia armazenada
5	O sistema de controle poderá gerar registros de auditoria.
6	O sistema de controle deverá proteger a integridade da informação transmitida.
7	O sistema de controle deverá detectar, prevenir e informar sobre os efeitos de um código malicioso.
8	O sistema de controle deverá proteger a confidencialidade da informação armazenada ou em trânsito.
9	O sistema de controle deverá segmentar as redes e proteger as fronteiras entre elas.
10	Os sistemas de controle deverão impedir que mensagens sejam recebidas por usuários ou sistemas externos.
11	O sistema de controle deverá suportar a divisão de dados, aplicações e serviços, de modo para a implementação de modelos de divisão entre zonas.
12	O sistema de controle deverá operar em modo degradado durante o advento de um ataque de negação de serviço.

Fonte: Autoria Própria, 2021

E a aba “Tipos de Malware”, por sua vez, contém um menu que contém alguns dos diversos tipos de malware existentes, como “Vírus”, “Worm” e “Trojan”. Cada item levará o usuário a uma página que exibe algumas das principais informações sobre o malware escolhido, como se pode observar pela figura 3.8:

Figura 3.8 - Aba “Tipos de Malware”



Fonte: Autoria Própria, 2021

Por último, a página “Quem Somos” exibe os responsáveis pelo desenvolvimento do projeto, bem como um link sobre o qual o usuário poderá clicar, levando-o para a página pessoal de cada um na rede social LinkedIn. Após a rolagem, no final da página será possível ver um endereço de e-mail para contato, caso o usuário deseje comunicar-se com os desenvolvedores do projeto. A Figura 3.9 mostra a aba “Quem somos”:

Figura 3.9 - Aba “Quem Somos”

Fonte: Autoria Própria, 2021

Após a criação local da página web, foi contratado um plano de hospedagem para que se realizasse a migração do website para um servidor web. Para isso, inicialmente foi instalada a ferramenta WordPress no painel de controle oferecido pela própria empresa de hospedagem. Em seguida foi instalado tanto no site hospedado, quanto no site local, um plugin chamado All in One WP Migration, para que ele pudesse criar uma cópia da página local, e em seguida replicá-la no servidor contratado. Assim, foi feita uma duplicação do website hospedado localmente no website do serviço contratado, mantendo-se as configurações, imagens, textos etc.

3.3 Histórico do desenvolvimento

O projeto foi dividido em várias etapas, com o total de tempo de desenvolvimento equivalente a um ano. Foi utilizado o software Project para construir um cronograma, organizar e dividir as tarefas. Todas as atividades programadas foram executadas conforme planejado, sendo que, quando possível, algumas tarefas foram antecipadas ou alteradas na forma de execução, mas sempre focando nas tarefas prioritárias, de acordo com o Quadro 3.1:

Quadro 3.1: Histórico do Desenvolvimento

Agosto 2020	• Entrega da ideia do projeto; • Aprofundamento do tema Cibersegurança na indústria 4.0; • Elaboração do cronograma no Project.
Setembro 2020	• Início da Fundamentação Teórica; • Início da Metodologia.
Outubro 2020	• Início da Introdução; • Início do Curso online de WordPress.
Novembro 2020	• Conclusão da Redação do TCC parte I; • Validação com o orientador.
Dezembro 2020	• Entrega da Versão Final do TCC parte I; • Conclusão do Curso online de WordPress; • Criação do Site.
Janeiro 2021	• Ajustes e testes no produto final do Site.
Fevereiro 2021	• Resumo da Monografia; • Abstract da Monografia.
Março 2021	• Migrar Site para o domínio definitivo; • Produção do artigo; • Início do desenvolvimento da monografia; • Início das Considerações Finais; • Entrega dos documentos com as assinaturas digitalizadas; • Testes no site.
Abril 2021	• Produção dos vídeos das apresentações do projeto; • Entrega filme de comprovação da execução do projeto; • Entrega da versão completa da monografia e artigo.

maio 2021	• Correções da monografia completa; • Correções do Artigo; • Entrega do vídeo para a defesa na banca; • Revisão da monografia.
Junho 2021	• Entrega final do pen drive com a monografia e artigo.

Fonte: Autoria própria.

3.4 Resultados

O desenvolvimento desse projeto resultou na criação de um website sobre a cibersegurança na indústria 4.0, que tem como público-alvo os profissionais da indústria, assim como os entusiastas da TIC. O website conta com os vários tópicos e conceitos abordados durante a pesquisa, para ajudar a ilustrar os casos de cibersegurança e para entender a importância de se preparar para esse desafio enorme que a indústria tem.

A falta de conhecimento sobre hospedagem dificultou na hora de colocar o site no ar, e foi preciso buscar auxílio do suporte da empresa, porém este processo se deu sem maiores dificuldades. A escolha para uma plataforma de gerenciamento de conteúdo trouxe um ganho na produtividade do desenvolvimento, pois a criação não precisou ser realizada através de linhas de código, e sim pelo Gutenberg, que é um editor para o WordPress com blocos simples e intuitivos.

Este projeto final se trata de algo extremamente necessário para o momento atual, pois ao longo das pesquisas realizadas, foi constatado que não existe qualquer outro site em português voltado exclusivamente para reunir informações sobre cibersegurança e ciberataques na indústria 4.0. Assim, este informativo web pode vir a se tornar uma forte arma na luta contra as ameaças cibernéticas.

3.5 Trabalhos futuros

Algumas ações planejadas para implementação futura são:

- Adicionar uma área para comentários nas páginas;
- Acrescentar uma página com bate-papo para interações entre usuários, incentivando a criação uma comunidade de cibersegurança;
- Espaço para divulgações, como uma página destinada a cursos, palestras e serviços de empresas parceiras que queiram utilizá-lo.

CONSIDERAÇÕES FINAIS

Este projeto surgiu a partir da observação do crescente número de casos de ciberataques industriais, decorrentes principalmente das vulnerabilidades provenientes da expansão tecnológica da Quarta Revolução Industrial. Entendeu-se que grande parte dos casos de incidentes com malwares ocorre pela desinformação por parte dos usuários, no caso, os colaboradores da indústria 4.0.

Assim, foi definido que o objetivo deste projeto seria a construção de uma plataforma web informativa totalmente em português, que reunisse as principais informações a respeito de temas relacionados à cibersegurança, para instruir e auxiliar aos envolvidos na indústria no combate às ameaças cibernéticas. Para tanto, o website deveria dispor as informações de maneira simples e intuitiva, e utilizando recursos gráficos como imagens, quadros e tabelas.

Foi estabelecida como primeira etapa o levantamento bibliográfico de todas as informações relevantes sobre o tema escolhido, para que assim o portal web fosse abastecido de conteúdo. Em seguida, foi necessário definir quais abas constariam no portal, para que o material obtido fosse efetivamente dividido, e neste momento foi observado que a cibersegurança é um tema que depende de constantes atualizações, sendo necessário que sempre estejam sendo feitas novas pesquisas.

Posteriormente, foi feita a construção efetiva do website, acessível apenas de um computador local, utilizando a tecnologia WordPress. É um sistema de gestão de conteúdo que permitiu que o desenvolvimento de todas as páginas fosse feito de maneira simplificada e visual, sem a necessidade de trabalhar com linhas de código.

Após a contratação de um serviço de hospedagem, o mesmo website desenvolvido localmente foi migrado para um servidor na internet, o que permitiu que todos os usuários que desejassem pudessem acessá-lo. Todo o conteúdo sobre cibersegurança levantado ao longo do projeto foi efetivamente adicionado e dividido entre as suas respectivas abas, para que possam servir de referência aos colaboradores da indústria 4.0.

REFERÊNCIAS

ARBULU, Rafael. Ciberataque faz hospital que tratava pacientes do coronavírus fechar as portas. **Canaltech**. São Bernardo do Campo, 16 mar. 2020. Disponível em: https://canaltech.com.br/seguranca/educacao-online-tambem-se-torna-alvo-para-criminosos-digitais-171018/. Acesso em: 03 set. 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. ISO/IEC 27002:2013:** tecnologia da informação, técnicas de segurança, código de práticas para controles de segurança da informação. Rio de Janeiro, 2013. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em: 28 mai. 2020.

_____. **ISO/IEC 27032:2012:** Tecnologia da Informação - Técnicas de segurança - Diretrizes para segurança cibernética, 09 jun. 2015. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=334079. Acesso em: 28 mai. 2020.

_____. **ISO/IEC 17799:2005:** Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação, 31 ago. 2005. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=306582. Acesso em: 28 mai. 2020.

BARBOSA, A. A.; COSTA, R. W. B.; SANTOS, R. **Ciências da Computação (1º período) [apostila]**: Pragas Digitais. Rio das Ostras: Universidade Federal Fluminense, 2005. 12 p. Disponível em: http://www2.ic.uff.br/~otton/graduacao/informaticaI/pragasdigitais.pdf. Acesso em: 24 out. 2020.

BAUMIER**. Soluções IEC 62443.** 2020. Disponível em: https://www.baumier.com.br/index.php/cesta/solucoes-iec-62443. Acesso em: 29 mai. 2020.

BEZERRA, Kleython Kell Vicente. *Firewall de nova geração: principais características e diferenciais tecnológicos*. 2015. 40p. Trabalho de Conclusão de Curso (Lato Sensu) - Centro Universitário de Brasília, Brasília, 2015.

BOETTCHER, M. Revolução Industrial - Um pouco de história da Indústria 1.0 até a Indústria 4.0. **Linkedin**. 26 nov. 2015. Disponível em:< https://www.linkedin.com/pulse/revolu%C3%A7%C3%A3o-industrial-um-pouco-de-hist%C3%B3ria-da-10-at%C3%A9-boettcher/?originalSubdomain=pt>. Acesso em: 29 set 2020.

BRANQUINHO, M. A. et al. **A. segurança de automação industrial e scada**. 1. ed. Rio de Janeiro: Elsevier, 2014.

BRETTEL, M. et al. How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. **International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering**. World Academy of Science, Engineering and Technology, v. 8, n. 1, p. 37-44, nov. 2014. Disponível em: https://doi.org/10.5281/zenodo.1336426. Acesso em: 10 mai. 2020.

CARDOSO, Ataide Pereira Junior; SACOMANO, José Benedito. Indústria 4.0 e a Internet das Coisas: Avaliação de Segurança dos Dispositivos. In: **ENEGEP**, 37., 2017, Joinville. **Anais eletrônicos.** Rio de Janeiro: ABEPRO, 2017. Disponível em: www.abepro.org.br/biblioteca/TN_STO_244_417_31524.pdf. Acesso em 25 mai. 2020.

CAVALCANTE, Z. V.; SILVA, M. L. S. da. **A importância da Revolução Industrial no mundo da Tecnologia. In:** ENCONTRO INTERNACIONAL DE PRODUÇÃO CIENTÍFICA, 7. 2011. Maringá. **Anais eletrônicos**. Maringá. 2011. Disponível em:< https://www.unicesumar.edu.br/epcc2011/wpcontent/uploads/sites/86/2016/07/zedequias_vieira_cavalcante2.pdf>. Acesso em: 10 mai. 2020.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **What is Cybersecurity?** Arlington: 2009. Disponível em: https://www.us-cert.gov/ncas/tips/ST04-001. Acesso em 24 mai. 2020.

DESRUISSEAUX, Daniel. **Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications.** Lake Forest: Schneider Electric, 2018. Disponível em: https://download.schneider-electric.com/files?p_Doc_Ref=998-20186845. Acesso em 05 out. 2020.

DONDA, Daniel. **Padrões e normas relacionadas à segurança da informação**. Daniel Donda, 29 fev. 2016. Disponível em: https://danieldonda.com/2016/02/29/padres-e-normas-relacionadas-segurana-da-informao/. Acesso em: 21 set. 2020.

MAYA, Alcides. **O que são redes de computadores**. Escola Técnica e Faculdade Alcides Maya, 2020. Disponível em: https://alcidesmaya.edu.br/blog/182-o-que-sao-redes-de-computadores. Acesso em: 24 out. 2020.

FERREIRA, Carlos. Revolução Industrial. **Todo Estudo**. Disponível em: https://www.todoestudo.com.br/historia/revolucao-industrial. Acesso em: 29 set. 2020.

FLICK, U. **Introdução à metodologia de pesquisa:** um guia para iniciantes. Porto Alegre: Penso, 2013.

FROTA, et al. **Indústria 4.0 no Brasil: oportunidades, perspectivas e desafios.** Rio de Janeiro: 2019. 63 p. Disponível em: https://www.firjan.com.br/lumis/portal/file/fileDownload.jsp?fileId=2C908A8A6895B4030168EC48A78E023D. Acesso em: 29 mai .2020.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores.** Amgh Editora, 2010.Disponível em: https://tpinformatica.com.br/site/2020/03/27/o-que-e-rede-de-computadores Acesso em: 23 out. 2020.

GEISSBAUER, D. R.; VEDSO, J.; SCHRAUF, S. Industry 4.0: Building the digital enterprise. **PWC**. Berlin, p. 8. 2016. Disponível em: https://www.pwc.com.br/pt/publicacoes/servicos/assets/consultoria-negocios/2016/pwc-industry-4-survey-16.pdf. Acesso em: 29 set. 2020.

GOES, Nuno. Cibersegurança na Indústria Nacional. **Robótica**. Porto: CIE, n. 114, p.56-62, jan./mar. 2019. Disponível em: http://www.robotica.pt/PDF/ROB114/dossier_.pdf. Acesso em: 24 mai. 2020.

GOMES, Pedro. **Principais protocolos de rede.** Opservices Ltda, 2019. Disponível em 29 mai. 2020. https://www.opservices.com.br/protocolos-de-rede/. Acesso em: 24 mai. 2020.

GONÇALVES, Ariane. **O que é CSS? Guia Básico para Iniciantes**. Hostinger, 16 ago. 2019. https://www.hostinger.com.br/tutoriais/o-que-e-css-guia-basico-de-css/. Acesso em: 22 out. 2020.

GOUD, Naveen. Details of CovidLock ransomware and Czech hospital infection. **Cybersecurity Insiders**. Baltimore, [2020]. Disponível em: https://www.cybersecurity-insiders.com/details-of-covidlock-ransomware-and-czech-hospital-infection/. Acesso em: 03 set. 2020.

INTERNATIONAL SOCIETY OF AUTOMATION. **ISA-99**: Segurança de sistemas de controle e automação industrial, 2007 Disponível em: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99. Acesso em: 28 mai. 2020.

KUROSE, James F.; ROSS, Keith W. **Rede de computadores e a Internet: uma nova abordagem**. 1 ed. São Paulo: Addison Wesley, 2003. Disponível em: http://www.univasf.edu.br/~edmar.nascimento/analise/analise_20121_aula01.pdf Acesso em: 29 mai. 2020.

LAPLANTE, Philip A. **Dictionary of computer science, engineering and technology**. Cleveland: CRC Press, 2000.

LEITE, Ana Marta Xavier Ferreira. **A Problemática da Cibersegurança e os seus desafios**. 2016. 22 f. Dissertação (Mestrado em Direito e Segurança) – Faculdade de Direito, Segurança e Democracia. Universidade Nova de Lisboa, Lisboa.

LONGEN, Andrei. O Que é HTML? Guia de Comandos HTML para Iniciantes. **WebLink**, 28 fev. 2019. Disponível em: https://www.weblink.com.br/blog/o-que-e-html/ . Acesso em: 22 out. 2020.

MATOS, Jhonata de Souza et al. **A Indústria 4.0 na economia brasileira: Seus benefícios, impactos e desafios.** 2018. 49p. Monografia (Bacharelado em Ciências Econômicas) - Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em: https://repositorio.ufu.br/bitstream/123456789/23894/1/Ind%C3%BAstriaEcnomiaBrasileira.pdf. Acesso em: 29 mai. 2020.

MEIRELLES, Fernando S. Pesquisa Anual do Uso de TI. São Paulo: FGV EAESP Pesquisa, 2020. Disponível em: https://eaesp.fgv.br/sites/eaesp.fgv.br/files/u68/fgvcia2020pesti-resultados.pdf. Acesso em 27 jun. 2020.

MENDOZA, Miguel, Ángel. **5 benefícios do alinhamento de processos com padrões de segurança**. welivesecurity, 16 jun. 2017. Disponível em: https://www.welivesecurity.com/br/2017/06/16/beneficios-alinhamento-padroes-seguranca. Acesso em: 28 mai. 2020.

MCMILLAN, Robert. Siemens: Stuxnet worm hit industrial systems. **Computerworld**. Framingham: IDG News, 14 set. 2010. Disponível em: https://www.computerworld.com/article/2515570/siemens--stuxnet-worm-hit-industrial-systems.html. Acesso em: 24 mai. 2020.
O'FLAHERTY, Kathy. How The Russian Government Created The Most Advanced Industrial Malware Ever Seen. **Forbes**. New Jersey: Forbes Media, 23 out. 2018. Disponível em: https://www.forbes.com/sites/kateoflahertyuk/2018/10/23/how-the-russian-government-created-the-most-advanced-industrial-malware-ever-seen/. Acesso em: 24 mai. 2020.

PAZ, Nathalia. **As normas ISO de cibersegurança que sua empresa deve seguir**. idblog, 2019. Disponível em: https://blog.idwall.co/normas-iso-ciberseguranca. Acesso em: 24 set. 2020.

PEREKALIN, Alex. **Dispositivos USB usados como vetor de ataque**. 24 abr 2019. Disponível em: https://www.kaspersky.com.br/blog/weaponized-usb-devices/11692/. Acesso em 14 nov. 2020.

PINTO, Amanda. Medium. **Estudo de caso de um centro de operação de geração de energia elétrica**. 07 ago. 2018. Disponível em: https://medium.com/@amandabhmg/seguran%C3%A7a-cibern%C3%A9tica-de-sistemas-de-controle-industriais-ea475c0eecbc Acesso em 06 out. 2020.

POZZEBON, Rafaela. **Diferenças entre: vírus, spam, spyware, worm, phishing, botnet, rootkit.** 10 jul. 2014. Disponível em: https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit . Acesso em: 23 out. 2020.

PRODANOV, C. C.; FREITAS, E. C. de. **Metodologia do trabalho científico:** métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

REIS, Rodrigo. **Modelo TCP/IP – Definição, camadas e funcionamento**. infotecnews, 2017. Disponível em: http://infotecnews.com.br/modelo-tcpip/. Acesso em: 24 out. 2020.

RICCI, Delcínio; CARVALHO, Edmilson de Souza; PEREIRA, Samáris Ramiro. **Manual de normalização de projeto de trabalho de graduação.** São Bernardo do Campo: Fatec, 2017. Disponível em: http://fatecsbc.edu.br/wp-content/uploads/2017/02/Manual_TCC_-_Revis%C3%A3o_2017_-_fev2017.pdf. Acesso em 30 out. 2020.

SAKURAI, R.; ZUCHI, J. D. As revoluções industriais até a indústria 4.0. **Revista Interface Tecnológica**, *[S. l.]*, v. 15, n. 2, p. 480-491, 2018. Disponível em: https://revista.fatectq.edu.br/index.php/interfacetecnologica/article/view/386. Acesso em: 24 set. 2020.
SILVA, Giancarlo. **Linguagem JavaScript?**. Canaltech, 28 jan. 2015. Disponível em: https://canaltech.com.br/internet/O-que-e-e-como-funciona-a-linguagem-JavaScript/. Acesso em: 22 out. 2020.

SILVA, M. C. A. da.; GASPARIN, J. L. **A Segunda Revolução Industrial e suas influências sobre a Educação Escolar Brasileira.** 2015. Disponível em:< http://www.histedbr.fe.unicamp.br/acer_histedbr/seminario/seminario7/TRABALHOS/M/Ma rcia%20CA%20Silva%20e%20%20Joao%20L%20Gasparin2.pdf>. Acesso em: 29 set. 2020

SILVEIRA, et al. **O Que é Indústria 4.0 e Como Ela Vai Impactar o Mundo.** Disponível em: https://www.citisystems.com.br/industria-4-0/. Acesso em: 27 mai 2020.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores: das LANs, MANs e WANs às redes ATM**. 2 ed. Rio de Janeiro: Campus, 1995. Disponível em: http://www. http://repositorio.ufla.br/jspui/dossier_.pdf. Acesso em: 28 mai. 2020.

SOBCZAK, Blake. First-of-a-kind U.S. grid cyberattack hit wind, solar. **E&E News**. Washington: E&E News, 31 out. 2019. Disponível em: https://www.eenews.net/stories/1061421301. Acesso em: 24 mai. 2020.

SOUSA, Rafaela. **Terceira Revolução Industrial**. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/geografia/terceira-revolucao-industrial.html. Acesso em: 29 set. 2020.

SOUZA, Ivan de. **História do WordPress: saiba como surgiu um dos maiores CMS do mundo**. Rockcontent, 21 set. 2020. Disponível em: https://rockcontent.com/br/blog/historia-wordpress/. Acesso em: 28 set. 2020.

_____. **Saiba o que é MySQL e como usar no site do seu negócio.** Rockcontent, 1 jul. 2020. Disponível em: https://rockcontent.com/br/blog/mysql/. Acesso em 31 out. 2020.

TEODORO, Viviane. **A Segunda Revolução Industrial**. Escola Educação. Disponível em: https://escolaeducacao.com.br/segunda-revolucao-industrial/. Acesso em: 29 set. 2020.

TORRES, Gabriel. **Redes de Computadores Curso Completo**. Axcel Books do Brasil Editora Ltda., 2001. Disponível em: http://www.http://repositorio.ufla.br/jspui/dossier_.pdf. Acesso em: 28 mai. 2020.

VENTURELLI, M. **Indústria 4.0: uma visão da automação industrial**. Automação Industrial, nov. 2017. Disponível em:< https://www.automacaoindustrial.info/industria-4-0- uma-visao-da-automacao-industrial/>. Acesso em: 29 set. 2020

VERVE INDUSTRIAL PROTECTION. **The State of OT Cyber Security**. Missouri, 2020. Disponível em: https://aaindustrial.com/resources/ebook/ebook-the-state-of-ot-cyber-security/. Acesso em 24 mai. 2020.

WE ARE SOCIAL. **Digital 2020: Brazil.** 2020. Disponível em: https://datareportal.com/reports/digital-2020-brazil. Acesso em 27 jun. 2020.

WELIVE SECURITY, **Dark web: produtos e serviços oferecidos por cibercriminosos**, 01 jun. 2020. Disponível em: https://www.welivesecurity.com/br/2020/06/01/dark-web-produtos-e-servicos-oferecidos-por-cibercriminosos/. Acesso em 23 out. 2020.

ANEXO A - PADRÕES DE SEGURANÇA DA IEC 62443:

NÍVEL DE SEGURANÇA 1	
Item #	**Requisito**
1	O sistema de controle poderá autenticar e autorizar usuários humanos. Contas de usuários poderão ser criadas e autenticadas. Força da senha configurável. Manter registro de tentativas falhas de login.
2	O sistema de controle poderá autenticar e autorizar usuários em rede sem fio.
3	O sistema de controle deverá permitir o monitoramento e controle de acesso de usuários não autorizados.
4	O sistema de controle poderá restringir códigos embutidos em e-mails ou mídia armazenada
5	O sistema de controle poderá gerar registros de auditoria.
6	O sistema de controle deverá proteger a integridade da informação transmitida.
7	O sistema de controle deverá detectar, prevenir e informar sobre os efeitos de um código malicioso.
8	O sistema de controle deverá proteger a confidencialidade da informação armazenada ou em trânsito.
9	O sistema de controle deverá segmentar as redes e proteger as fronteiras entre elas.
10	Os sistemas de controle deverão impedir que mensagens sejam recebidas por usuários ou sistemas externos.
11	O sistema de controle deverá suportar a divisão de dados, aplicações e serviços, de modo para a implementação de modelos de divisão entre zonas.
12	O sistema de controle deverá operar em modo degradado durante o advento de um ataque de negação de serviço.
13	Proibir funções, protocolos e serviços desnecessários.
14	Os sistemas de controle deverão realizar backup a níveis de usuário e sistema.

NÍVEL DE SEGURANÇA 2	
Item #	**Requisito**
1	O sistema de controle deverá autenticar e autorizar processos de softwares e dispositivos.
2	O sistema de controle deverá autenticar usuários humanos e softwares envolvidos na comunicação sem fio.
3	O sistema de controle deverá suportar o padrão ICP (Infraestrutura de Chaves Públicas) e autenticação baseada em certificados digitais, se utilizados.
4	O sistema de controle deverá negar solicitações de acessos de redes não-confiáveis, a menos que sejam aprovadas pelo responsável.
5	O sistema de controle deverá permitir que os usuários autorizados definam e modifiquem as permissões de acesso.
6	O sistema de controle deverá implementar proteção contra código malicioso em todos os pontos de entrada e saída da rede.
7	O sistema deverá proteger a integridade das sessões em rede.
8	O sistema de controle deverá proteger as informações auditadas.
9	O sistema de controle deverá proteger a confidencialidade durante acesso remoto a redes não-confiáveis
10	O sistema de controle deverá ter a capacidade de segmentar fisicamente as redes do sistema de controle das redes não associadas aos sistemas de controle.
11	O sistema de controle deverá gerar uma lista dos componentes instalados, juntamente com suas propriedades.

NÍVEL DE SEGURANÇA 3	
Item #	**Requisito**
1	O sistema de controle deverá suportar a verificação e autenticação multifator para interfaces não-confiáveis.
2	O sistema de controle deverá identificar e autenticar os processos de software de maneira única.
3	O sistema de controle deverá suportar o gerenciamento de contas unificado.
4	O sistema de controle deverá proteger chaves privadas usando mecanismos de hardware.
5	O sistema de controle deverá identificar e informar sobre dispositivos de rede não autorizados.

6	O sistema de controle deverá verificar a integridade de códigos móveis antes de permitir sua execução.
7	O sistema de controle deverá providenciar um sistema de trilha de auditoria centralmente gerenciável.
8	O sistema de controle deverá sincronizar os relógios internos com frequências configuráveis.
9	O sistema de controle deverá suportar mecanismos criptográficos para reconhecer mudanças na informação durante a comunicação.
10	O sistema de controle deverá gerenciar centralmente os mecanismos de proteção contra códigos maliciosos.
11	O sistema de controle deverá suportar backup automático com frequência configurável.
12	O sistema de controle deverá informar as atuais configurações de segurança nos dispositivos finais.

Fonte: Adaptado de Desruisseaux (2018)

APÊNDICE A - MANUAL DO USUÁRIO:

Fonte: Autoria própria, 2021

SUMÁRIO

Fonte: Autoria própria, 2021

1. INTRODUÇÃO

1.1.Proposta

Este trabalho aborda os principais tópicos relacionados à cibersegurança na Indústria 4.0, com foco nas vulnerabilidades encontradas nas redes industriais. Seu desenvolvimento visa o público inserido na parcela dos colaboradores envolvidos na Indústria 4.0, desde o nível estratégico, da alta administração, até o operacional, da mão de obra.

O objetivo deste projeto foi a criação de um informativo em uma plataforma web, com a finalidade de instruir e auxiliar aos colaboradores da Indústria 4.0 com as principais informações sobre temas relacionados à cibersegurança. É interessante saber que, até o momento, não existia nenhum portal informativo em língua portuguesa dedicado exclusivamente para a cibersegurança no contexto da Indústria 4.0, o que ressalta ainda mais a importância deste projeto.

1.2. Projeto

A fim de atender a esse segmento, a proposta deste trabalho trata-se da elaboração de um informativo sobre os principais tópicos de cibersegurança, bem como maneiras de se prevenir, em forma de um website. O portal contém um menu, que leva para páginas dedicadas a cada tópico, como conceitos gerais, notícias dos ciberataques mais recentes, e métodos de prevenir riscos à cibersegurança. Cada página aborda os conteúdos de forma simples e objetiva, com o auxílio de recursos, como imagens e gráficos.

1.3. Justificativa

Diversas empresas ao redor do mundo estão vulneráveis a ciberataques, como por exemplo a invasão a uma usina nuclear no Irã pelo vírus Stuxnet, em 2010. Além disso, é conhecido que uma das tecnologias mais utilizadas no mundo atual são os smartphones, e conforme indicado pela 31ª Pesquisa Anual do FGV (2020), no Brasil existem dois smartphones ativos por pessoa, em média. Também vale ressaltar que, conforme a pesquisa Digital 2020 feita pelo DataReportal (2020), o brasileiro passa, em média, 9 horas por dia conectado à Internet. Esses dados foram fundamentais para a escolha do tema deste projeto, no caso, o

Fonte: Autoria própria, 2021

desenvolvimento de um website informativo. Nesse contexto, foi muito importante a criação de um portal que ajude a informar sobre a cibersegurança na Indústria 4.0, aprofunde a compreensão das estruturas de segurança mais recentes, desenvolva o pensamento crítico em relação ao assunto, e induza todos os envolvidos a inserirem novas práticas em suas atividades. Também vale notar que ter uma fonte de informação que aborde os últimos incidentes de segurança ocorridos pelo mundo pode auxiliar as empresas a não cometerem os mesmos erros dos alvos desses ataques.

Fonte: Autoria própria, 2021

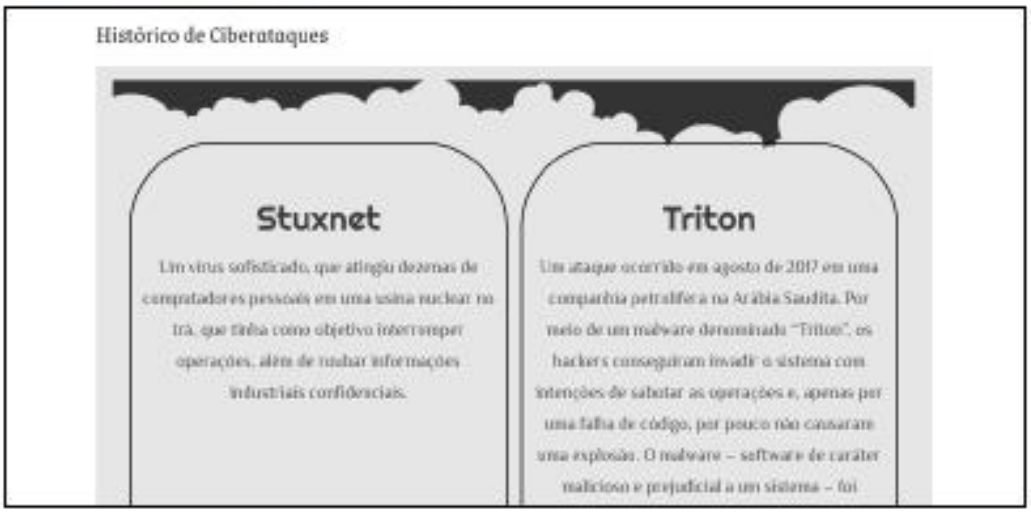
2. PÁGINA INICIAL

Na página inicial, é possível ver uma barra de menus na parte superior da tela. Ali, existem sibdivisões, ou *links*, que levam a cada uma das principais seções do site: "Home"; "Boas Práticas"; "Notícias"; "Conceitos Gerais" e "Quem Somos".

Se o usuário desejar rolar a página para baixo, encontrará uma área chamada "Ameaças na Indústria". Ali, estarão destacados alguns dos casos importantes de ciberataques, e logo abaixo há um botão clicável com um link que leva à página "Histórico de Ciberataques".

Fonte: Autoria própria, 2021

Na página "Histórico de Ciberataques", há uma tabela onde estará descrita detalhadamente uma lista de ciberataques industriais, para que o usuário possa se informar. Para ler mais, o usuário deverá rolar a página para baixo.



Fonte: Autoria própria, 2021

3. BOAS PRÁTICAS

A página "Boas Práticas" reúne uma tabela que informa algumas das mais importantes e recomendadas práticas para manutenção da segurança cibernética de uma indústria, envolvendo as áreas de dados, redes, operações e pessoas. Para a sua leitura, o usuário deverá apenas utilizar a barra de rolagem.

Fonte: Autoria própria, 2021

4. NOTÍCIAS

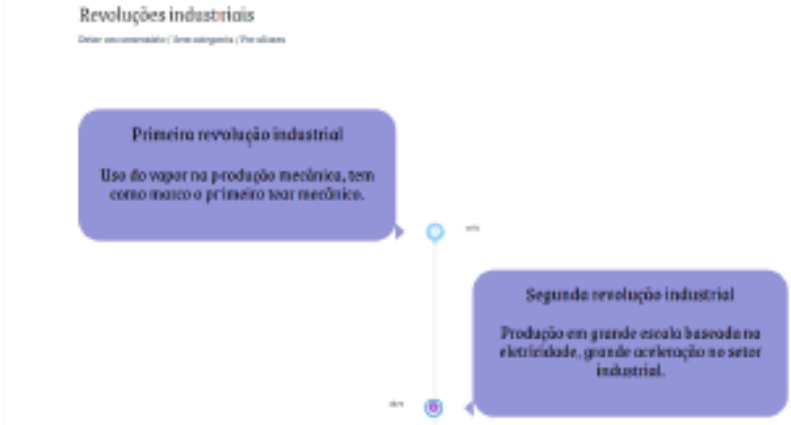
Na página "Notícias", o usuário poderá encontrar quadros com links para as principais notícias envolvendo cibersegurança e indústria 4.0, através do botão "Leia Mais", bem como as suas respectivas fontes, caso queira ler a notícia completa. A interação do usuário com essa página poderá ser feita por meio da barra de rolagem, e clicando nos botões.

Fonte: Autoria própria, 2021

5. CONCEITOS GERAIS

A aba de "Conceitos Gerais" possui um caráter teórico, pois aborda de maneira informativa os principais conceitos relacionados à cibersegurança e Indústria 4.0, como: "Revoluções Industriais"; "Redes"; "Cibersegurança"; "Padrões e Normas de Segurança"; e "Tipos de Malwares".

Nesta página, os conteúdos são dispostos em forma de tópicos, de maneira que o usuário poderá usar a barra de rolagem, e clicar no botão "saiba mais" ao lado do tópico desejado, caso queira obter informações mais detalhadas. Assim, ele será redirecionado a uma outra página, a qual explicará sobre o conceito escolhido de maneira mais detalhada.



Fonte: Autoria própria, 2021

6. PADRÕES DE SEGURANÇA

A aba de "Padrões de Segurança" trata a respeito de algumas das normas de cibersegurança conforme definidas por instituições padronizadoras nacionais internacionais, como a ISO e a IEC. Ao final da página, o usuário poderá encontrar um link que o levará a uma tabela em alguns dos padrões de cibersegurança definidos pela IEC 62443.

Fonte: Autoria própria, 2021

7. TIPOS DE MALWARE

E a aba "Tipos de Malware", por sua vez, contém um menu que contém alguns dos diversos tipos de malware existentes, como "Vírus", "Worm" e "Trojan". Cada item levará o usuário a uma página que exibe algumas das principais informações sobre o malware escolhido.

Fonte: Autoria própria, 2021

8. QUEM SOMOS

Por último, a página "Quem Somos" exibe os responsáveis pelo desenvolvimento do projeto, bem como um link sobre o qual o usuário poderá clicar, levando-o para a página pessoal de cada um na rede social LinkedIn.

Após a rolagem, no final da página será possível ver um endereço de e-mail para contato, caso o usuário deseje comunicar-se com os desenvolvedores do projeto.

Fonte: Autoria própria, 2021