UNIVERSIDADE PAULISTA

ICET - INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA

CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

PROJETO INTEGRADO MULTIDISCIPLINAR

PIM I

Projeto de estrutura de TI para trabalho home office em uma consultoria de informática.

Nome	R.A
Lívia Vilhena de Paula	G808EJ-6
Eduardo Nunes Bueno	G80CEG-7
Leonardo Faria Marques	N069BB-3
Bryan Patrick Bueno Monte	G8084A5
Breno Luiz Bueno Fonseca	G71CEA9
Leonardo Silva Favaro	G812271

SÃO JOSÉ DOS CAMPOS – SP

JUNHO/2023

Projeto de estrutura de TI para trabalho home office em uma consultoria de informática.

Projeto Integrado Multidisciplinar (PIM) desenvolvido como exigência parcial dos requisitos obrigatórios à aprovação semestral no Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas da UNIP (Universidade Paulista), orientado pelo corpo docente do curso.

São José dos Campos – SP

- **JUNHO/2023**

RESUMO

A finalidade do projeto era elaborar uma empresa no qual o foco seria gerir suporte no ramo da cibersegurança, com o objetivo de auxiliar contratantes a protegerem seus sistemas e dados contra ameaças virtuais. A empresa forneceria serviços de mentoria para indivíduos e organizações, visando aumentar a conscientização e fornecer conhecimentos especializados sobre melhores práticas de segurança cibernética.

Durante o projeto foi estudado os melhores sistemas e aplicações a fim de garantir melhor contato com o usuário e performance, também foi pautado as estatísticas de empregabilidade de profissionais no ramo de consultoria, foi definido uma estrutura organizacional para que as atividades sejam coordenadas de forma eficiente, foi estabelecido um canal de comunicação para que a empresa consiga um alcance de um determinado público alvo e foram escolhidas ações de sustentabilidade para garantir a preservação ambiental. Com o levantamento dessas pesquisas, espera-se que a empresa possa ter uma boa performance em todos os ramos viabilizando a segurança de informação, em geral, das empresas parceiras, realizando monitoramento de acessos, manutenção de sistemas de proteção, educação de usuário final e identificação de pontos vulneráveis do sistema para que não haja invasões e garantir a proteção dos sistemas e dados digitais contra ameaças cibernéticas.

Palavras Chaves: cibersegurança, proteção de sistemas, segurança de informações.

ABSTRACT

The purpose of the project was to develop a company focused on providing support in the cybersecurity field, with the aim of assisting clients in protecting their systems and data against virtual threats. The company would offer mentoring services to individuals and organizations, aiming to increase awareness and provide specialized knowledge on best practices in cybersecurity. During the project, the best systems and applications were studied to ensure better user engagement and performance. Employment statistics for professionals in the consulting field were also taken into account. An organizational structure was defined to coordinate activities efficiently, and a communication channel was established to reach a specific target audience. Sustainability actions were chosen to ensure environmental preservation.

With the findings from these research efforts, it is expected that the company will perform well in all areas, enabling the overall information security of partner companies. This includes monitoring access, maintaining protection systems, educating end-users, and identifying system vulnerabilities to prevent invasions and ensure the protection of digital systems and data against cyber threats.

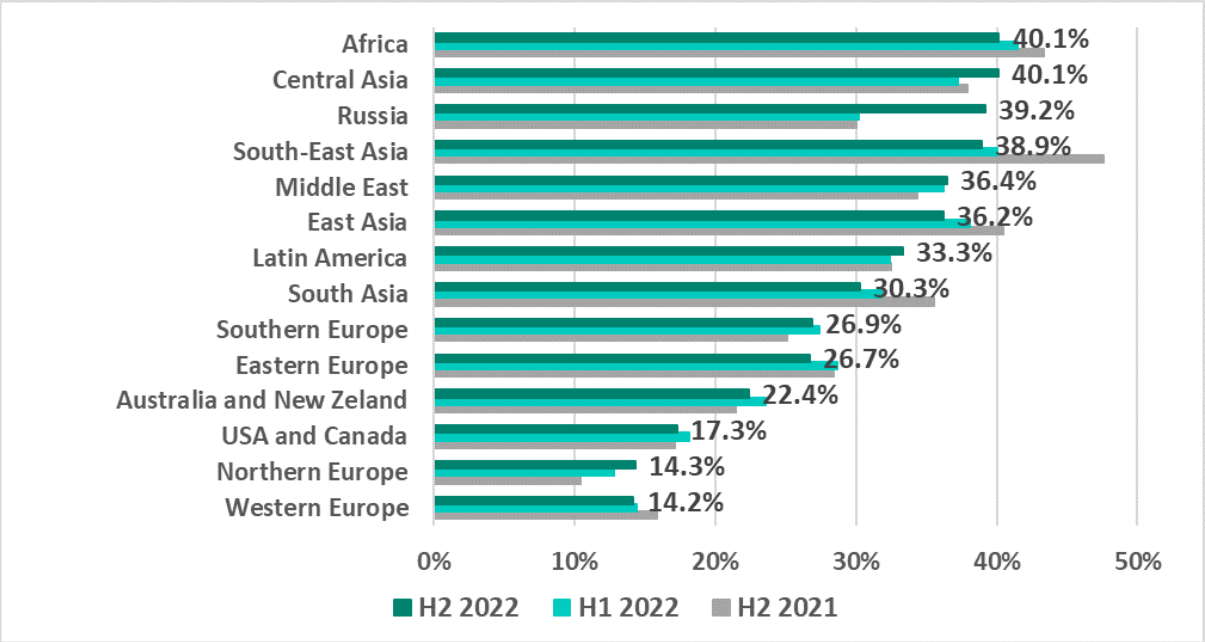
Keywords*: cybersecurity, protection, information security.*

SUMÁRIO

1. INTRODUÇÃO

Atualmente, o perigo de ataques cibernéticos tem crescido gradualmente ao longo dos anos. De acordo com a matéria jornalística (https://www.cisoadvisor.com.br/mais-de-40-dos-sistemas-industriais-sofreram-ataques-em-2022/#:~:text=Mais%20de%2040%25%20dos%20sistemas%20de%20controle%20industrial%20(ICS),partir%20da%20telemetria%20da%20Kaspersky) no ano passado, mais de 40% dos sistemas de controle industrial (ICS), sofreram algum tipo de ataque cibernético conforme os dados compiladores a partir da telemetria da *Kaspersky*.

Regiões do mundo classificadas por porcentagem de computadores ICS nos quais objetos maliciosos foram bloqueados:



Fonte: *Kaspersky*

Devido a este problema, criamos a empresa *SecurityTS* que foca na proteção de dados de empresas parceiras, contra essas invasões inesperadas. Nossa empresa oferece diversos tipos de serviços, dentre eles:

- Educação de usuário final;
- Segurança de aplicativos;
- Segurança de redes;
- Segurança *web*;
- Segurança de informação.

O objetivo da empresa e cuidar das seguranças de empresas parceiras ou de clientes parte, dar manutenção nos sistemas de proteção, monitorar acessos e identificar pontos vulneráveis do sistema, a fim de não ocorrer invasões inesperadas.

Nosso foco é dar consultoria a empresas que possuem dados e informações importantes para que não haja alteração ou roubo das demais. Por isso, além de fornecer esse serviço, é de extrema importância a educação dos usuários, a fim de não entrarem em regiões virtuais suspeitas, facilitando intrusões.

Para melhor entendimento dos sistemas da empresa, foram feitos tópicos, de ferramentas utilizadas para montagem dessa empresa, a seguir.

2. ORGANIZAÇÃO DE COMPUTADORES

A segurança da informação desempenha um papel fundamental na empresa, onde os recursos computacionais necessitam de monitoramento constante. Isso inclui equipamentos, servidores, arquivos digitais e banco de dados, a fim de garantir o funcionamento adequado de todos os componentes.

Os recursos computacionais abrangem tanto *hardware* quanto *software*, responsáveis pelo processamento, armazenamento e transmissão de dados, proporcionando maior mobilidade e praticidade. A empresa adotará a disponibilização de notebooks para os funcionários, que serão equipados com placa mãe, processador AMD *Ryzen* 5, 2 pentes de memória RAM de 8GB cada e um SSD de 480GB.

Além disso, depois de uma pesquisa feita no site da *Microsoft* (*https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-cloud-computing*) chega-se na conclusão que será adotada uma abordagem de computação em nuvem híbrida, nuvens públicas e privadas por meio de uma tecnologia que permite o compartilhamento de dados e aplicativos entre elas. Essa abordagem flexível permitirá que os funcionários utilizem recursos computacionais, armazenamento e rede por meio da internet, reduzindo os custos associados a servidores e máquinas locais. A escolha para essa finalidade será o "*Google Cloud Platform*" (*https://cloud.google.com/docs/overview?hl=pt-br*), que oferece segurança avançada e facilidade de gerenciamento.

3. PRINCÍPIOS DE SISTEMAS DE INFORMAÇÃO

Dado o foco da empresa na segurança e no relacionamento com o público, é essencial garantir um sistema fácil de usar e intuitivo para que os clientes possam fornecer feedback sobre a empresa e seus funcionários. Além disso, a comunicação entre todos os funcionários deve ser ágil e eficiente.

O sistema de feedback estará incorporado ao site da empresa, e os dados coletados serão armazenados para posterior análise em planilhas e gráficos. Essas informações serão apresentadas em reuniões usando a ferramenta "*Microsoft* Viva" (*https://learn.microsoft.com/pt-br/viva/microsoft-viva-overview*), que integra os dados da empresa com o público. As reuniões serão conduzidas através do "*Microsoft Teams*" (*https://learn.microsoft.com/pt-br/microsoftteams/teams-overview*) uma plataforma que possibilita compartilhamento de arquivos e realização de reuniões. Cada membro da equipe terá acesso a informações específicas do seu setor e cargo.

A empresa também oferecerá cursos gratuitos aos funcionários, a fim de capacitá-los sobre as funcionalidades disponíveis na plataforma. Essas medidas contribuirão para aumentar a eficiência da empresa, uma vez que os dados serão acessados de maneira simples, as reuniões podem ser realizadas em home office utilizando os computadores fornecidos pela empresa, resultando em uma redução nos custos operacionais. Além disso, teremos uma visão mais clara dos dados estatísticos e áreas que precisam ser aprimoradas dentro da empresa.

4. FUNDAMENTOS DE SISTEMAS OPERACIONAIS

No contexto da defesa cibernética, a escolha dos sistemas operacionais *Microsoft Windows* e *Linux* tem implicações importantes e ficará disponível para a escolha do contratante. A segurança cibernética é uma preocupação crítica nos dias de hoje, e é essencial escolher sistemas operacionais que possuam recursos robustos para proteger contra ameaças cibernéticas. O *Microsoft Windows* é amplamente utilizado em todo o mundo, o que o torna um alvo atraente para *hackers* e *malware*.

No entanto, o *Windows* também investiu significativamente em recursos de segurança ao longo dos anos, ele possui um conjunto abrangente de ferramentas de gerenciamento que podem ser usadas para monitorar e proteger os sistemas contra ameaças, além disso, a interface intuitiva do *Windows* facilita tanto para os usuários quanto para os profissionais de

TI implementarem medidas de segurança e adotarem práticas recomendadas. Portanto, ao escolher o *Windows*, a organização deve estar ciente dos desafios de segurança associados e implementar medidas de defesa cibernética adequadas para proteger seus sistemas.

Por outro lado, o *Linux* é conhecido por sua segurança e estabilidade. Sua baixa popularidade em comparação com o *Windows* faz com que seja menos visado por *hackers*, o que resulta em menos *malwares* desenvolvidos para esse sistema operacional. Isso não significa que o *Linux* seja imune a ataques, mas a probabilidade de ser alvo é menor. No entanto, é importante notar que o *Linux* requer um conhecimento mais técnico para sua utilização e manutenção, o que pode exigir recursos adicionais de treinamento e suporte especializado nesse sistema.

Ao considerar a defesa cibernética, é fundamental implementar medidas como *firewalls*, antivírus, atualizações regulares de segurança, políticas de acesso adequadas e monitoramento contínuo dos sistemas. Além disso, é importante estar ciente das vulnerabilidades específicas de cada sistema operacional escolhido e adotar práticas de segurança apropriadas para diminuir vulnerabilidades.

Em resumo, a escolha do *Microsoft Windows* e do *Linux* como sistemas operacionais levou em conta tanto a facilidade de uso e a compatibilidade quanto a segurança e a necessidade de personalização. Para garantir uma defesa cibernética eficaz, independentemente do sistema operacional escolhido, é essencial implementar medidas adequadas de segurança e estar ciente dos desafios e vulnerabilidades específicos associados a cada plataforma.

5. ESTATÍSTICA

Devido à Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em 2018, o campo de segurança da informação está enfrentando um alto crescimento nos últimos anos. A LGPD estabeleceu diretrizes e regulamentos rigorosos para o tratamento de dados pessoais, o que levou a uma maior conscientização sobre a importância da proteção dos dados tanto para indivíduos quanto para empresas.

Com a crescente popularização da internet e o aumento do fluxo de dados pessoais e empresariais relacionados à internet, tornou-se crucial, para as empresas, contar com uma consultoria especializada em segurança. Essa consultoria deve estar vinculada às empresas,

independentemente de sua área de atuação ou porte, a fim de garantir que todas as medidas necessárias sejam tomadas para proteger os dados pessoais de funcionários, clientes e parceiros comerciais.

Além disso, a consultoria de segurança pode ajudar as empresas a implementar políticas e procedimentos de segurança eficazes, realizar auditorias e avaliações de risco, fornecer treinamento em conscientização de segurança para os funcionários e ajudar na resposta a incidentes de segurança, como violações de dados.

É importante destacar que a conformidade com a LGPD não é apenas uma questão de evitar penalidades e multas, mas também de estabelecer confiança com os clientes e demonstrar compromisso com a proteção dos dados pessoais. Portanto, ter uma consultoria de segurança especializada é uma estratégia essencial para as empresas se adaptarem às exigências da LGPD e garantirem a proteção adequada dos dados.

De acordo com a empresa "*Next Move Strategy Consulting*" o mercado global de produtos e serviços de cibersegurança deve mais do que triplicar até 2030, saltando dos US$ 197 bilhões de faturamento registrados em 2021 para US$ 657 bilhões, de acordo com um novo relatório da *Next Move Strategy Consulting.*

Segundo a *Next Move*, três grandes impulsionadores irão aquecer a demanda por produtos e serviços de cibersegurança: o aumento dos ataques de *phishing* e *malware* às empresas; a expansão da adoção de dispositivos IoT (internet das coisas) e de uso da inteligência artificial, além de funcionários usando seus próprios dispositivos em ambientes remotos; e o número crescente de ataques cibernéticos em todo o mundo. A consultoria projeta que o mercado global de segurança cibernética deve atingir US$ 300 bilhões até 2027, com CAGR de pouco mais de 11% durante o período de previsão, que vai de 2019 a 2027, estudo recente da empresa havia projetado que o segmento chegaria a US$ 32,6 bilhões até 2028, com taxa composta de crescimento anual de 18,8%

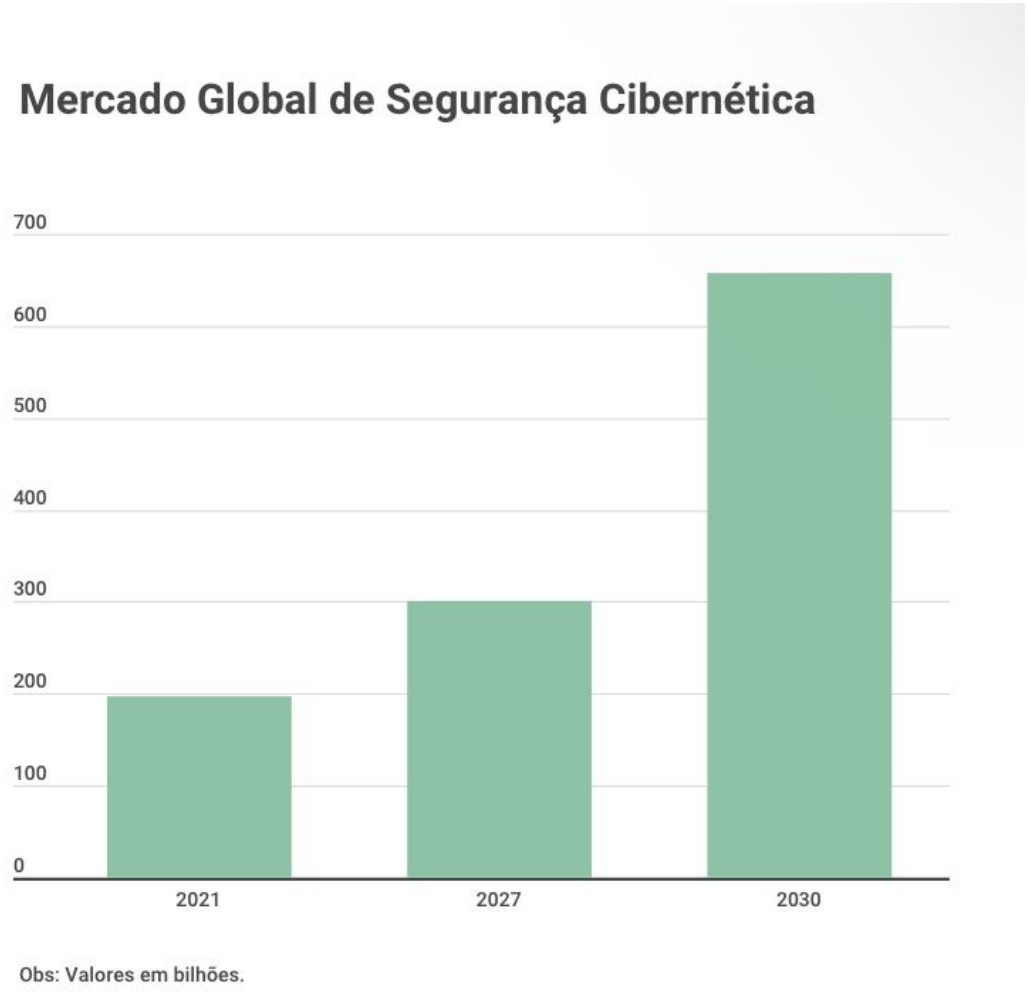


Figura 1: Mercado global de segurança cibernética. Fonte: Autoria própria.

Nos últimos anos, o interesse pela segurança de TI cresceu significativamente. Isso se deve em grande parte ao crescimento contínuo de ameaças cibernéticas complexas e persistentes, ao uso de tecnologias como dispositivos móveis, Internet das Coisas e nuvem, e à crescente necessidade de conformidade regulatória e proteção de dados. Em conjunto com a crescente demanda, os salários na área de segurança de TI também aumentaram. De acordo com *Job Glassdoor*, o salário médio anual para engenheiros de segurança de TI nos Estados Unidos é de cerca de US$ 120.000, enquanto um analista de segurança ganha em média cerca de US$ 85.000 por ano. Em comparação com outros setores de TI, os salários no setor de segurança de TI geralmente são mais altos.

6. LÓGICA

Com o aumento do fluxo de dados pessoais e empresariais na internet, é de suma importância garantir a proteção dessas informações. Uma consultoria especializada em segurança pode ajudar as empresas a identificar os dados críticos que precisam ser protegidos, implementar medidas de segurança adequadas e garantir a conformidade com regulamentações de privacidade, como o GDPR (Regulamento Geral de Proteção de Dados). Sendo assim, é imprescindível que profissionais que trabalhem com segurança de dados não tenham um salário referente a sua importância na empresa.

O mercado apresente grande crescimento pois está cada dia mais comum empresas e pessoas serem vítimas de ataques virtuais a fim de terem suas informações violadas. Os profissionais de segurança são os responsáveis por evitar que tais atos sejam realizados,

Sendo assim, as empresas enfrentam constantes problemas para garantir o fácil e eficaz entendimento das pessoas beneficiadas referente aos recursos e serviços que oferecem. Para solucionar tais problemas, é essencial contar com algoritmos e fluxogramas bem definidos, capazes de representar as etapas necessárias para alcançar as soluções desejadas. Os fluxogramas fornecem representações visuais de etapas do processo, essas representações são extremamente úteis para entender a sequência de ações necessárias, visualizar pontos críticos e identificar possíveis melhorias no dia de trabalho, sendo assim, foi desenvolvido um fluxograma da rotina de trabalho e um para processos de resolução de eventuais problemas representado respectivamente abaixo:

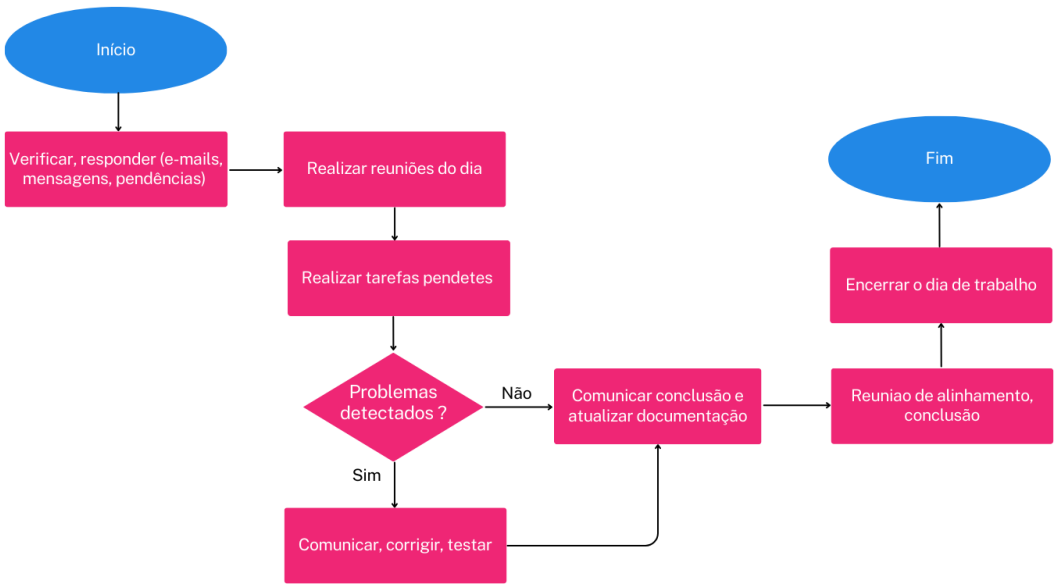


Figura 1: Fluxograma representando a rotina de trabalho. Fonte: Autoria própria.

Neste fluxograma acima é possível observar as principais partes e ações que um funcionário deve tomar durante seu período de trabalho, tanto na empresa como em *Home-Office*. Passos como a verificação de e-mails e reuniões diárias são de suma importância para que todos os funcionários estejam cientes de objetivos, metas e prazos estipulados para realização de tarefas. Com base em pesquisas realizadas foi possível observar que empresas que possem rotinas de trabalho definidas apresentam um melhor desempenho na realização de tarefas cotidianas e ajudam na introdução de novos funcionários ao ritmo da empresa.

Abaixo temos um exemplo de fluxograma baseado em passos que os funcionários devem seguir quando algum problema for detectado em alguma empresa contratante ou internamente a fim de sempre seguir o mesmo padrão de atendimento aos clientes e de resolução de problemas. Quando algum usuário presenciar um erro ele irá realizar a abertura de um *ticket*, para entrar em contato com nosso suporte, caso o erro já seja de conhecimento da equipe será respondido que já estamos cientes dos problemas reportados, e passaremos uma data estipulada para o usuário de quando a resolução do problema estará concluída, junto com uma mensagem de agradecimento por ter nos comunicados.

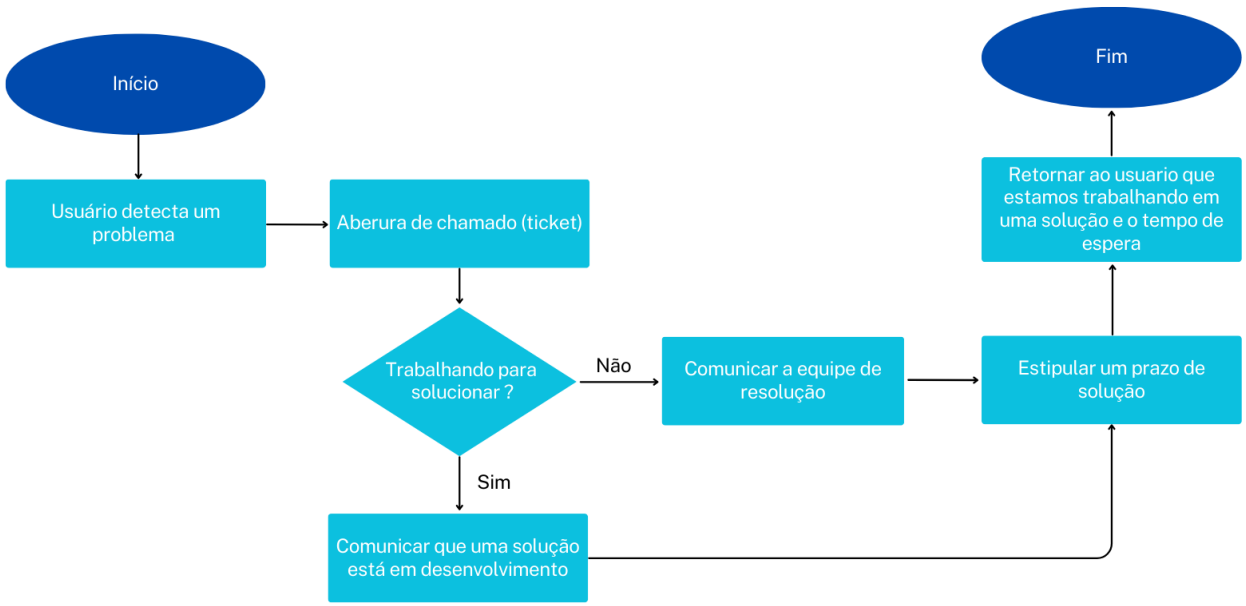


Figura 2: Fluxograma representando resoluções de problemas. Fonte: Autoria própria.

7. DESENVOLVIMENTO SUSTENTÁVEL

O desenvolvimento sustentável na tecnologia é fundamental para garantir a preservação do meio ambiente e a continuidade da vida do planeta. Isso inclui o uso de fonte de energia renováveis, a redução do consumo de recursos naturais, a produção de equipamentos eletrônicos com materiais recicláveis e a implementação de políticas de descarte responsável de resíduos eletrônicos. Além disso, a tecnologia pode ser utilizada para desenvolver soluções que contribuam para a sustentabilidade em diversas áreas, como transporte, agricultura e energia.

Algumas estratégias para reduzir o consumo de energia elétrica dos equipamentos de informática são:

1. Desligar os equipamentos quando não estiverem em uso. (monitores, computadores, impressoras, celulares e tabletes)

2. Ativar o modo de economia de energia nos monitores e computadores. (Além da preocupação com o meio ambiente, poupar energia elétrica também proporciona economia financeira. Além disso esse sistema desliga quando o computador não está sendo utilizado por muito tempo.)

3. Utilizar dispositivos de alimentação de eficiência energética

4. Desativar dispositivos de hardwares desnecessários. (Assim como o CD/DVD que podem ser substituídas por dispositivos de armazenamento USB, placas de rede sem fio e placas de som)

5. Configurar os recursos de economia de energia do sistema operacional. (Esses recursos estão incluindo a memória principal, assim como o próprio processado (CPU), entre os arquivos e os dispositivos de I/O.)

Essas medidas podem ajudar a reduzir significativamente o consumo de energia elétrica dos equipamentos de informática. Usando essas estratégias o consumo de energia irá ser bem menor do que sem essas estratégias.

Equipamentos eletrônicos obsoletos ou com defeito pode ser descartado em ponto de coletas específicos, como posto de coletas mantidos por empresa de reciclagem ou por programas de reciclagem de *E-WASTE* (lixo eletrônico), Resíduos de equipamentos elétricos

e eletrônicos (REEE) ou e-lixo são termos utilizados para estar se referindo a todos esses equipamentos elétricos e eletrônicos. Também é importante descartar esses equipamentos corretamente porque eles contêm materiais tóxicos, incluindo mercúrio, chumbo e outros metais pesados, que podem contaminar o solo e a água se não forem tratados adequadamente. Ademais, muitos desses componentes eletrônicos que podem ser recuperados e reutilizados em novos produtos.

8. COMUNICAÇÃO APLICADA

De acordo com uma matéria jornalística feita pela CNN Brasil (https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94), uma empresa de soluções de segurança cibernética (*Fortinet*) fez um levantamento de dados de ataques cibernéticos no Brasil, sendo eles 94% superior na comparação com o primeiro semestre do ano passado, quando foram 16,2 bilhões de registros. O objetivo da nossa empresa é diminuir esses números de ataques, para que o ambiente virtual se torne algo mais confiável e seguro. Queremos acessar, de preferência, empresas que possuem uma grande quantidade de dados e informações reservadas e que zelam pela privacidade deles.

Para que a nossa empresa alcance exatamente esse público, é preciso de uma equipe de *marketing* e publicidade para criar imagens de divulgação do nosso serviço, com escrita de forma fática e apelativa, de modo que atraia o interesse das corporações necessitadas em tal benefício. As imagens criadas por essa equipe serão transmitidas nas redes sociais virtuais e para impulsionar ainda mais o conhecimento da nossa empresa, é de extrema importância a ida em eventos sobre o assunto, para assim criar vínculos com empresas já atuantes neste mesmo mercado e com empresas renomadas que precisam do nosso serviço.

Além da divulgação, no interior da empresa usaremos diversas formas de comunicação, sendo elas com respeito e de forma estratégica. É necessário que haja reuniões para discutir formas de melhora da empresa, o nível dela atualmente, qualidades e reclamações que devem ser atendidas, e muito mais. Para comprovação futura das discussões e decisões tomadas em toda reunião, deve haver um ATA em cada um desses encontros, que contém a data e o local da reunião, o nome dos presentes nela, a descrição do assunto a ser tratado, o relato dos assuntos com o nome de quem o manifestou, registro da conclusão e soluções, e por fim, deve ser aprovada e assinada pelos presentes na reunião. Para a facilidade das comunicações entre setores da empresa, serão disponibilizados e-mails corporativos que

darão acesso também a plataforma do *Teams*, da *Microsoft*, para o trabalho *home-office*. A cada serviço novo gerado pela empresa, deve-se fazer uma ordem de serviço, a qual deve ser numerada, datada e assinada pela autoridade do setor, deve ter a escrita de forma simples e direta, esse documento será importante para organização da demanda no fim do mês, podendo analisar se a empresa está crescendo, ou não, comercialmente.

Por fim e de extrema importância, o *press-release* para divulgação de texto pronto da imprensa:

8.1 Press-release

22 de maio - São josé dos Campos-SP

Empresa capaz de oferecer proteção contra ataques cibernéticos.

A *SecurityTS* promete proteger os dados da sua empresa contra invasões cibernéticas de forma simples e eficaz.

SecurityTS é a nova empresa no mercado da cibersegurança que tem a inauguração prevista para o começo do próximo mês. Mesmo recente, a empresa já garantiu a eficácia na proteção de dados e informações das empresas contratantes. Ela se encarregará do monitoramento dos acessos da sua empresa, manutenção no sistema de proteção e identificação de pontos vulneráveis do sistema a fim de não ocorrer invasões inesperadas. E para novidade de diversas empresas, a *SecurityTS* irá oferecer educação do usuário final, para ensinar as pessoas a identificar o perigo no mundo virtual e não entrar em sites suspeitos para não haver problemas futuros e roubo de dados importantes, afinal, como a própria *SecurityTS* diz " O futuro é o mundo virtual. "

Informações:

Comitê organizador: +55(12) 2011-2022.

www.securityts.com.br | securityts@gmail.com.br

9. DESENVOLVIMENTO DO PROJETO

Este projeto tem como objetivo principal integrar os conhecimentos das disciplinas de Organização de Computadores, Princípios de Sistemas de Informação, Fundamentos de Sistemas Operacionais, Estatística, Lógica e Desenvolvimento Sustentável. A proposta visa utilizar tecnologias e práticas que promovam a segurança de empresas e pessoas, garantindo a eficiência e a responsabilidade na tomada de decisões seguindo a lei.

A disciplina de Organização de Computadores fornecerá os conhecimentos necessários para o entendimento da estrutura física dos computadores e dos dispositivos de armazenamento. Isso permitirá a escolha adequada de hardware, levando em consideração critérios de eficiência energética, durabilidade e fácil manuseio.

Os princípios de Sistemas de Informação serão aplicados no projeto para o desenvolvimento de sistemas que atendam às necessidades da organização, sejam flexíveis, escaláveis e seguros. Será dada ênfase na integração de diferentes módulos e na garantia da disponibilidade e confidencialidade das informações.

A disciplina de Fundamentos de Sistemas Operacionais contribuirá para a seleção e configuração adequada de sistemas operacionais que sejam eficientes e seguros, otimizando o uso dos recursos computacionais e garantindo a proteção das informações organizacionais.

A disciplina de Estatística desempenhará um papel fundamental na análise de dados e na obtenção de informações relevantes para a tomada de decisões sustentáveis. Serão utilizadas técnicas estatísticas para analisar o consumo de recursos, avaliar indicadores de desempenho ambiental e social, e identificar oportunidades de melhorias com base em dados quantitativos e qualitativos.

A disciplina de Lógica fornecerá a base para o desenvolvimento de sistemas de informação com arquitetura lógica consistente e coerente. A aplicação de princípios lógicos garantirá a correta estruturação dos dados e a validade das operações realizadas nos sistemas, evitando erros e inconsistências.

Com base nos princípios do desenvolvimento sustentável, serão adotadas medidas para minimizar o impacto ambiental da infraestrutura de TI, como o uso de fontes de energia renovável, a virtualização de servidores para reduzir o consumo de energia e a implementação de políticas de descarte adequado de equipamentos eletrônicos.

A comunicação aplicada desempenha um papel fundamental na disseminação de mensagens significativas e eficazes para o público-alvo. No projeto foi elaborado formas para garantir que o projeto seja alcançado por todas as pessoas de forma significativa e positiva.

10. CONCLUSÃO

A segurança cibernética é um desafio crescente no mundo empresarial, pois a constante evolução da tecnologia traz consigo ameaças cada vez mais sofisticadas. No contexto do projeto em questão, tivemos como objetivo abordar esse problema e fornecer soluções através de uma empresa a fim de auxiliar na proteção de possíveis ataques e a garantia do suporte necessário.

Ao longo da pesquisa e análises realizadas, identificamos as principais áreas que são alvos de ataque, como a falta de conscientização dos funcionários sobre segurança cibernética, a ausência de medidas adequadas de proteção de dados e a falta de uma estratégia abrangente de gerenciamento de riscos. Com base nesses pontos, elaboramos uma série de soluções estratégicas para sanar riscos e fortalecer a postura de segurança da empresa contratante.

Em primeiro lugar, destacamos a importância da conscientização e treinamento dos colaboradores em relação às melhores práticas de segurança cibernética, ao capacitar a equipe para reconhecer e lidar com possíveis ameaças, reduzimos a probabilidade de ataques decorrentes de ações inadvertidas ou de negligência.

Além disso, sugerimos a implementação de um conjunto abrangente de medidas técnicas de proteção de dados, incluindo firewalls, sistemas de detecção de intrusões e criptografia, tais medidas ajudarão a fortalecer as defesas da empresa contra invasões e garantir a integridade e confidencialidade das informações sensíveis.

Outra solução proposta foi o estabelecimento de uma estratégia de gerenciamento de riscos, que envolve a identificação, avaliação e mitigação dos riscos de segurança cibernética. Isso permitirá que a empresa esteja preparada para lidar com possíveis ameaças, minimizando danos e garantindo a continuidade das operações.

Ao adotar essas soluções, a empresa investirá em sua própria proteção e no fortalecimento de sua posição no mercado. A segurança cibernética é um diferencial competitivo nos dias de hoje, e as empresas que priorizam a proteção de seus ativos digitais ganham a confiança dos clientes e parceiros comerciais.

No entanto, é importante ressaltar que a segurança cibernética é um campo em constante evolução, com novas ameaças e vulnerabilidades surgindo regularmente. Portanto, os estudos e a busca contínua por atualizações e soluções inovadoras são fundamentais para garantir a eficácia e a adaptabilidade das medidas de segurança implementadas.

Ao concluir este projeto, a empresa estará mais bem preparada para enfrentar os desafios da segurança cibernética e, consequentemente, poderá diversificar suas atividades e se consolidar no segmento de mercado em que atua. A proteção dos dados e a confiança dos clientes serão fortalecidas, abrindo portas para oportunidades de crescimento e sucesso sustentável.

Portanto, o constante incentivo do prosseguimento dos estudos nessa área é crucial para o mundo moderno. A segurança cibernética é uma responsabilidade contínua, e investir nesse campo é um passo essencial para garantir a longevidade e credibilidade no ramo empresarial

11. REFERÊNCIAS

Mais de 40% dos sistemas ICS sofreram ciberataques em 2022.Ciso *Advisor,* 2023. *https://www.cisoadvisor.com.br/mais-de-40-dos-sistemas-industriais-sofreram-ataques-em-2022/#:~:text=Mais%20de%2040%25%20dos%20sistemas%20de%20controle%20industrial%20(ICS),partir%20da%20telemetria%20da%20Kaspersky* .2023. Página 5.

O que é computação em nuvem? :Um guia para iniciantes. *Azure Microsoft*. *https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-cloud-computing#faq* .2023. Página 6.

Visão geral do *Google Cloud*. *Google Cloud*. *https://cloud.google.com/docs/overview?hl=pt-br* . 2023. Página 6.

Visão geral *Microsoft* Viva. *Microsoft learn*, 05/04/2023. *https://learn.microsoft.com/pt-br/viva/microsoft-viva-overview* . 2023. Página 7.

Bem-vindo ao *Microsoft Teams*. *Microsoft learn*, 26/03/2023. *https://learn.microsoft.com/pt-br/microsoftteams/teams-overview .2023*. Página 7.

Next Move Strategy Consulting. https://www.nextmsc.com/ . 2023. Página 9.

OLIVEIRA, Ingrid. Levantamento mostra que ataques cibernéticos no Brasil cresceram 94%: País é o 2º na América Latina com mais ataques cibernéticos em 2022. CNN Brasil, 19/08/2022*. https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/* . 2023. Página 14.