UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO
PRÓ-REITORIA DE GRADUAÇÃO
DEPARTAMENTO DE CIÊNCIAS EXATAS E TECNOLOGIA DA INFORMAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Noilton Wilson da Silva

Segurança da Informação em Empresas de Pequeno e Médio Porte em Assú-Rn:

Manutenção de Equipamentos, Vulnerabilidades Físicas, Lógicas e Riscos De Engenharia Social

ANGICOS
2024

Noilton Wilson da Silva

Segurança da Informação em Empresas de Pequeno e Médio Porte em Assú-Rn:

Manutenção de Equipamentos, Vulnerabilidades Físicas, Lógicas e Riscos De Engenharia Social

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Francisco de Assis Pereira Vasconcelos de Arruda.

ANGICOS

2024

S586s

Silva, Noilton Wilson.
Segurança da Informação em Empresas de Pequeno E Médio Porte em Assú-Rn: Manutenção de Equipamentos, Vulnerabilidades Físicas, Lógicas e Riscos De Engenharia Social / Noilton Wilson Silva. - 2024. 57 f.: il.

Orientadora: Francisco de Assis Pereira Vasconcelos de Arruda.
Monografia (graduação) - Universidade Federal Rural do Semi-árido, Curso de Sistemas de Informação, 2024.

1. Segurança da Informação. 2. Suporte técnico. 3. Empresas. I. Pereira Vasconcelos de Arruda, Francisco de Assis, orient. II. Título.

Ficha catalográfica elaborada por sistema gerador autômato conformidade com AACR2 e os dados fornecidos em pelo) autor(a).
Biblioteca Campus Angicos
Bibliotecário: Helder Romero Maia Duarte
CRB: 15/673

Noilton Wilson da Silva

Segurança da Informação em Empresas de Pequeno e Médio Porte em Assú-Rn:
Manutenção de Equipamentos, Vulnerabilidades Físicas, Lógicas e Riscos De Engenharia Social

Monografia apresentada à Universidade Federal Rural do Semi-Árido como requisito para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Francisco de Assis Pereira Vasconcelos de Arruda.

Defendida em: 18/10/2024

BANCA EXAMINADORA

_____
Prof. Dr. Francisco de Assis Pereira Vasconcelos de Arruda (UFERSA)
Orientador-Presidente

_____
Profa. Dra. Joêmia Leilane Gomes de Medeiros (UFERSA)
Membro Examinador

_____
Profa. Dr. Paulo Henrique Lopes Silva (UFERSA)
Membro Examinador

AGRADECIMENTOS

Agradeço, Dr. Francisco de Assis P. V. de Arruda, pela orientação e apoio. A minha mãe por sempre estar me apoiando, incentivando a continuar, me dando exemplos.

Dedico este trabalho a meu pai, Francisco Ilson (*in memoriam*), que tanto queria me ver formado e sempre mostrou a importância de se dedicar em tudo que almeja, colocando sempre em foco os estudos.

Aos amigos: Carlos Junior, Rafaela Simone, Aline Araujo, Paulo Freire, Jailma Alves, que torcem por minhas conquistas e sempre estão ao meu lado.

RESUMO

Este trabalho explora a relevância da segurança da informação em empresas de pequeno e médio porte na cidade de Assú-RN, destacando as ameaças físicas e virtuais que essas empresas enfrentam. Quanto às ameaças lógicas em relação à segurança da informação, incluem-se invasões, roubo de dados, infecção por vírus e malwares, além de ataques cibernéticos. Na cidade, aumentaram as reclamações sobre a carência de profissionais qualificados para prestar suporte e consultoria adequadas para segurança das empresas. O objetivo deste trabalho foi o de criar uma cartilha para conscientizar as pequenas e médias empresas de Assu-RN sobre a importância da segurança em TI, que muitas vezes enfrentam limitações de recursos. A cartilha destaca a importância da segurança dos dados e dos equipamentos, além de mostrar como uma equipe de suporte de TI pode ajudar a manter a integridade dos sistemas, por meio da análise dos riscos físicos e lógicos nas empresas de pequeno e médio porte, com o intuito de garantir a eficiência e a eficácia de seu suporte técnico. Para ter uma conclusão das necessidades perante a carência do suporte na cidade foi feito um levantamento por meio de questionário nos pontos críticos no suporte técnico, e assim ajudando a fortalecer as empresas e garantir a continuidade dos negócios e proteger a reputação das empresas. O principal resultado deste trabalho, além da pesquisa realizada, foi a confecção de uma apostila e material de divulgação de boas práticas de segurança da informação.

Palavras-chave: segurança da informação; suporte técnico; empresas.

ABSTRACT

This work explores the relevance of information security for small and medium-sized businesses in the city of Assú-RN, highlighting the physical and virtual threats these businesses face. Regarding logical threats to information security, these include intrusions, data theft, infections by viruses and malware, as well as cyberattacks. Complaints have increased in the city about the lack of qualified professionals to provide adequate support and consulting for company security. The objective of this work was to create a guide to raise awareness among small and medium-sized businesses in Assú-RN about the importance of IT security, as they often face resource limitations. The guide emphasizes the importance of data and equipment security, and demonstrates how an IT support team can help maintain system integrity by analyzing the physical and logical risks faced by small and medium-sized businesses, aiming to ensure the efficiency and effectiveness of their technical support. To draw conclusions on the needs concerning the lack of support in the city, a survey was conducted through a questionnaire addressing critical points in technical support, thereby helping to strengthen businesses, ensure business continuity, and protect companies' reputations. The main result of this work, in addition to the research conducted, was the development of a manual and promotional materials on information security best practices. The main result of this paper, in addition to the research conducted, was the creation of a manual and dissemination material on best practices for information security.

Keywords: information security; technical support; enterprises.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE ANEXOS

LISTA DE SIGLAS E ABREVIATURAS

GDPR	General Data Protection Regulation
ISMS	Information Security Management System
ANPD	Autoridade Nacional de Proteção de Dados
LGPD	Lei Geral de Proteção de Dados
SGSI	Sistema de Gestão de Segurança da Informação
SI	Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

O cenário empresarial está em constante evolução. As pequenas e médias empresas, hoje dependem significativamente de informações e de toda uma infraestrutura técnica de tecnologia da informação para gerenciar as operações das empresas.

A tecnologia da informação é fundamental para o suporte, nas atividades gerenciais, na eficácia operacional das empresas. O fornecimento e a proteção adequada das informações tornam-se essenciais na gestão organizacional. De acordo com Mascarenhas Neto (2019), os avanços tecnológicos transformaram a maneira como as organizações geram, processam e compartilham informações. A convergência tecnológica desafia os paradigmas da segurança da informação, para garantir sigilo, integridade e disponibilidade dos dados. Assim, foi difundido um novo modelo de gestão que enfatiza a proteção dos dados gerados e resguardados pela empresa, tanto quanto à proteção contra uso indevido e possíveis violações ou manipulação por agentes externos. Nesse sentido, a segurança da informação protege as informações de diferentes tipos de ameaças para garantir a continuidade dos negócios, minimizar perdas e aumentar o retorno sobre o investimento, investimentos e oportunidades de negócios.

A relevância do tema mostra-se no nível de informação proporcionado pelo avanço tecnológico e na necessidade de controlá-la, pois muitas vezes as organizações têm dificuldade em estabelecer modelos adequados de sistemas e níveis de controle de segurança.

Independentemente do tamanho ou estrutura da organização, GAT INFOSEC (2022) afirma que os alvos de ataques podem ser ativos de informação pertencentes a qualquer empresa ou pessoa, independentemente do ambiente. Esses ativos fazem parte de uma extensa cadeia, e as empresas podem sofrer perdas diretas e indiretas. Isso inclui desde a interrupção de ambientes produtivos ou operações críticas até violações de dados sensíveis, impactos na reputação da marca, multas e prejuízos nas relações com o mercado.

É fundamental que as empresas estabeleçam políticas de segurança bem definidas, aplicando-as consistentemente em toda a organização. Isso envolve a implementação de diversas medidas de segurança, como o uso de senhas robustas, a criptografia de dados sensíveis, a configuração de firewalls, a adoção de software antivírus e a realização regular de backups.

1.1. Justificativa

A manutenção de sistemas e equipamentos (terminais, redes e servidores) é crucial para garantir a continuidade dos negócios, minimizar perdas e aumentar o retorno do investimento. Com o avanço tecnológico, a quantidade de informações que as empresas precisam gerenciar aumentou significativamente, tornando mais desafiador estabelecer modelos adequados de sistemas de segurança e níveis de controle. As empresas, independentemente do porte, precisam estar atentas às ameaças e tomar medidas proativas para proteger seus dados.

Do Vale (2022), afirmar que as pequenas e médias empresas geralmente com a falsa sensação de segurança no ambiente virtual e a crença de que não são alvos para criminosos virtuais, faz com que empresários não busquem conhecer seus riscos, consequentemente, não realizando investimentos na área de segurança cibernética. Todo mundo está envolvido com a segurança da informação, muitas vezes por meio de contramedidas de segurança. Essas contramedidas são, por vezes, impostas por normas regulatórias e às vezes implementadas por meio de normas internas. Além disso, tem-se:

> O conhecimento sobre segurança da informação é importante para todos os funcionários. Não faz diferença se você trabalha em uma organização com ou sem fins lucrativos, pois todas as organizações enfrentam riscos semelhantes. Os funcionários precisam saber por que devem cumprir diariamente as regras de segurança. Os gerentes imediatos precisam ter esse entendimento, uma vez que são responsáveis pela segurança da informação no seu departamento. Esse conhecimento básico também é importante para todos os profissionais, incluindo os trabalhadores autônomos, que não possuem funcionários, visto que são responsáveis por proteger suas próprias informações (Hintzbergen, 2018, p. 24).

Assim, as empresas devem ter políticas de segurança bem definidas e aplicá-las de forma consistente em toda a organização. Isso inclui a implementação de medidas de segurança, como uso de senhas fortes, criptografia de dados confidenciais, firewalls, uso de software antivírus, backup*s* regulares e treinamento dos funcionários. A segurança da informação é uma questão relevante e crítica para o sucesso de qualquer empresa no atual ambiente de negócios.

MORAES (2004), o suporte de TI é fundamental na gestão estratégica da informação nas empresas que são: garantir o bom e constante funcionamento do sistema, implementar tecnologias acessíveis financeiramente, treinamento apropriados aos funcionários e no envolvimento do dirigente no processo de implementação. Sendo, importante no âmbito das pequenas empresas, viabilizando tecnologia da informação às suas necessidades (MORAES, 2004).

Assim sendo, propõe-se neste trabalho o desenvolvimento de uma cartilha para conscientizar as empresas de pequeno e médio porte da cidade de Assu-RN sobre a importância da proteção dos dados e o papel fundamental do suporte de TI na manutenção da integridade dos equipamentos e sistemas. A cartilha tem o objetivo principal apresentar políticas e procedimentos de segurança, orientar sobre mecanismos de proteção e ajudar na promoção do treinamento e conscientização da segurança da informação nessas empresas.

1.2. Objetivos

As subseções a seguir contém os objetivos gerais e específicos deste trabalho.

1.2.1. Objetivo Geral

Elaborar uma cartilha para conscientizar as empresas de pequeno e médio porte da cidade de Assu-RN, sobre a importância de investir em medidas básicas de segurança de TI, destacando que, mesmo com recursos limitados, a cartilha pode ser uma ferramenta essencial para evitar problemas relacionados a equipamentos e sistemas, além de garantir a proteção dos dados, ressaltando o papel da equipe de suporte de TI na manutenção da integridade deles.

1.2.2. Objetivos Específicos

- Identificar as principais ameaças de segurança da informação enfrentadas por empresas de pequeno e médio porte em Assu-RN.
- Desenvolver uma cartilha de segurança da informação, considerando as limitações financeiras e de recursos das empresas de pequeno e médio porte em Assu-RN, que deve incluir procedimentos de segurança, mecanismos de proteção, formas de treinamento e conscientização.
- Divulgar a cartilha de segurança da informação por meio de canais relevantes.
- Monitorar o engajamento e a aceitação da cartilha de segurança da informação por meio de métricas a serem definidas.
- Avaliar o impacto da cartilha de segurança da informação por meio de métricas como redução no número de ataques cibernéticos.
- Analisar os resultados obtidos e propor ajustes e melhorias à cartilha.

1.3. Organização do Documento

Este documento é composto por cinco capítulos, organizados da seguinte forma: no Capítulo 1, foram apresentados a introdução, justificativa e objetivos. O Capítulo 2 aborda a fundamentação teórica, incluindo tópicos como a gestão de segurança da informação e a ISO 27001. No Capítulo 3, a metodologia é detalhada, incluindo os materiais, métodos, construção da cartilha, e boas práticas para manter dados e equipamentos seguros. O Capítulo 4 foca na confecção da cartilha, abordando seu conteúdo e design. Por fim, o Capítulo 5 apresenta os resultados e considerações finais, detalhando resultados quantitativos relacionados ao grau de instrução e conhecimento em informática e à segurança. O documento inclui uma seção sobre trabalhos futuros, referências e anexos.

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada a fundamentação teórica do trabalho proposto e está dividido em três seções: 2.1 Gestão de Segurança da Informação e a ISO 27001; 2.2 Impacto da engenharia social na segurança da informação; 2.3 A segurança da informação e a conformidade com a LGPD.

2.1. Gestão de Segurança da Informação e a ISO 27001

A norma ISO 27001 refere-se a uma série de diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação em uma empresa. RAMOS, Elias et al. (2021) afirma que com a norma é possível implementar camadas de proteção contra incidentes que afetam a disponibilidade, confidencialidade ou integridade das informações da organização.

De acordo com Hintzbergen et al. (2018), as normas da ISO 27001 são aplicáveis em todas as organizações, independente de tipo, tamanho ou natureza. A implementação da norma traz uma série de benefícios que avalia os riscos, permitindo a identificação de vulnerabilidades que afetam os ativos da empresa e a elaboração de um plano de ações para prevenir tais problemas. As organizações que se adequam às normas, aumentam a confiança e a satisfação dos clientes e parceiros (RAMOS, Elias et al., 2021).

No contexto do Sistema de Gerenciamento da Segurança da Informação (SGSI), as partes interessadas podem incluir funcionários, clientes, fornecedores, governo, investidores, parceiros e outros envolvidos. Compreender esses aspectos é fundamental para definir os limites de um sistema de gerenciamento de segurança da informação, conforme estabelecido na norma ISO 27001 (2013). RAMOS, Elias (2021), define que as organizações devem identificar esses limites e avaliar a aplicabilidade do SGSI para estabelecer o escopo de sua implementação. Para definir esse escopo, a norma sugere que a organização leve em consideração tanto as condições internas quanto as externas, bem como os requisitos, interfaces e dependências entre as atividades da própria organização e de outras entidades, quando aplicável.

Em resumo, a ISO 27001 recomenda que o Sistema de Administração da Segurança da informação seja baseado na análise do ambiente micro e macro; identificação de todas as partes envolvidas no SGSI e seus requisitos; detecção de atividades realizadas pela organização e realizadas por terceiros; e definir o escopo ou seja, o escopo do SGSI (em inglês, *Information Security Management System* - ISMS). No entanto, para que o sistema de gestão da segurança

da informação seja bem-sucedido, a ISO 27001 (2013) propõe que a organização deva estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação. Isso só é possível com a contribuição de todos os envolvidos com o SGSI e com o comprometimento da Alta Direção, que deve demonstrar liderança.

Outro aspecto relevante, e cabe à alta direção é a elaboração de uma política de Segurança da Informação que: seja apropriada ao propósito da organização; inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação; inclua um comprometimento para satisfazer os requisitos aplicáveis, relacionados com segurança da informação; e inclua um comprometimento para a melhoria contínua do sistema de gestão da segurança da informação.

Lyra (2015) afirma que as organizações devem estabelecer e implementar um processo de avaliação de riscos. Isso envolve aplicar um processo específico para proteção dos 3 pilares, denominados CID, exemplificados na Figura 1, sendo:

- **Confidencialidade:** As informações são transmitidas de maneira sigilosa e confidencial, garantindo que apenas pessoas autorizadas tenham acesso a elas.
- **Integridade:** Assegura que a informação chegue ao destino de forma íntegra e inalterada, garantindo que o conteúdo se mantenha inalterado durante todo o processo de transmissão.
- **Disponibilidade:** visa assegurar que as informações estejam sempre acessíveis e prontas para serem consultadas pelo usuário, a qualquer momento.

Figura 1 - 3 Pilares da segurança da informação

Fonte: Google (2024)

Mirabili Junior (2023), destaca alguns aspectos adicionais para fortalecer os três pilares da segurança da informação. Na Figura 2 exemplificam-se os 6 pilares:

Figura 2 - 6 Pilares da segurança da informação

Fonte: Google (2024)

Os pilares acrescentados são:

- **Autenticidade:** Garantir a origem confiável das informações. Em outras palavras, ela assegura que cada dado pertence à fonte que o declara.
- **Conformidade:** Assegurar que todos os processos obedeçam às normas e leis vigentes e devidamente regulamentadas.
- **Irretratabilidade** ou **Não-Repúdio:** Esse é o pilar que refere habilidade do sistema que aponta se o usuário realizou uma ação específica.

Na fase de tratamento dos riscos, a ISO 27001 sugere que a organização deve selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, Hintzbergen et al. (2018) consideram que, com base nos resultados da avaliação de risco, é necessário determinar todos os controles que devem ser implementados para as opções escolhidas de tratamento do risco de segurança da informação.

Requisitos específicos da ISO 27001 incluem:

- Estabelecimento de uma política de segurança da informação, que deve ser aprovada pela alta administração da organização;

- Identificação dos ativos de informação que precisam ser protegidos e avaliação dos riscos associados a esses ativos;
- Implementação de controles de segurança da informação para gerenciar os riscos identificados, incluindo controles físicos, técnicos e administrativos;
- Designação de um responsável pela segurança da informação, que deve ser responsável pelo desenvolvimento e implementação do SGSI;
- Monitoramento e avaliação contínuos do SGSI para garantir que ele esteja funcionando de maneira eficaz e atendendo aos requisitos da norma;
- Realização de auditorias internas e externas regulares para verificar a conformidade com as normas.

2.2. Impacto da engenharia social na segurança da informação

De acordo com De Souza Pereira (2022), as empresas que adotam novas tecnologias de segurança para dificultar a exploração de vulnerabilidades podem, impensadamente, abrir portas para novas ameaças. As ameaças são como os pontos de partida para ataques ou violações em sistemas. Elas podem surgir também de forma intencional, quando um usuário tem a intenção deliberada de prejudicar a organização. Conforme De Souza Pereira (2022), os incidentes podem ser: acidental, que pode ser por descuido ou falta de informação; passivo, que não reflete impacto no negócio quando ocorrido; e ativo, incluindo a manipulação de informações, resultando em conteúdo inválido ou não confiável.

Conforme Mitnick (2003), muitos profissionais de Tecnologia da Informação (TI) erroneamente acreditam que as empresas estão imunes a ataques apenas por utilizarem produtos de segurança padrão, como firewalls, sistemas de detecção de intrusos ou autenticação avançada com dispositivos como tokens temporais (*one-time passwords - OTPs*) ou cartões biométricos. No entanto, essa crença é uma ilusão perigosa. Confiar apenas em produtos de segurança é como viver em um mundo de fantasia: mais cedo ou mais tarde, esses profissionais se tornarão vítimas de um incidente de segurança.

Piovesan (2019), atesta que a Engenharia Social é direcionada exclusivamente ao ser humano, explorando a psicologia e as interações pessoais. Isso abre um amplo leque de possibilidades para o engenheiro social, que busca identificar as vulnerabilidades de um

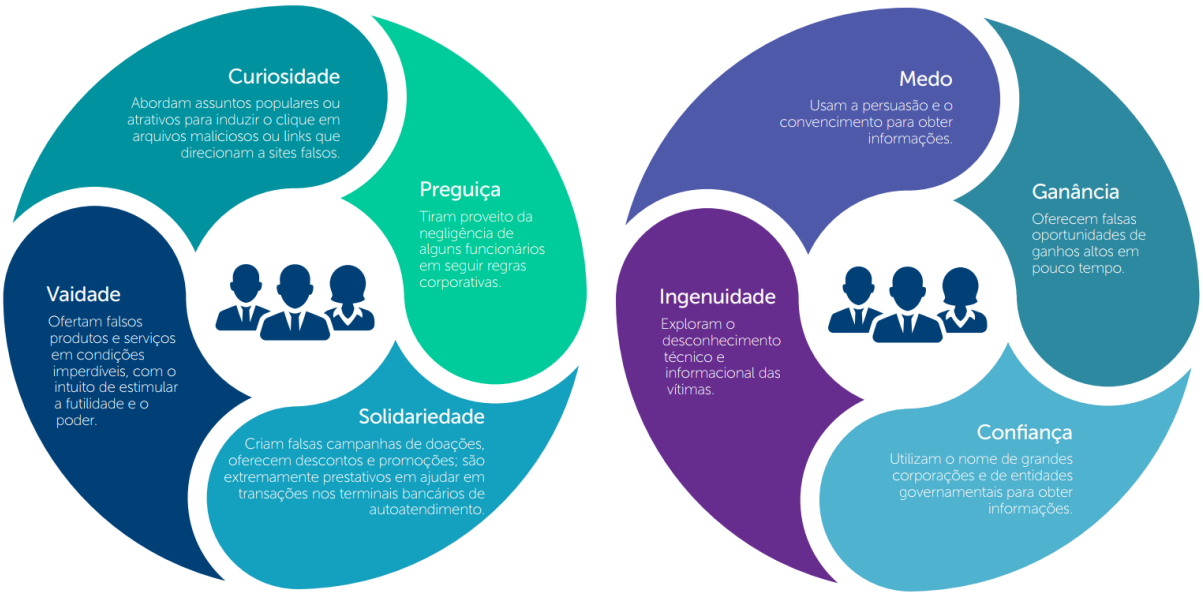
funcionário e trabalhar nelas para se aproximar, estabelecer vínculos e ganhar confiança, com o objetivo final de executar um golpe.

Para o MPSP, Ministério Público (2017), os engenheiros sociais coletam dados pessoais publicamente divulgados em locais como restaurantes, aeroportos, elevadores, táxis, hotéis e bancos. No entanto, o verdadeiro poder deles reside na exploração dos seguintes sentimentos humanos para atingir suas vítimas:

- **Curiosidade**: frequentemente abordam assuntos populares ou atraentes para induzir o clique em arquivos maliciosos ou links que direcionam a sites falsos. Eles sabem como explorar a curiosidade e os interesses das pessoas, tornando suas iscas irresistíveis.
- **Preguiça**: Aproveitam da falta de atenção de alguns funcionários em seguir as regras corporativas.
- **Solidariedade**: São extremamente prestativos, envolver as vítimas em situações aparentemente legítimas, mas que, na verdade, escondem suas verdadeiras intenções.
- **Vaidade**: Oferecem produtos, promessas tentadoras e serviços falsos, apresentando condições aparentemente imperdíveis. Tudo isso tem um objetivo de estimular a futilidade e o desejo de poder nas vítimas.
- **Medo**: Habilidosos na persuasão e do convencimento. Utilizam essas táticas para obter informações valiosas, muitas vezes explorando o medo como um gatilho para que as pessoas revelem o que desejam ocultar.
- **Ganância**: Oferecem falsas oportunidades de altos lucros em um curto período, criando isca irresistível para atrair aqueles que buscam enriquecimento rápido.
- **Confiança**: Exploram a confiança das pessoas e utilizam o nome de grandes corporações e entidades governamentais como isca para obter informações. Cria uma fachada respeitável para ganhar acesso aos dados que desejam.
- **Ingenuidade**: Se aproveitam da ingenuidade das vítimas. Exploram o desconhecimento técnico e informacional, contando com a falta de conhecimento específico para obter acesso a informações sensíveis.

Em virtude disto, as empresas devem dar a devida atenção ao fator humano relacionado a segurança da informação, assim tendo funcionários bem treinados, resultando em uma empresa mais segura e consciente. Um resumo dessas estratégias é mostrado na Figura 3.

Figura 3 - Estratégia da engenharia social



Fonte: Cartilha MPSP (2017)

Para aplicar essas fases na engenharia social é fundamental utilizar táticas adequadas para cada contexto. Batista (2015), aponta algumas delas:

- **Coleta de informações**: Durante a fase de coleta de informações, o engenheiro social geralmente obtém uma quantidade significativa de dados. No entanto, a verdadeira dificuldade reside em organizá-los de maneira que se tornem úteis. Pensar como um engenheiro social é essencial nesse processo. O engenheiro social está sempre atento aos detalhes e faz perguntas sobre tudo.

- **Elicitação**: Habilidade de fazer perguntas inteligentes é fundamental para obter respostas relevantes. A elicitação, como técnica, é tão poderosa que muitos governos educam e alertam seus funcionários sobre seu uso, uma vez que é amplamente empregada por espiões em todo o mundo.

- **Pretexto**: Embora muitos associem o pretexto apenas a contar histórias ou mentiras para serem encenadas durante uma operação de engenharia social, a definição vai, além disso. O pretexto pode ser entendido como uma história de fundo completa, incluindo personalidade e atitudes, que serve para mascarar o engenheiro social e ajudá-lo a enganar sua vítima.

- **Phishing**: Normalmente utilizado por meio de correio eletrônico, telefone ou mensagens, onde o engenheiro se passa por outra pessoa de confiança, assim a vítima pode passar informações ou acessar links maliciosos.

- **Identificar e Mitigar Ataques**: São softwares encaminhados para as vítimas, por e-mails (phishing) ou pendrives, que são instalados de forma com que o alvo não tenha seu conhecimento, assim o engenheiro social consegue extrair informações. Esses softwares podem ser vírus, trojan, keyloggers.

Utilizando informações estratégicas, paciência, criatividade e até mesmo apelos sentimentais, os golpistas operam sob o pretexto de emergências ou da necessidade de garantir máxima segurança. Ao escolher cuidadosamente suas vítimas, as chances de sucesso em seus golpes aumentam consideravelmente. Por isso, é crucial estarmos sempre alerta e continuamente conscientes dos riscos. Conforme o MPSP, Ministério Público (2017), as dicas para proteção das informações corporativas são:

- **Não forneça dados pessoais**: senhas ou informações sensíveis por telefone, e-mail ou redes sociais. Golpistas frequentemente se passam por operadores de central de atendimento ou funcionários de instituições financeiras.

- **Não forneça informações sobre a empresa**: evite fornecer informações sobre a empresa, sua estrutura física, o quadro de funcionários ou as rotinas internas, a menos que você tenha certeza de que o solicitante é confiável.

- **Fique atento**: Lembre-se de que os bancos legítimos não solicitam confirmação de dados pessoais relacionados a contas bancárias, senhas ou cartões por esses meios. Se alguém entrar em contato pedindo essas informações, desconfie e verifique antes de fornecer qualquer dado.

- **Cuidado no acesso on-line**: quando acessar ambientes on-line que exigem login e senha, desmarcar a opção de memorização de senhas e sempre clique em ‘Sair’ ao final da sua navegação.

- **Não falar sobre assuntos corporativos confidenciais**: Lembre-se de evitar descuidos ao discutir assuntos confidenciais da empresa por telefone ou em ambientes como elevadores e corredores. Sempre tem alguém a espreita de colher informações e usá-las para fins maliciosos.

- **Não confie em tudo o que ouvir ou ler**: tenha cuidado ao compartilhar links. A veiculação de notícias falsas é um grande meio para a prática de engenharia social.

- **Cuidado com o lixo**: Quando você for descartar documentos impressos ou materiais que contenham informações importantes, lembre-se de fragmentá-los antes de jogá-los no lixo.

De Souza Pereira (2022), afirma que os seres humanos são propensos a erros, a engenharia social permanece como uma ferramenta que explora uma das maiores vulnerabilidades: a tendência humana de agir de forma emocional e precipitadamente vazar informações importantes, possibilitando ataques. Mesmo quando as empresas quando investem consideravelmente em equipamentos e softwares para criar um ambiente seguro, ela permanece vulnerável a ataques. Além disso, é fundamental manter as políticas de segurança atualizadas e garantir que todos os colaboradores estejam cientes delas. Isso contribui para uma organização alinhada com as diretrizes de segurança da empresa. Além das políticas, existem outros métodos eficazes, como a realização de cursos e palestras. Essas iniciativas visam treinar e conscientizar os colaboradores, fornecendo orientações específicas sobre como agir em diferentes situações de segurança.

2.3. A segurança da informação e a conformidade com a LGPD

Na Europa está em vigor o Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation* – GDPR), sigla EU 2016/679. Em 2018, o Brasil aprovou a Lei Geral de Proteção de Dados (LGPD), que é fortemente inspirada no GDPR e compartilha muitos princípios e disposições de proteção de dados. A LGPD é vista como um passo importante para aumentar a proteção dos dados pessoais dos cidadãos brasileiros e se alinhar com os padrões internacionais de privacidade de dados.

A LGPD, Lei nº 13.709/2018, foi sancionada somente em 18 de agosto de 2018, alterando a lei nº 12.965, de 23 de abril de 2014 (o Marco Civil da Internet), que foi criada com o intuito de direcionar o tratamento de dados no Brasil. O tratamento de dados é todo o processo que deve ser feito com um dado, desde o momento que ele é coletado e colocado em um Banco de Dados, permanecendo até o momento que é excluído.

Segundo Rapôso et al. (2019), o surgimento da globalização e a expansão da Internet trouxe excesso de dados gerados a cada minuto, em inúmeras transações comerciais e sociais, demonstrando a necessidade de definição de parâmetros em forma de lei, para haver total

responsabilidade na conduta desta relação, necessitando de normatizações para a segurança da informação.

A responsabilidade das empresas na coleta, tratamento e armazenamento de dados pode ser apoiada nos três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, focando a proteção à privacidade online, a liberdade de expressão e a segurança da informação de pessoas naturais (PEIXOTO, 2020).

Em comprimento da LGPD, as empresas que coletam e manipulam dados precisam garantir a segurança contra as ameaças e os possíveis vazamentos de seus locais de tecnológicos dos últimos tempos, definidos como mecanismos computacionais destinados a levantar dados relevantes para prestar auxílio ao processo de tomada de decisão.

O artigo 48 da Lei 13.709/18 (LGPD), que elenca as ações que devem ser observadas de imediato pela empresa em caso de vazamento de dados, determina, de forma impositiva, que o controlador dos dados deve comunicar à autoridade nacional e aos titulares dos dados, imediatamente, o evento que possa colocar em risco direitos individuais. O controlador é a pessoa ou entidade que toma decisões sobre o tratamento dos dados pessoais, sendo responsável por determinar as finalidades e os meios de processamento.

A LGPD foi criada com a intenção de proteger os dados de qualquer pessoa, e impedindo que empresas manipulem ou comercializem dados pessoais, dentro ou fora do país. O cidadão, quando sentir seus direitos violados, pode acionar a justiça, impedindo que os detentores dos dados continuem manipulando dados pessoais de forma irregular, causando danos e prejuízos para usuários, os proprietários das informações

Visando o lado das empresas, aquelas que já possuem maturidade com um plano de segurança e investimentos na estrutura de segurança dos dados coletados no seu negócio, terão menos desafios e investimentos a se adequarem à LGPD. Uma forma eficiente das empresas demonstrarem boa-fé com o tratamento dos dados são com condutas implementadas em uma boa política de segurança interna, sem punições pela falta de conformidades, quando a Lei for efetivamente cobrada pelos órgãos competentes.

Diante de tudo que foi exposto anteriormente, a pesquisa dos assuntos abordados foi essencial para o desenvolvimento de materiais informativos precisos e úteis que complementam pontos relevantes do projeto. Mostrando com clareza a importância da segurança da informação nas empresas e os perigos que cercam as empresas quando não se usa recursos de prevenção

para identificar as principais ameaças e vulnerabilidades.

A Gestão de Segurança da Informação ajudou na construção da cartilha para auxiliar na proteção das informações contra as ameaças e riscos, melhorando a confiabilidade da operação da empresa, em especial:

- Na prevenção da fragilidade humana, onde estudos sobre engenharia social ajudam, a mostrar os perigos da técnica de manipulação psicológica que visa a enganar pessoas para revelar informações confidenciais da empresa. É uma das principais ameaças usada para contornar medidas de segurança tecnológicas e obter acesso a informações confidenciais.

- A importância da segurança de dados, já que muitas empresas não têm conhecimento que devem garantir a privacidade e a proteção de dados dos indivíduos. A lei geral de proteção de dados (LGPD) entrou em vigor no Brasil em setembro de 2020, essa lei que estabelece sanções para quem violar regras de proteção de dados.

- Além disso, existem outros fatores importantes que ressaltam a necessidade de as empresas manterem a proteção de equipamentos, sistemas e dados. É fundamental também que usuários e funcionários sejam treinados para enfrentar riscos e ameaças, tanto tecnológicas quanto humanas, que estão sempre à espreita para potencializar um ataque.

OAB, Jornal Da Advocacia (2023), a lei trouxe pontos extremamente positivos para o país, e nos casos de não conformidade, as consequências advindas da Autoridade Nacional de Proteção de Dados (ANPD) são as aplicações das sanções previstas em lei.

3. METODOLOGIA

Para atingir os objetivos geral e específico apresentados no Capítulo 1, neste trabalho se propôs a confecção de uma cartilha para conscientizar as empresas de pequeno e médio porte sobre importância e funções desempenhadas pelo do suporte de TI ao manter equipamentos, sistemas e dados seguros.

Jakkal (2022), afirma que "o que torna as PMEs particularmente vulneráveis é o fato de elas geralmente terem menos recursos e não possuírem uma equipe de segurança especializada". A cartilha de segurança da informação pode ser uma ferramenta essencial para ajudar administradores, gestores e funcionários da empresa a compreenderem os perigos decorrentes da falta de manutenção dos equipamentos (servidores, terminais e ambiente de rede), bem como dos perigos cibernéticos.

Neste capítulo são apresentados os materiais e métodos utilizados para desenvolver o trabalho. Os materiais estão relacionados às ferramentas e tecnologias, já os métodos são um conjunto de atividades de apoio necessárias para construção da cartilha. Sendo assim, o capítulo se divide em: 3.1 Materiais, 3.2 Métodos, 3.3 Confecção da Cartilha.

3.1. Materiais

Para a confecção de uma cartilha impressa, foram verificadas formas adequadas para garantir uma boa leitura, utilizando a estratégia de copywriting, de uma linguagem clara e simples, sem jargões técnicos ou termos complexos que possam confundir o leitor. E sobre essa técnica, ALBRIGHTON, Tom (2013), afirma que, a melhor maneira de se comunicar é a escolha certa das palavras, uma arte útil e criativa para deixa a leitura mais sugestiva.

Para tornar a cartilha mais dinâmica e atrativa, foram incluídas tanto imagens reais quanto figuras animadas nas ilustrações, com o objetivo de despertar maior interesse do leitor pelo conteúdo. Foram definidos os seguintes parâmetros para a definição do conteúdo:

- Tamanho aproximado do formato A5: 17cm x 20cm, capa com detalhe da lateral esquerda azul espelhado 17cm x 7cm.
- Ilustração com desenhos dos equipamentos: servidores, terminais, ícones de segurança, telas de login e exemplos de phishing.
- Extensão da cartilha com 10 páginas, impressão frente e verso, na última página uma tabela de controle de manutenção.

- Software para desenvolvimento das artes da cartilha será o Adobe Photoshop para edição de imagens da capa, CorelDRAW 2020 para criação dos desenhos, que ilustrarão as páginas.

3.2. Métodos

Para a evolução do trabalho proposto, foi utilizado o conhecimento fornecido pelo suporte de TI, que identificou fatores como a falta de continuidade na manutenção de sistemas e terminais na maioria das empresas. Observou-se que muitos colaboradores, têm pouco conhecimento das ferramentas tecnológicas que utilizam, o que impede de comunicar com clareza as dificuldades que enfrentam. A maioria das falhas ocorre devido à falta de conhecimento tecnológico dos usuários, que não conseguem relatar adequadamente os problemas ao suporte. Com isso, ao identificar esses pontos frágeis, puderam ser definidos os temas abordados na construção da cartilha.

3.3. Construção da Cartilha

A cartilha foi elaborada com etapas e sequência claramente definidas, visando estabelecer uma organização eficiente e uma abordagem prática e lógica. As etapas subsequentes incluem: Manter os dados, equipamentos e sistemas das empresas seguras, boas práticas da segurança da informação, manutenção em dia, segurança em redes, análise de vulnerabilidade e risco, conscientização da conformidade com a LGPD.

3.3.1. Manter os dados e equipamentos seguros

A importância do auxílio do suporte da TI (Tecnologia da informação) essencial para manter a integridade das empresas, prevenir futuras falhas e prevenir perda de equipamentos e sistemas, garantido a segurança dos dados e informações.

Os objetivos específicos do suporte de TI na segurança da informação incluem:

- Problemas técnicos: resolver problemas técnicos enfrentados pelos usuários. Assim sendo problema de hardware, software, rede e segurança.

- Infraestrutura: manter e garantir que a Infraestrutura esteja em boas condições. Sendo esses a manutenção preventiva, atualização de software e hardware, gerenciamento de rede e backup de dados.

- Garantir a segurança: o suporte de TI analisa as vulnerabilidades e corrige os pontos frágeis que põem em risco a segurança da empresa, garantindo a integridade dos dados. Isso pode incluir a instalação e manutenção de firewalls, antivírus, soluções de backup, além de outras medidas de segurança.

- Melhorar a eficiência: melhorar a eficiência da empresa por meio da automação de tarefas repetitivas e reduzir o tempo necessário para a realização de processos administrativos, resultando em economia de tempo e recursos.

3.3.2. Boas práticas da segurança da informação

Para garantir boas práticas de segurança da informação, é fundamental treinar e conscientizar os funcionários. A equipe deve entender como funciona sua ferramenta básica de trabalho e seguir algumas recomendações do suporte técnico. Entre elas estão: atualizar softwares, controlar acessos, fazer cópias de segurança, estabelecer uma política de segurança, usar senhas fortes e adotar um bom antivírus.

3.3.3. Manutenção em dia

A manutenção preventiva evita imprevistos nos momentos em que o bom funcionamento dos equipamentos é mais necessário. Ela consiste em uma verificação completa de todos os sistemas vitais dos equipamentos, garantindo que continuem operando de forma eficiente. Sem a manutenção periódica, a empresa assume riscos iminentes, como a ocorrência de acidentes ou problemas na parte lógica, ou física dos equipamentos.

3.3.4. Segurança no ambiente de rede

O ambiente de rede é um dos mais complexos no suporte às empresas. A maioria delas não segue as orientações e recomendações para o bom funcionamento da comunicação entre equipamentos e terminais. Uma infraestrutura qualificada e organizada facilita a manutenção e aumenta a segurança empresarial.

Na Figura 3, tem-se um exemplo de rede comprometida por não ter equipamentos adequados e estarem totalmente desorganizados. Os equipamentos inadequados e cabeamento sem qualidade e desorganizado, comprometem muito o funcionamento da rede da empresa, causando lentidão, paralisação e demora no reparo desse ambiente de rede.

Figura 4 - Estrutura de rede comprometida.

Fonte: Autoria própria (2022)

Um ambiente de rede estruturado, com organização e equipamentos adequados, facilita a identificação das conexões dos cabos, agiliza a manutenção e, consequentemente, reduz significativamente os custos, que anteriormente eram elevados devido à necessidade de manutenções frequentes.

Para manter a eficiência do ambiente de rede, é necessário a implementação de ferramentas de gerência automática do fluxo da rede, agilizando os serviços que eram complexos. Essa ferramenta é ideal para manter o controle de tudo que se passa no ambiente interno e externo, fortalecendo a segurança, blindando o tráfego dos dados, facilitando o controle de acesso e monitoramento de navegação.

Nakamura (2007), para proteção do ambiente de rede das organizações, utiliza-se métodos e ferramentas essenciais que são:

- **Firewall:** é uma ferramenta que limita o acesso às portas do computador e, assim, impede a entrada de invasores, somente usuários autorizados terão permissão para executar algumas funcionalidades da máquina. Basicamente, o Firewall impede a entrada e saída de informações confidenciais, controlando a transferência de dados do computador através da internet, e prevenindo o acesso de arquivos privados à rede. Uma

boa gestão do Firewall faz toda a diferença, protegendo a rede de vários riscos e vulnerabilidades.

- **IDS** e o **IPS**: O IDS (*Intrusion Detection System*) e o IPS (*Intrusion Prevention System*) complementam o trabalho do Firewall. O IDS identifica qualquer tipo de atividade estranha na rede. Por exemplo: Downloads excessivos de arquivos. Após fazer isso, ele manda essa informação de alerta para o IPS, que vai tomar as ações de bloqueio do IP que está executando esses downloads na rede.

- **Web Filter**, proteção interna, já que nem todos os ataques são externos; na verdade, muitos deles vêm de dentro da sua própria rede. Sendo assim, é essencial uma proteção para quem está na rede: os computadores e os usuários da rede. Essa é a função do Web Filter (ou filtro de navegação). Ele, basicamente, executa um monitoramento dos sites acessados no ambiente empresarial, atuando como um filtro que restringe o que pode ou não pode ser acessado, protegendo, assim, a navegação.

- **VPN** como proteção para o acesso remoto tornou-se essencial! E é exatamente isso que a VPN faz: ela cria um túnel seguro, criptografando todos os dados que ali trafegam, onde somente o usuário autorizado pode acessar a rede da empresa. O sistema de acesso temporário serve basicamente para proteger os visitantes da rede; ele realiza o monitoramento da rede para garantir que todas as vulnerabilidades dos dispositivos e acessos dos visitantes não sejam um risco para a rede da empresa.

3.3.5. Análise de vulnerabilidade e risco

Na cidade de Assú–RN, poucas empresas de suporte de informática prestam serviços mais voltados para automação comercial, como assessoria, revenda e suporte de software, segurança tecnológica ou análise de vulnerabilidade. Esse motivo é dedicado nesta página da cartilha à importância da prevenção de futuras falhas e ao fortalecimento da segurança da empresa.

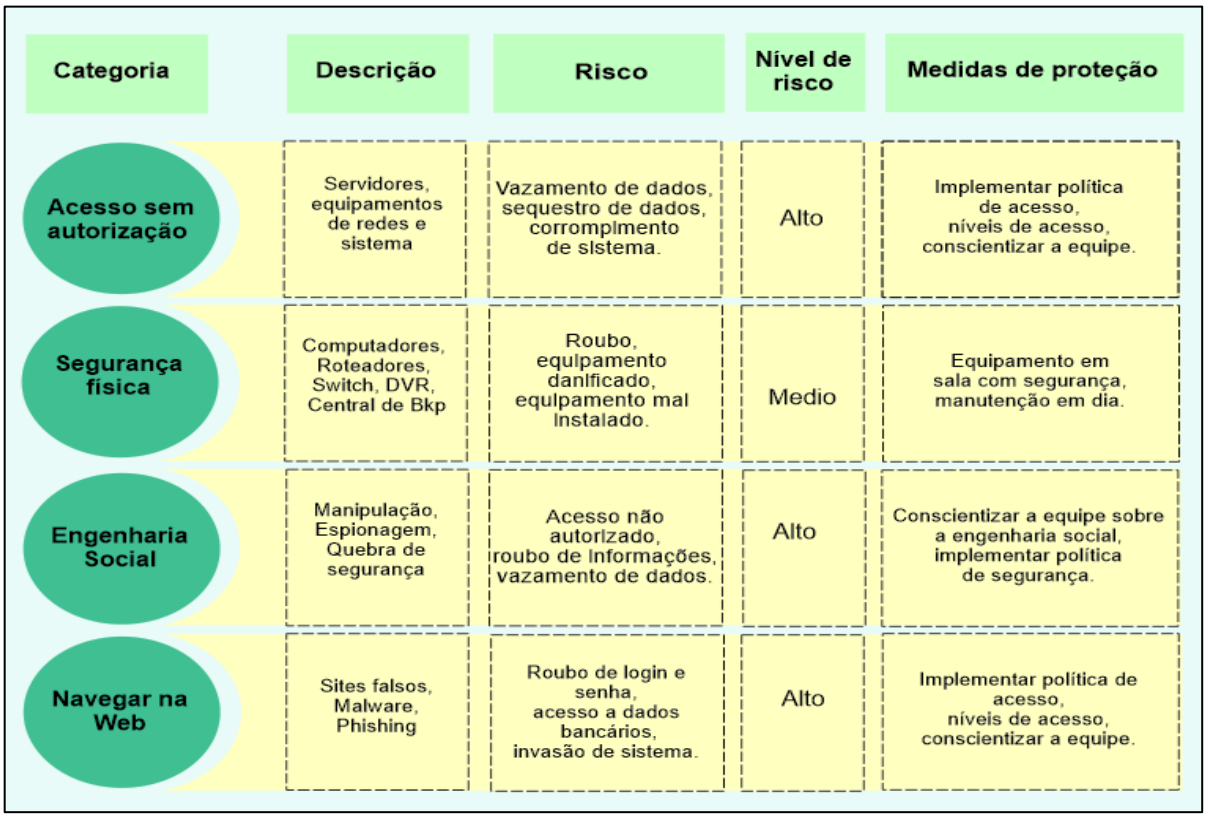
Conforme Jakkal (2022), as pequenas e médias empresas necessitam de segurança avançada. Grande parte dessas PMEs conta com antivírus tradicionais, que fornecem uma única camada de proteção; o ideal é ter várias camadas com as 5 fases: identificar, proteger, responder, recuperar.

A análise de vulnerabilidade é essencial para ambos os portes, mas não tem somente caráter preventivo, uma vez que é fundamental para garantir a melhoria contínua de serviços e

da segurança, evitando risco: físicos e lógicos. Conforme a IBM (2023), o risco se expande em milhares de novas vulnerabilidades, relatadas em aplicações e dispositivos antigos e novos.

Na Figura 1, o levantamento das fragilidades encontradas na maioria das empresas atendidas pela equipe de suporte de TI. Os pontos frágeis descrito por: categoria, descrição, risco, nível de risco e medidas de proteção.

Figura 5 - Análise de Vulnerabilidade e Risco



Fonte: Autoria própria (2022)

O processo de análise de vulnerabilidade e risco é importante na gestão da segurança da informação. Isso inclui identificar, analisar e classificar vulnerabilidades que podem comprometer a segurança da sua infraestrutura tecnológica.

> Para extrair todo o potencial de uma análise de riscos, é preciso considerar em seu escopo todo o espectro de ativos presentes no ambiente corporativo que, de forma direta ou indireta, suportam seus processos de negócio. Além disso, é fator crítico de sucesso mapear os relacionamentos dos processos com os ativos, pois só assim será possível gerar um diagnóstico efetivamente orientador e alinhado com os interesses da empresa (SÊMOLA, Marcos, 2014).

Compreender as vulnerabilidades é crucial para entender as ameaças que elas representam. A classificação de vulnerabilidades permite coletar dados sobre a frequência, analisar tendências de vulnerabilidades, correlacionar com incidentes, exploits e artefatos, e

avaliar a efetividade das contramedidas (Seacord e Householder, 2005). A seguir, estão alguns pontos importantes sobre a análise de vulnerabilidade e risco:

- **Identificar Vulnerabilidades:** Após análise, todas as falhas e potenciais ameaças à segurança de uma infraestrutura tecnológica são identificadas. Isso pode incluir falhas em configurações de software, ausência de atualizações de segurança, permissões de acesso padrão, e outros.
- **Analisar Vulnerabilidades:** Uma vez identificadas as vulnerabilidades, elas são analisadas para entender o impacto que poderiam ter na segurança da informação. Isso permite que a empresa conheça os pontos fracos da sua cibersegurança.
- **Classificar Vulnerabilidades:** Utiliza pares de atributos e valores para fornecer uma visão multidimensional das vulnerabilidades. As vulnerabilidades são identificadas e então classificadas com base em seu nível de risco. Isso ajuda a priorizar quais vulnerabilidades devem ser tratadas primeiro.
- **Gerenciar Riscos:** Após a classificação, a gestão de riscos envolve a adoção de medidas para mitigar os riscos identificados. Isso pode incluir a correção de falhas, a implementação de controles de segurança adicionais e a educação dos usuários sobre práticas seguras.

A análise de vulnerabilidade e risco é um processo contínuo e deve ser realizada regularmente para garantir que novas vulnerabilidades sejam identificadas e tratadas prontamente.

3.3.6. Conscientização da conformidade com a LGPD

Com as recentes visitas da equipe de suporte de TI para o preenchimento do formulário para verificar o nível de conhecimento da equipe das empresas, foi constatado que a maioria das empresas da cidade de Assú-RN não tem conhecimento sobre a LGPD (Lei Geral de Proteção de Dados), não tendo a noção da relevância da manutenção da segurança dos dados. Se a boa prática da manutenção da proteção não estiver adequada à legislação que estabelece regras para o tratamento de dados dos indivíduos, a empresa pode sofrer multas, penalidades e perdas de contratos por não se adequar à LGPD. O órgão federal responsável pela fiscalização do cumprimento da lei LGPD e aplicação das penalidades é ANPD (Autoridade Nacional de Proteção de Dados), com logo visto na Figura 6.

Figura 6 - Autoridade Nacional de Proteção de Dados

Fonte: Autoria própria (2022)

Os riscos para a não adequação à LGPD levam sanções por descumprimento. Conforme a OAB, Jornal da Advocacia (2023), a certificação de inadequação do regulamento da ANPD leva a sanções que variam conforme a complexidade da infração, bem como com outros fatores, as seguintes:

- **Advertência:** serve como um aviso de que a organização ou indivíduo está em desacordo com as disposições da LGPD e deve tomar medidas corretivas para se adequar às normas de proteção de dados. É a mais branda das sanções.

- **Multa:** A multa pode ser simples, ou seja, aplicada uma vez sobre a infração, ou diária, sendo aplicado um valor permanente a cada dia que a infração persistir. Elas possuem um limite de até 2% do faturamento do grupo econômico no último ano de exercício fiscal, podendo chegar ao máximo de R$ 50 milhões por infração.

- **Restringir o uso de dados pessoais:** A empresa infratora poderá ter, de maneira parcial ou total, o bloqueio dos dados referentes à infração, até que a empresa esteja regularizada.

- **Bloqueio ou eliminação permanente:** em casos mais graves, a suspensão pode ser mantida, mesmo que a empresa tenha regularizado o tratamento, podendo o bloqueio (ou eliminação) dos dados ser até mesmo permanente. É possível, ainda, que a ANPD proíba parcial ou totalmente as atividades relacionadas ao uso de dados, ainda que não tenham ligação direta com a infração em questão.

- **Publicizar a infração:** dentre as possibilidades de penalidade está o dever de publicizar a ocorrência de uma infração. Tornar uma infração à LGPD um acontecimento público pode ter muitas consequências e, claro, pode afetar a imagem de uma empresa perante seus clientes. A sanção de publicização pode ter efeitos pequenos ou muito grandes, a depender do quanto as pessoas afetadas se importam com a proteção de seus dados pessoais.

- **Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados:** A ANPD (Autoridade Nacional de Proteção de Dados) pode proibir, temporária ou definitivamente, o exercício de atividades relacionadas ao tratamento de dados pessoais.

Conforme a OAB, Jornal da Advocacia (2023), garantir a privacidade e proteção das informações é muito importante, as empresas têm que deixar evidente a finalidade dos dados de funcionários e clientes, por exemplo, o ciclo de vida dos dados pessoais, do momento da coleta por consentimento ou outra base legal até o arquivamento, ou eliminação deles.

A LGPD pode gerar muitas dúvidas, principalmente entre pessoas empreendedoras que estão iniciando sua jornada digital ou entre as mais antigas sem uma consultoria empresarial atualizada. É muito importante se preocupar com ela por conta das vulnerabilidades que envolvem o tratamento de dados pessoais.

É com essa base que na cartilha são apresentados detalhes da conformidade da Lei Geral de Proteção de Dados, mostrando as vantagens que as organizações que se adaptam às normas podem ter. Empresas que se adequam à LGPD oferecem vantagens aos titulares. A seguir, estão alguns exemplos.

- **Redução de Riscos:** Medidas de segurança diminuem violações e vazamentos de dados, protegendo a reputação da empresa e evitando perdas financeiras.
- **Valorização da Reputação:** A conformidade com a LGPD fortalece a imagem da empresa, atraindo novos investidores e valorizando seu principal ativo intangível.
- **Gerenciamento Eficiente de Dados:** A LGPD exige práticas adequadas para o manejo de dados pessoais, resultando em processos mais claros e seguros.
- **Fortalecimento da Confiança:** O comprometimento com a proteção de dados pessoais aumenta a credibilidade das empresas e solidifica relacionamentos com os clientes, elevando a lealdade e a satisfação.

3.3.7. Engenharia social

A maioria das empresas não sabe o que são ataques de engenharia social; por não ter a noção sobre o assunto, compartilham informações importantes para todos os setores da empresa, passando, sem saber, assuntos que para eles são irrelevantes, mas para os criminosos são informações riquíssimas para serem exploradas. Por não saberem lidar com esse problema,

essa parte da cartilha é direcionada para ajudar as empresas a conscientizarem os funcionários sobre como acontecem os ataques e como proteger as informações, ajudando a blindar a equipe de futuros ataques.

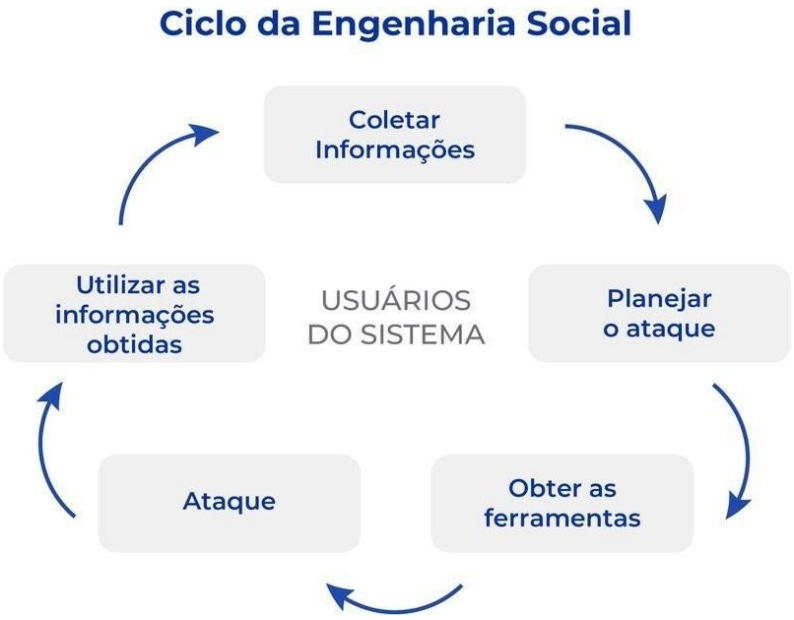
As pessoas são suscetíveis a manipulações na internet, por desatenção ou desconhecimento, sendo alvos de criminosos que exploram essa vulnerabilidade para obter informações privadas e dados confidenciais. Para Mitnick, (2003) "A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que, na verdade, ele não é, ou pela manipulação".

A estratégia de ouvir profundamente o outro, considerando cuidadosamente as necessidades de alguém, cria uma conexão entre o golpista e a vítima. Isso deixa essa pessoa mais vulnerável; então, os cibercriminosos utilizam todas as técnicas, combinando e escolhendo a melhor maneira de atingir suas vítimas. Existem diversos tipos de golpes dos quais podemos cair, quando os criminosos atuam na construção de narrativas falsas, em que a vítima se envolve verdadeiramente, incapaz de perceber que está sendo enganada! O *phishing* ocorre quando a vítima clica em um link malicioso ou em um e-mail suspeito, abrindo uma porta do seu dispositivo para os criminosos. Já o *ransomware* acontece quando o dispositivo ou sistema é invadido - geralmente por falha humana - e dados são roubados. Para Mitnik (2003):

> Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções tais como medo, agitação ou culpa. Eles fazem isso usando os gatilhos psicológicos — os mecanismos automáticos que levam as pessoas a responderem às solicitações sem uma análise cuidadosa das informações disponíveis. Todos queremos evitar as situações difíceis para nós mesmos e para os outros. Com base nesse impulso positivo, o atacante pode jogar com a simpatia de uma pessoa, fazer a sua vítima se sentir culpada ou usar a intimidação como uma arma (Mitnick, 2003).

A Figura 7, apresenta os estágios no ciclo na engenharia social, explica como funciona as estratégia dos criminosos quando identificam as vítimas, eles planejam formas e argumentos convincentes, para manter uma aproximação, ganhar a confiança para em seguida colocar em prática os métodos de ataque, conseguindo a coletar os dados importantes, utilização as informações obtidas, após executar o ataque, eles somem ou continua no ciclo até colher mais informação para novo ataque (IBM, 2023).

Figura 7 - Estratégia da Engenharia Social



Fonte: Google

Estágios da engenharia social:

- **Credibilidade e confiança:** Ao demonstrar comprometimento com a proteção dos dados pessoais de seus clientes, as empresas aumentam sua credibilidade e fortalecem a confiança com seus usuários. Isso pode resultar em relacionamentos mais sólidos com os clientes, aumentando a lealdade e a satisfação.

- **Coleta de informações**: No primeiro estágio do ciclo de vida da engenharia social, os invasores coletam informações valiosas sobre seu alvo. Isso pode incluir a pesquisa da presença online do alvo, a identificação de possíveis vulnerabilidades e a coleta de dados sobre indivíduos dentro da organização. O objetivo é adaptar seu ataque para parecer convincente e relevante.
- **Gancho:** Uma vez que os invasores tenham informações suficientes, eles criam um cenário ou uma isca convincente, muitas vezes usando táticas psicológicas para manipular o comportamento humano. Isso pode envolver a elaboração de um e-mail, telefonema ou mensagem enganosa que pareça legítima e atraente para o alvo. O "gancho" foi projetado para despertar a curiosidade do alvo ou explorar suas emoções.
- **Exploração:** Com o alvo engajado, o invasor explora sua confiança, curiosidade ou emoções para atingir seus objetivos. Esta etapa pode envolver convencer o alvo a revelar informações confidenciais, como credenciais de login, ou a realizar ações que beneficiem o invasor, como baixar malware ou transferir fundos.

- **Execução:** Na fase final, o plano do atacante se concretiza. Eles utilizam as informações ou ações obtidas nas etapas anteriores para atingir seus objetivos maliciosos. Isso pode envolver a obtenção de acesso não autorizado aos sistemas, o roubo de dados confidenciais ou o dano financeiro ao alvo, ou à organização.

Segundo as análises da IBM (2023), é difícil impedir a engenharia social por ela depender da psicologia humana em vez de soluções tecnológicas. Por isso, os ataques são mais contundentes na organização, já que um erro de apenas um funcionário pode comprometer a integridade corporativa. Para defesa contra a engenharia social, seguem as etapas que os especialistas recomendam para mitigar o risco e o sucesso dos golpes são:

- Treinamento de conscientização de segurança: Explica para os funcionários a política de segurança, como atuam os golpistas, como proteger os dados e detectar ataques.
- Políticas de controle de acesso: Implementa acesso para quem tenha sido depurado na autenticação do usuário.
- Tecnologia de segurança: Sistema de filtro contra spam e gateways para impedir ataques de phishing.

A evolução tecnológica trouxe inúmeros benefícios para a sociedade. No entanto, à medida que as novas tecnologias evoluíram, as vulnerabilidades dos sistemas também aumentavam exponencialmente. Hackerd e golpistas aproveitam essas falhas, aplicando certas técnicas, combinadas com o poder de persuasão, transformam-nas em oportunidades para prática de crimes (MPSP, Ministério Publico, 2017).

4. CONFECÇÃO DA CARTILHA

4.1. Conteúdo da cartilha

O conteúdo da cartilha foi concebido com base nas necessidades das empresas, visando despertar uma compreensão expressiva da realidade diante dos usos inadequados das ferramentas da informação, como computadores, redes e sistemas internos. O uso inadequado dessas ferramentas pode acarretar vários problemas sérios, podendo paralisar o funcionamento da empresa.

A página inicial mostra a importância do suporte de TI (tecnologia da informação) para a manutenção e proteção das organizações, enfatizando a necessidade de profissionais capacitados para um bom funcionamento e segurança da empresa.

Nas páginas seguintes, são apresentadas informações com imagens e exemplos de como a manutenção de equipamentos em dia, além de mostrar o perigo que acontece se a manutenção regular não for mantida, conforme as informações do suporte. São abordadas questões como os riscos da navegação em links desconhecidos e não autorizados pela empresa, além do vazamento de informações sigilosas por meio de conversas e documentações impressas.

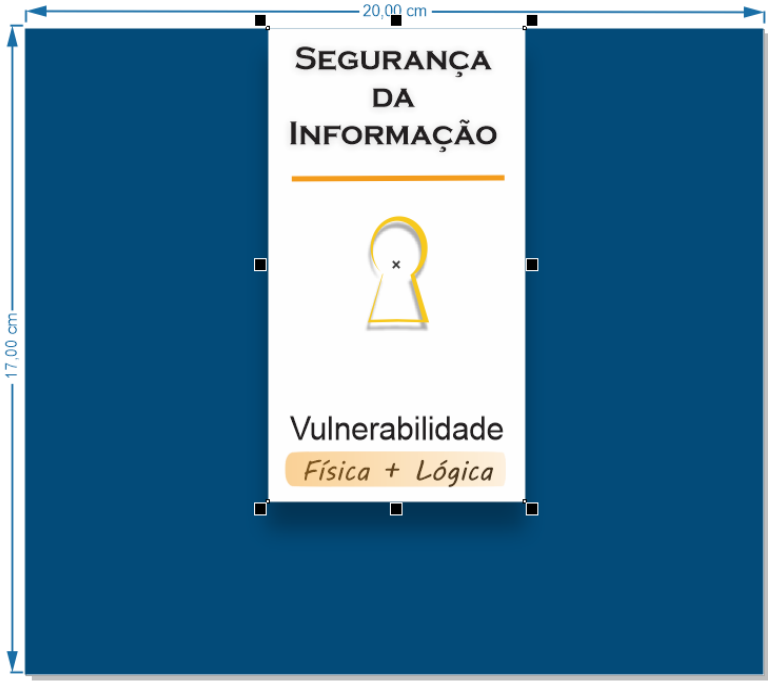
É por meio dessas informações que o conteúdo da cartilha busca conscientizar tanto empresas quanto funcionários sobre a importância da segurança da informação.

4.2. Design da cartilha

O desenvolvimento deste trabalho foi baseado com suporte de profissionais de TI, com as dificuldades de entendimento dos clientes na área tecnológica e a fragilidade física e lógicas onde trabalha, e com isso foi possível ver os pontos mais críticos para elaborar a cartilha de maneira que facilitasse o entendimento e impactasse-se o leitor.

A estrutura da cartilha foi elaborada com programa de arte gráfica CorelDRAW versão 2020, tratamento das ilustrações com o Photoshop CS6. A dimensão proposta foi de 17cm de altura e 20cm de largura, facilitando o manuseio. Foi usado também o programa de edição de imagens o Photoshop CS6 para redimensionar e tratar as ilustrações para ser trabalhada no Corel Draw.

Figura 8 - Capa da Cartilha.



Fonte: Autoria própria (2023)

Figura 9 - Verso da Cartilha

Fonte: Autoria própria (2023)

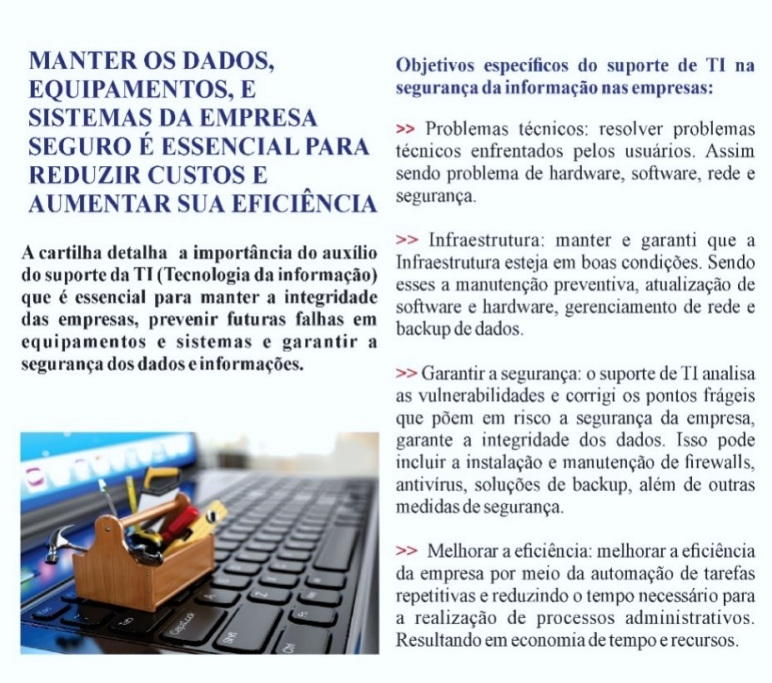
Na página seguinte, apresentação da cartilha (Figura 10), mostra-se a importância do suporte do TI para a manutenção da segurança e funcionalidade das empresas.

Figura 10 - Apresentação e a importância do TI.

Fonte: Autoria própria (2023)

Na Figura 11 detalha-se o objetivo específico do suporte da segurança da informação nas empresas. Explicação das etapas de qualificação da manutenção da segurança, trabalho e análise de vulnerabilidade que as empresas enfrentam no dia a dia com: problemas técnicos, infraestrutura e segurança.

Figura 11 - Objetivo do suporte.



Fonte: Autoria própria (2023)

Algumas figuras estampadas na parte física de equipamentos mostram a realidade de quando não há uma manutenção adequada, detalhando os riscos que a empresa corre e possíveis prejuízos incalculáveis. Essa é a intenção de mostrar o máximo possível da realidade presente em setores de assistência técnica.

Figura 12 - Problema físico

Fonte: Autoria própria (2023)

As imagens mostram a realidade encontrada na maioria das empresas que perdem vários equipamentos por não se adequarem às recomendações sugeridas pelo suporte técnico.

Na maioria das vezes, o chamado ao suporte técnico é aberto quando o problema já está instalado. Esses danos geralmente são irreversíveis e podem levar à paralisação da empresa, resultando em muitos prejuízos.

O fator mais comum é a acumulação de poeira e umidade, que cria uma oxidação na placa eletrônica, fazendo uma película isolante nos componentes, principalmente os condutores revestidos em cobre, como: slot, memória, USB, conectores de rede e outros.

Com o tempo, esse acúmulo de poeira e umidade eleva a temperatura dos componentes por falta de ventilação proporcionada pelo travamento das ventoinhas de ventilação dos coolers, que ajuda a resfriar os dissipadores (placa metálica que fica em contato direto com o chip).

A oxidação, além de fazer isolamento e causar falha de comunicação entre componentes elétricos, causa corrosão nos contatos de peças revestidas com cobre, um dano que é difícil de reverter e que, na maioria das vezes, a empresa tem que substituir o equipamento.

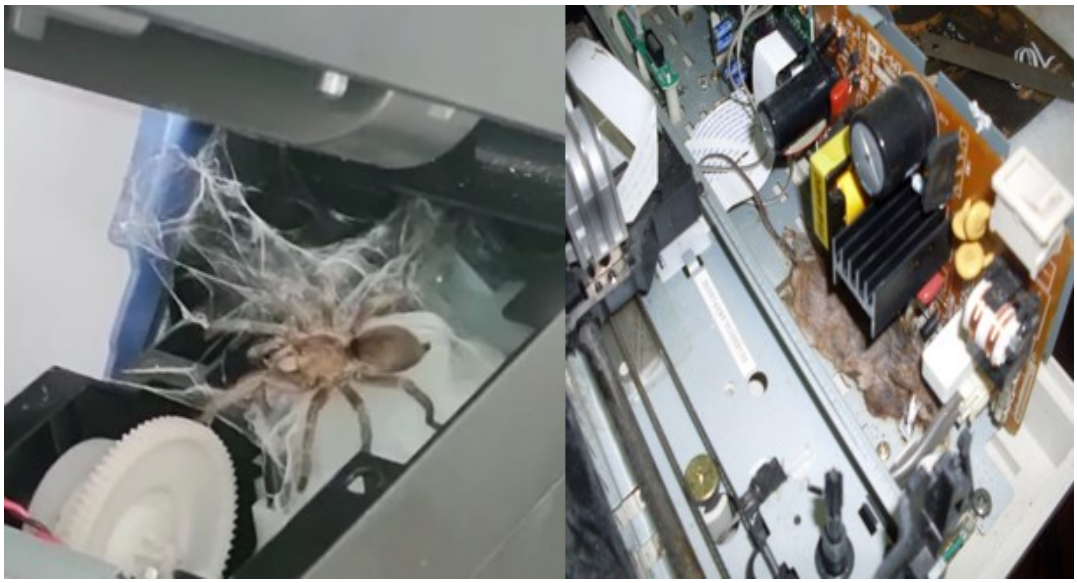
A falta de manutenção preventiva reduz bastante a vida útil de equipamentos; limpeza e lubrificação periódica reduzem os riscos de falhas constantes e perda total dos eletrônicos.

Ventilação e dissipação de calor comprometidas levam a um superaquecimento, causado pela sujeira; isso acarreta vários problemas graves que são:

- Na redução da vida útil dos componentes e mau funcionamento do sistema.
- A atuar como um isolante térmico, impedindo que o calor seja dissipado eficientemente. Isso faz com que os componentes internos do computador aqueçam mais rapidamente e atinjam temperaturas mais altas do que o normal.
- Condução elétrica: Em casos extremos, a poeira acumulada pode se tornar condutiva e causar curtos-circuitos nos componentes eletrônicos, levando a danos permanentes.

Figura 13, têm-se ilustrações de pequenos animais encontrando dentro de equipamentos, que foram danificados. Onde não tem uma manutenção adequada, além do acúmulo de sujeira, vira casa de moradores ou visitantes indesejáveis.

Figura 13 - Pequeno animais invasores.

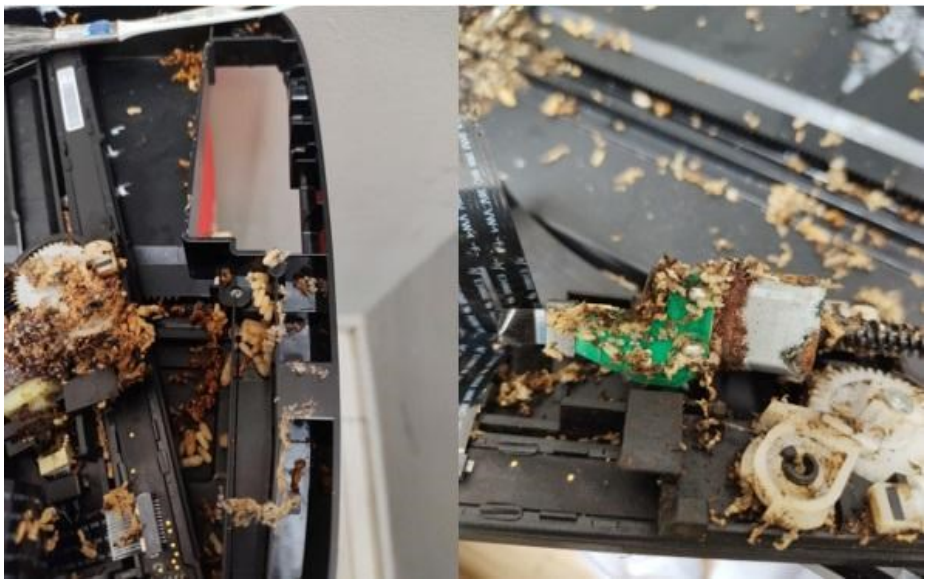


Fonte: Autoria própria (2023)

Equipamentos isolados e sem manutenção se tornam abrigo de pequenos animais ou insetos. Por mais isolado que esteja e bem protegido, o ambiente escuro e silencioso é a moradia perfeita para pequenos animais; em qualquer fresta, há uma grande porta para se instalarem silenciosamente, e assim, aos poucos, vão danificando e comprometendo o funcionamento dos equipamentos.

Na Figura 14, mostra com detalhes os danos causados por um formigueiro que destruíram os circuitos e motores eletrônicos de um scanner da impressora multifuncional, o scanner não era frequentemente usado, passando meses sem uso, somente usavam para impressão, quando foi necessário o uso do scanner foi percebido o enorme formigueiro.

Figura 14 - Danos Eletrônico.



Fonte: Autoria própria (2023)

A principal porta de entrada de pequenos animais e insetos é a ventilação dos equipamentos, por menor que seja, para insetos isso não é obstáculo, sendo sempre importante manter vigilantes e manter a manutenção em dia para evitar surpresas desagradáveis.

As figuras na cartilha destacam a importância do suporte de TI para a segurança e funcionamento das empresas. Os riscos de falta de manutenção e acúmulo de sujeira foram mostrados, revelando problemas como oxidação nas placas eletrônicas e superaquecimento, além de facilitar a presença de pequenos animais nos equipamentos. Diante do exposto, no próximo capítulo são apresentados os resultados e considerações finais.

5. RESULTADOS E CONSIDERAÇÕES FINAIS

O principal resultado obtido foi a elaboração da cartilha, que serviu como um guia prático para a segurança da informação. Outros resultados também foram identificados, como a conscientização das empresas sobre a importância da segurança de TI e a aceitação da cartilha pelos gestores. A versão para impressão da cartilha está disponível em: https://drive.google.com/file/d/188T77V3AGBDwRdJWR9Hg91_4mIS32DS5

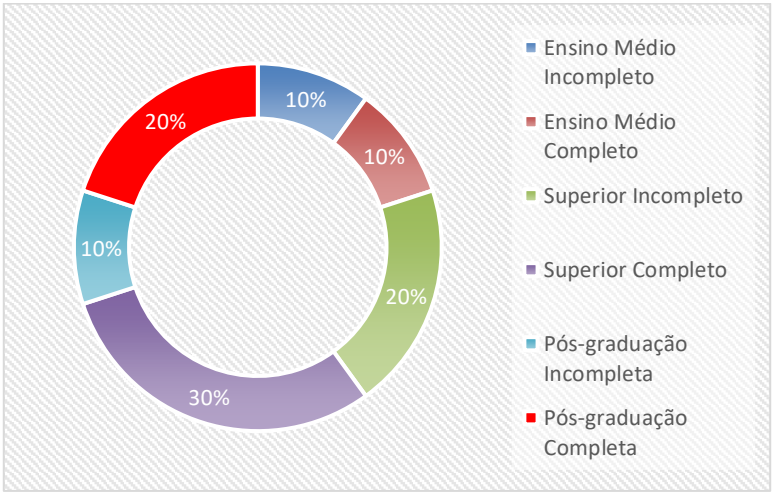
Para a coleta dos dados da pesquisa, foram utilizados questionários objetivos e simples, com 12 perguntas, baseadas nas dificuldades relatadas quando as empresas fazem chamados de incidentes ao suporte de TI. A pesquisa foi encaminhada para 10 empresas e respondida somente pela gerência ou diretoria para obter uma plenitude nas respostas.

Em cada empresa visitada, a finalidade da pesquisa e a coleta dos dados foram explica das e detalhadas. As respostas foram todas positivas e bem aceitas pelos responsáveis das emp resas.

5.1. Resultado Quantitativo - Grau de Instrução e Conhecimento em Informática.

No Gráfico 1, ilustra-se o grau de instrução dos usuários é equivalente à porcentagem, a maioria tem o grau de instrução superior completo que é 30%, e 20% são pós-graduados e 20% Superior incompleto. Destes usuários, nem um tem formação na área tecnologia e alguns com conhecimento na área técnica.

Gráfico 1 - Grau de instrução.

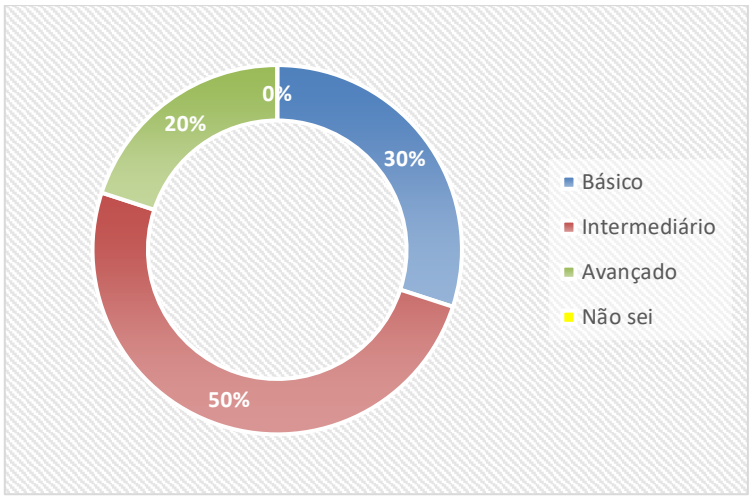


Fonte: Autoria própria (2024)

O nível de conhecimento de informática, nota-se que a maioria dos usuários tem níveis intermediários, 50% são capazes de realizar tarefas comuns no computador, como navegar na

internet e usar programas básicos, 30% sabem o básico: usar e-mail e realizar tarefas simples (Word e Excel) e 20% nível avançado, capaz de resolução de problemas técnicos. No Gráfico 2 mostra-se a representação das porcentagens.

Gráfico 2 - Nível de conhecimento em informática.

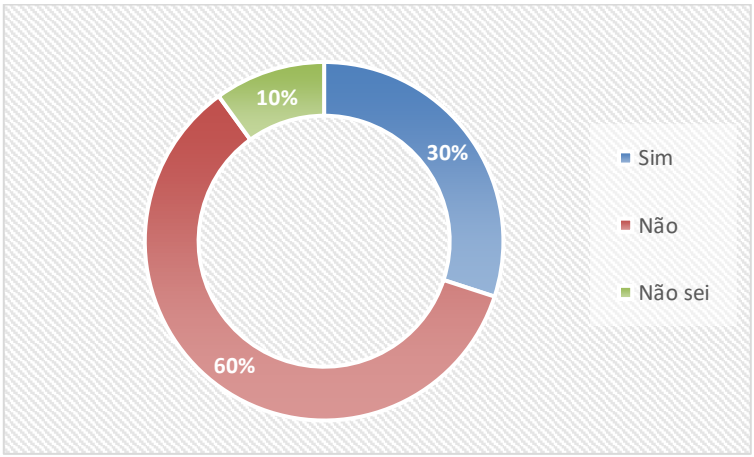


Fonte: Autoria própria (2024)

5.2. Resultado Quantitativo - Segurança da Informação

No Gráfico 3, nota-se que a maioria das empresas não seguem corretamente as normas de segurança, 60% não usam restrições de acesso à internet, deixando os usuários livres para interagir em qualquer plataforma, colocando em risco os dados e software, 30% estão adequados, com acesso gerenciado pelo administrador, bloqueando qualquer acesso fora da lista liberada pela empresa.

Gráfico 3 - Computadores com restrições para acessar a Internet.

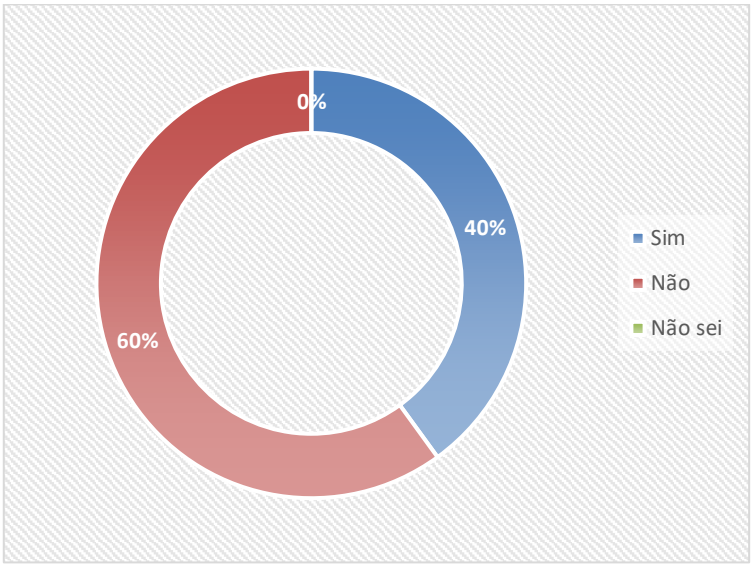


Fonte: Autoria própria (2024)

E no Gráfico 4, observa-se, como apontado no Gráfico 3, que as normas de segurança não são seguidas corretamente pelas empresas. 60% não utilizam restrições aos computadores,

com o cadastro de usuário e senha; os computadores são deixados expostos, arriscando serem acessados por um usuário mal-intencionado, o que pode levar a empresa a ter sérios prejuízos, com perda ou vazamento de dados. 40% têm o acesso aos computadores gerenciado com usuário e senha, desta forma, o controle de acesso das máquinas é mantido.

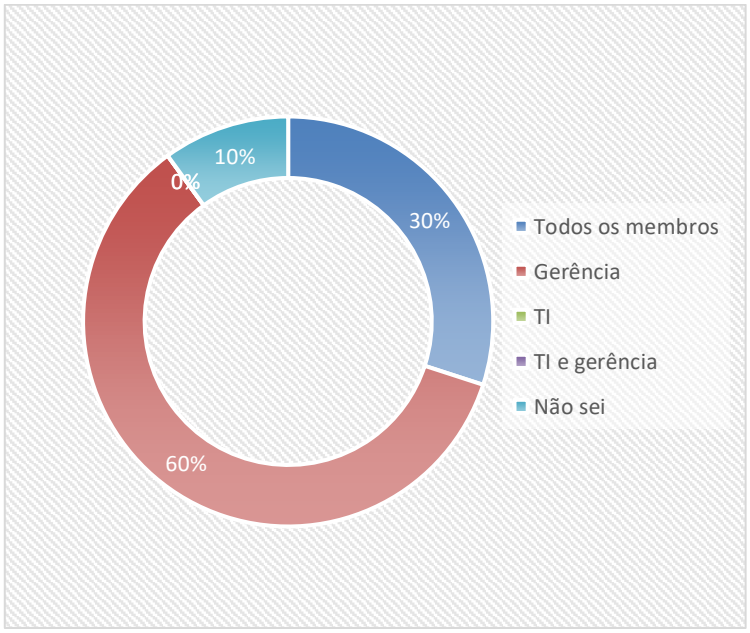
Gráfico 4 - Restrições para acessar computadores.



Fonte: Autoria própria (2024)

Analisando o Gráfico 5, observa-se que o cuidado com as restrições de acesso foi demonstrado pela maioria dos respondentes. Cerca de 60% dos acessos ao servidor são destinados à gerência. No entanto, ainda há uma parcela que requer atenção: 30% têm acesso livre concedido a todos os membros, e 10% não sabem exatamente quem está sendo acessado.

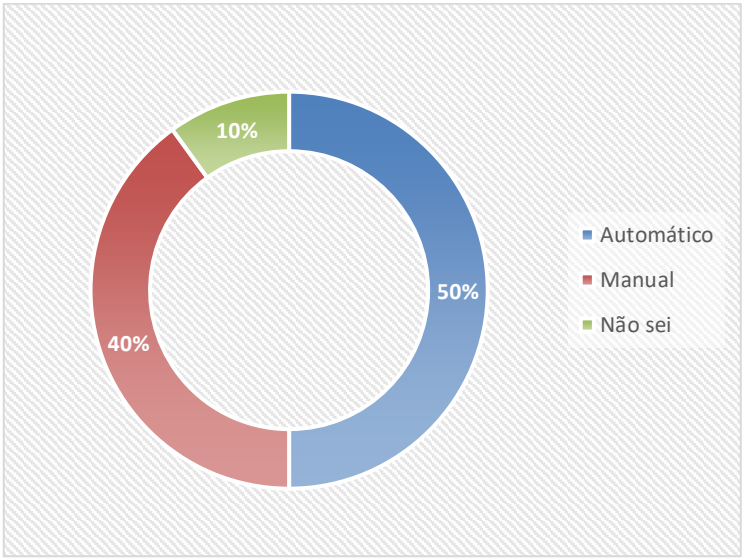
Gráfico 5 - Restrições para acessar o servidor.



Fonte: Autoria própria (2024)

O backup automático refere-se à prática de salvar dados na nuvem, programando o sistema para guardar os arquivos sempre que houver alguma alteração ou manipulação executada pelo usuário. Cerca de 50% dos usuários optam pelo modo automático, utilizando serviços em nuvem. No entanto, 40% ainda realizam *backups* manualmente, o que não é recomendado, seja usando pendrives, DVDs ou o próprio disco rígido onde o sistema operacional está instalado. Surpreendentemente, 10% dos entrevistados não souberam informar qual método utilizam.

Gráfico 6 - Forma de backup.



Fonte: Autoria própria (2024)

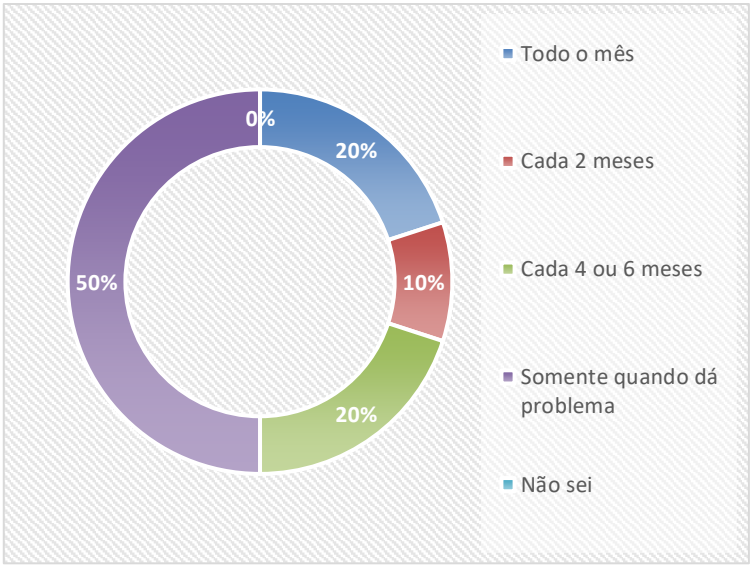
No Gráfico 7, é mostrada a realidade das empresas na questão da segurança física, onde, na maioria das vezes, os chamados para o suporte são abertos somente quando os equipamentos estão quase sem solução. Quando se trata da manutenção periódica, têm-se as seguintes abordagens:

- Cerca de 50% dos usuários esperam até que o equipamento apresente problemas para, então, entrar em contato com o suporte técnico e realizar a manutenção.
- Uma parcela de 20% estabelece uma abordagem pontual, realizando a manutenção dos equipamentos todos os meses.
- Outros 20% preferem uma manutenção periódica em intervalos de 2 ou 6 meses.
- E, por fim, 10% mantêm uma rotina de manutenção a cada 2 meses.

Nos atendimentos feitos pelo suporte técnico, é notório o quanto a informação sobre os problemas acarretados pela falta de manutenção nos equipamentos não é possuída pela maioria

das empresas e, sem saber os riscos, o funcionamento do setor de informática da empresa acaba sendo negligenciado. Essa falta de atenção pode resultar em consequências indesejadas.

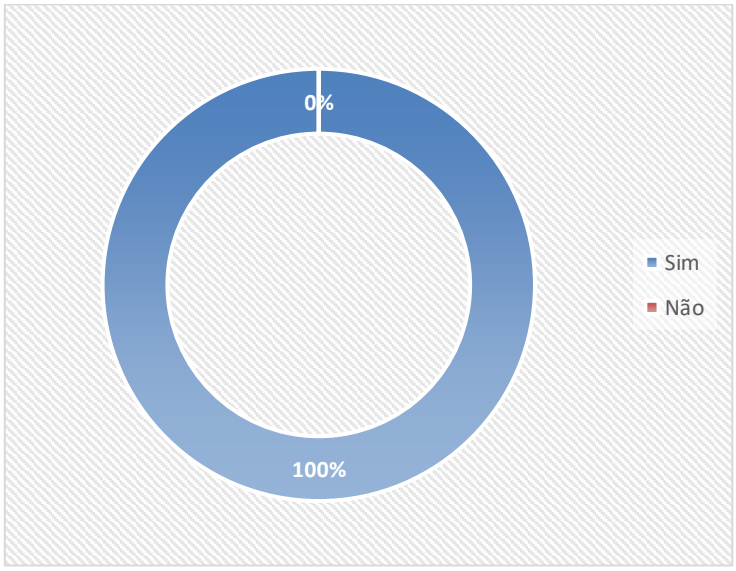
Gráfico 7 - Período de manutenção.



Fonte: Autoria própria (2024)

O Gráfico 8, sobre a cartilha da segurança da informação, obteve ótima aceitação, 100% acharam que é uma ferramenta essencial para boas práticas da segurança empresarial, ajudando a manter os funcionários atentos sobre os perigos cibernéticos. Muito satisfatório a aceitação desse trabalho, que servira para trabalhos futuros.

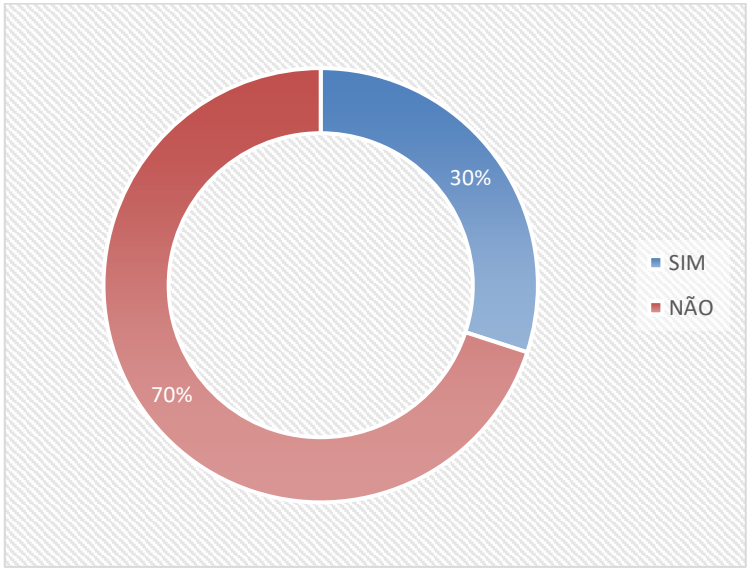
Gráfico 8 - Sobre a importância da cartilha.



Fonte: Autoria própria (2024)

O Gráfico 9, 70% relataram que não sofreram invasão de hackers ou vírus, 30% sofreram com vírus e invasão de hackers, que deixam danos e grandes prejuízos.

Gráfico 9 - Ataque Cibernético.



Fonte: Autoria própria (2024)

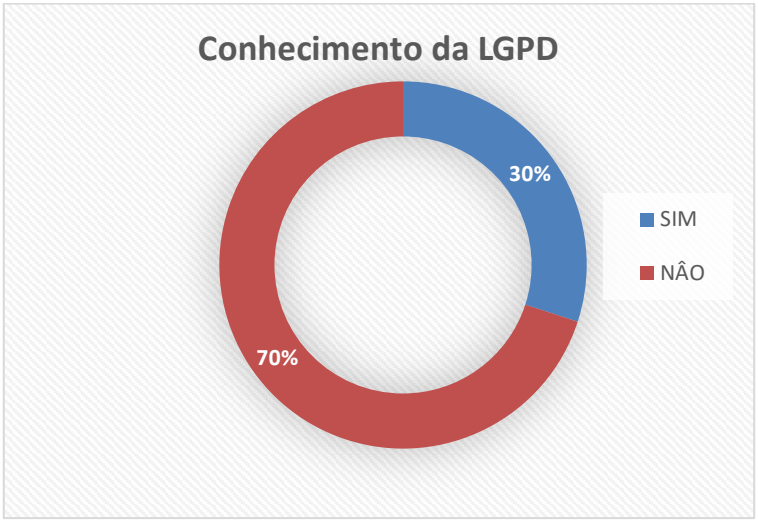
Na sequência as respostas dos usuários sobres experiência de ataque de Hackers:

- Dois clientes tiveram grandes prejuízos, quando o servidor da empresa deles tiveram os dados sequestrados, um deles perdeu o backup do dia e o outro teve um prejuízo maior, pois o backup não estava em dia, não usava a forma de salvar automático, perdeu quase todos os dados.

- Um informou que um dos computadores não estava funcionando na rede, pois o antivírus entrou em ação imediatamente quando o vírus se instalou e isolou o terminal infectado do ambiente de rede.

Na maioria das empresas visitadas e que responderam ao questionário, percebe-se que muitas delas não tinham noção da importância da LGPD (Lei Geral de Proteção de Dados). Essas empresas lidam diariamente com informações de clientes, seja em formato impresso ou digital. Portanto, seria fundamental que um controle rigoroso sobre os dados coletados fosse mantido. Infelizmente, a falta de conhecimento sobre a Lei de Proteção de Dados pode ser um obstáculo para garantir a segurança dessas informações. No Gráfico 10, 30% sabiam do que se tratava a lei, e 70% não tinham ideia sobre o assunto.

Gráfico 10 - Questionário LGPD.

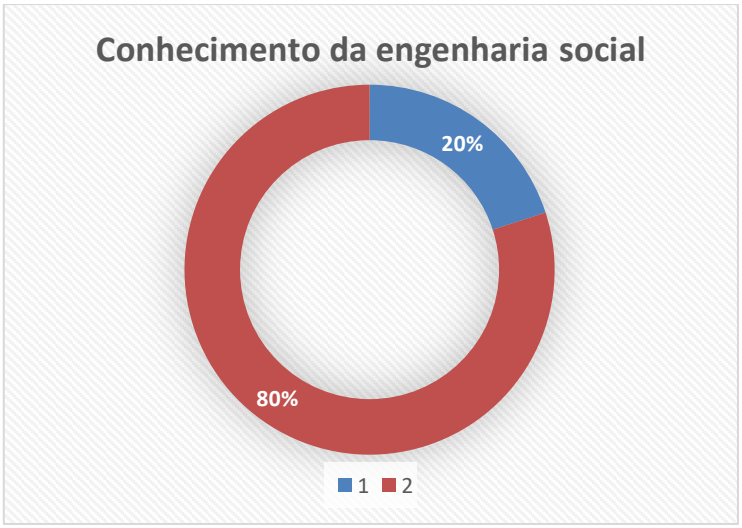


Fonte: Autoria própria (2024)

No Gráfico 11, resultado do levantamento, é verificado se as empresas estão se protegendo contra vazamento ou roubo de informações causados pela engenharia social e se têm noção do que se trata. Somente 20% são informados sobre engenharia social e 80% não tem conhecimento 0,

sobre o assunto.

Gráfico 11 - Questionário Engenharia social.



Fonte: Autoria própria (2024)

As empresas que responderam aos questionários possuem um grande volume de dados de clientes, incluindo documentos de licitação. Essa riqueza de informações torna-as um alvo perfeito para os engenheiros sociais.

Após responderem ao questionário, foram informados sobre as práticas dos criminosos e os riscos que a empresa enfrenta quando os dados não são devidamente protegidos. Todos ficaram surpresos, e muitos se questionaram se já haviam sido vítimas na empresa.

Após serem respondidos, foram informados sobre como agem os criminosos, os perigos que a empresa corre quando os dados não são protegidos. Todos ficaram surpresos, e vários tiveram dúvidas se já foram vítimas na empresa ou não.

Por fim, os principais resultados da pesquisa revelaram a criação de uma cartilha prática para a segurança da informação. O levantamento destacou que muitos funcionários têm nível superior, mas poucos têm formação na área de tecnologia. A maioria possui conhecimentos intermediários em informática, conseguindo realizar tarefas básicas, mas a segurança das empresas é insuficiente.

Cerca de 60% das empresas não adotam restrições de acesso à internet, o que expõe seus dados a riscos. Além disso, 60% não utilizam senhas para proteger computadores, facilitando o acesso não autorizado. Quanto ao acesso aos servidores, 30% liberam para todos os membros, o que é preocupante. A prática de backup automático é seguida por apenas 50%, e muitos ainda preferem métodos manuais.

Sobre a manutenção dos equipamentos, 50% dos usuários esperam até que algo quebre para chamar o suporte, o que pode causar problemas maiores. A cartilha foi considerada essencial para melhorar a segurança empresarial, com 100% de aceitação entre os respondentes.

Na questão de ataques cibernéticos, 30% relataram já ter sofrido invasões, resultando em perdas significativas. A falta de conhecimento sobre a LGPD e engenharia social também foi evidente, com 70% das empresas desconhecendo a lei e 80% sem informação sobre engenharia social.

Conclui-se que, apesar de algumas empresas terem consciência da importância da segurança da informação, muitas ainda carecem de conhecimento e práticas adequadas. A cartilha pode ser um passo importante para mudar essa realidade, mas é fundamental continuar a educação sobre segurança digital e proteção de dados.

6. TRABALHOS FUTUROS

O desenvolvimento deste estudo tornou-se factível através da necessidade de conhecimento dos suportes de TI acerca da temática. Os métodos utilizados mostraram-se satisfatórios para a concepção da ferramenta de conscientização da segurança da informação.

A cartilha de conscientização será submetida posteriormente à validação e atualizações de seu conteúdo por profissionais especialistas no assunto. O propósito dessa iniciativa é torná-la aplicável em vários contextos dentro da área de tecnologia da informação. Isso contribuirá para fortalecer continuamente a segurança nas empresas e aumentar o conhecimento dos funcionários, protegendo-os contra golpes futuros e garantindo a eficiência dos equipamentos.

Futuramente, poderão servir como fonte de pesquisas para projetos como este, que possam ser elaborados.

REFERÊNCIAS

ALBRIGHTON, Tom. The abc of copywriting. **Norwich: ABC Business Communications Ltd**, 2013.

AMARO, Mariana. **Golpes de engenharia social cresceram em 2021**. 2021. Disponível em: <https://www.infomoney.com.br/minhas-financas/golpes-de-engenharia-social-cresceram-saiba-o-que-sao-e-como-proteger-seu-dinheiro/>. Acesso em: 8 mar. de 2023.

BATISTA, Felippe Limongi. **Métodos e práticas utilizadas em engenharia social com o intuito de obstar o roubo de informações sensíveis.** Projeto apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como uma das atividades do programa de Metodologia Cientifica do curso de Pós Graduação Lato Sensu na área de Redes de Computadores com Ênfase em Segurança. Brasília (DF) 2015.

BRASIL, Ministério da Justiça. **ANPD publica regulamento de aplicação de sanções administrativas:** Resolução da ANPD que permite à Autoridade aplicar punições por descumprimento à Lei Geral de Proteção de Dados (LGPD). [*S.I*]: Ministério da Justiça e Segurança Pública, 27 de fev. 2023. Atualizado 28 de fev. 2023. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria >. Acesso em 8 de ago. 2024.

CAVALCANTI, Leo. **Segurança da informação e Compliance.** 2021. Disponível em: < https://www.linkana.com/en/blog/seguranca-informacao-compliance/>. Acesso em: 14 mar. 2003.

DE SOUZA PEREIRA, Lucas Avanci; VICENTINE, Augusto Luciano; RIZO, Andre Castro. Impactos da engenharia social na segurança da informação. **Revista Brasileira em Tecnologia da Informação**, v. 4, n. 1, p. 48-58, 2022.

DO VALE, Fábio et al. A SEGURANÇA DIGITAL NAS PEQUENAS E MÉDIAS EMPRESAS: DESAFIOS E POSSÍVEIS SOLUÇÕES. **Revista Latino-Americana de Estudos Científicos**, p. e38919-e38919, 2022.

GAT INFOSEC. **Gerenciamento da superfície de ataque**: Inventario exposto e risco de terceiros: identificar e gestão de ativos, riscos e vulnerabilidades cibernético. GAT INFOSEC, 2022. Disponível em: < https://www.gatinfosec.com/wp-content/uploads/2022/11/ebook-superficie-20221026.pdf > Acesso em 15 de ago. 2024.

HINTZBERGEN, Jule et al. **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. Brasport, 2018.

IBM. **O que é engenharia social?** 2023 Disponível em: < https://www.ibm.com/br-pt/topics/social-engineering >. Acesso em: 25 ago. 2024.

IBM. **O que é segurança cibernética?**. Disponível em: < https://www.ibm.com/br-pt/topics/cybersecurity >. Acesso em: 13 mai. 2023.

JAKKAL, Vasu. (2022). **Microsoft lança Defender for Business para ajudar a proteger pequenas e médias empresas**. Disponível em Microsoft: < https://news.microsoft.com/pt-br/microsoft-lanca-defender-for-business-para-ajudar-a-proteger-pequenas-e-medias-empresas/ >. Acesso em 12 de mar. de 2023.

KASPERSKY. **Engenharia social em destaque: dos truques clássicos às novas tendências,** 2023**.** Disponível em**:** < https://www.kaspersky.com.br/blog/social-engineering-tricks/21491/ > . Acesso em 24 de jul. 2024.

LUNARDI, Guilherme Lerch; DOLCI, Pietro Cunha; MAÇADA, Antônio Carlos Gastaud. Adoção de tecnologia de informação e seu impacto no desempenho organizacional: um estudo realizado com micro e pequenas empresas. **Revista de Administração**, v. 45, n. 1, p. 5-17, 2010.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. Brasília: [s. n.], 2015. 173 p. ISBN 978-85-920264-1-7.

MARCONDES, José Sérgio. **Segurança Física e Lógica da Informação: Diferença e Convergência.**[2017?]**.** Disponívelem: <https://gestaodesegurancaprivada.com.br/seguranca fisica-e-logica-nas-organizacoes/>. Acesso em: 14 mar.2023.

MASCARENHAS NETO, PEDRO TENÓRIO; ARAÚJO, WAGNER JUNQUEIRA. **SEGURANÇA DA INFORMAÇÃO Uma visão sistêmica para implantação em organizações**. João Pessoa: EDITORA DA UFPB, 2019. 160 p.

MICROSOFT. **Definição de InfoSec (segurança da informação)**. Disponível em: < https://www.microsoft.com/pt-br/security/business/security-101/what-is-information security-infosec>. Acesso em: 13 mar. 2023.

MIRABILI JUNIOR, Renato. **Conheça os Pilares da Segurança da Informação** - Protiviti. 21 ago. 2023. Disponível em: https://www.protiviti.com.br/cybersecurity/pilares-seguranca-da-informacao/. Acesso em: 12 jul. 2024.

MITNICK, Kevin D. Simon, William L. **Mitnick–A Arte de Enganar–Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education**, 2003.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Cláudia Fernandes; ESCRIVÃO FILHO, Edmundo. A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa. **JISTEM-Journal of Information Systems and Technology Management**, v. 1, p. 27-43, 2004.

MPSP, Ministério Publico. Cartilha ENGENHARIA SOCIAL: saiba como identificar possíveis armadilhas e se proteger de golpes. São Paulo: Ministério Publico, 2017. Cartilha. Disponível em:<https://www.mpsp.mp.br/documents/20122/1280138/cartilhaengenhariasocial.pdf/d0599369-8ca8-a5b2-469e-6b78c9232068?t=1662672945005&download=true>. Acesso em: 10 de ago. 2024.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. Novatec Editora, 2007.

NARDELLI, Cleber. Segurança da Informação e LGPD Aplicado no Desenvolvimento de Software. In: **Anais da V Escola Regional de Engenharia de Software**. SBC, 2021. p. 169-178.

NEVES, Denise Lemes Fernandes; et al. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber** - v.13 - p. 186-198 - 2021.

OAB, Jornal Da Advocacia. **LGPD| Sanções administrativas por descumprimento da lei: como agir para evitar?**, São Paulo: OAB (Ordem dos Advogados do Brasil), 24 de ago.2023.<https://jornaldaadvocacia.oabsp.org.br/noticias/lgpd-sancoes-administrativas-por-descumprimento-da-lei-como-agir-para-evitar/ >. Acesso em 19 de ago. 2024.

PEIXOTO, **A. S. Lei de Proteção de Dados**: entenda em 13 pontos! Politize, 2020. DemocraciaDigital. Disponívelem: <https://www.politize.com.br/lei-de-protecao-de-dados/#:~:text=A%20LGPD%20complementa%20o%20escopo,da%20seguran%C3%A7a%20das%20informa%C3%A7%C3%B5es%20pessoais >. Acesso em: 03 de mar. 2023.

PIOVESAN, Leonardo Gubert et al. ENGENHARIA SOCIAL: Uma abordagem sobre Phishing. **Revista Científica Faculdade de balsas**. v. 10, n. 1, p. 45-49, 2019.

RAMOS, Elias et al. Orientações para implementação do Sistema de Gestão de Segurança da Informação com base na ISO 27001 e o Ciclo PDCA. In: **FatecSeg-Congresso de Segurança da Informação**. 2021.

RAPÔSO, Cláudio Filipe Lima et al. LGPD-Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação: Revisão Sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58-67, 2019.

Seacord, Robert C., and Allen Householder. "**A structured approach to classifying security vulnerabilities.**" (2005).

SÊMOLA, Marcos. **Gestão da Segurança da Informação Uma Visão Executiva.** 2. ed. São Paulo: Campus, 2014. 171 p. ISBN 978-85-352-7178-2.

TCU. Tribunal de Contas da União. Boas práticas em segurança da informação / Tribunal de Contas da União. - 4. ed. - Brasília : **TCU, Secretaria de Fiscalização de Tecnologia da Informação**, 2012. 103 p.

APÊNDICE A – QUESTIONÁRIO SUPORTE DE TI

Universidade Federal Rural do Semi-árido – **UFERSA**
Departamento de Ciências Exatas e Tecnologia da Informação – **DCETI**
Bacharelado em Sistemas de Informação – **BSI**
Trabalho de Conclusão de Curso – **TCC**
Noilton Wilson e Francisco de Assis

Delineamento do Perfil do Usuário

SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE PEQUENO E MÉDIO PORTE NA CIDADE DE ASSÚ-RN: VULNERABILIDADES FÍSICAS E LÓGICAS

Obs.: Marque apenas 1 alternativa em cada item.

1 - Seu grau de instrução:
- O Ensino Médio Incompleto
- O Ensino Médio Completo
- O Superior Incompleto
- O Superior Completo
- O Pós-graduação Incompleta
- O Pós-graduação Completa

2 - Você é do sexo:
- O Masculino
- O Feminino

3 - Você pertence à faixa etária de:
- O Menos de 18 anos
- O 18-23 anos
- O 24-29 anos
- O 30 -35 anos
- O Acima de 35 anos

4 - Qual o seu nível de conhecimento em Informática?
- O Básico
- O Intermediário
- O Avançado
- O Não sei

5 - Os computadores da empresa têm restrições para acessar a Internet?
- O Sim
- O Não
- O Não sei

6 - Cada funcionário tem usuário e senha para acessar os computadores?
- O Sim
- O Não
- O Não sei

7 - Quem tem acesso ao servidor?
- O Todos os membros
- O Gerência

- O TI
- O TI e Gerência
- O Não sei

8 - **Existe um *backup* periódico e que funciona?**

- O Automático
- O Manual
- O Não sei

9 - **Qual a periodicidade de manutenção de equipamentos?**

- O Todo mês
- O Cada 2 meses
- O Cada 4 ou 6 meses
- O Somente quando dá problema
- O Não sei

10 - **Uma cartilha e palestra de conscientização da segurança da informação ajudaria os funcionários a terem consciência dos danos que as ações dele podem causar à organização e ajudar na prevenção contra ameaças?**

- O Sim
- O Não

11 - **A empresa sofreu com invasão de Hackers ou de vírus? Em caso afirmativo, quais os danos?**

12 - **Tem conhecimento sobre a LGPD (Lei Geral de Proteção de Dados)?**

- O Sim
- O Não

13 - **Sabe o que é ataques da Engenharia Social?**

APÊNDICE B – TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Universidade Federal Rural do Semi-árido - **UFERSA**
Departamento de Ciências Exatas e Tecnologia da Informação - **DCETI**
Bacharelado em Sistemas de informação - **BSI**
Trabalho de Conclusão de Curso - **TCC**
Noilton Wilson e Francisco de Assis

Termo de Consentimento Livre e Esclarecido

SEGURANÇA DA INFORMAÇÃO EM EMPRESAS DE PEQUENO E MÉDIO PORTE NA CIDADE DE ASSÚ-RN: VULNERABILIDADES FÍSICAS E LÓGICAS

Convido cordialmente a sra (sr.) a participar do processo de consentimento para utilização dos dados. O objetivo deste convite é obter seu consentimento informado e esclarecido para a criação de uma cartilha da segurança da informação para conscientizar as empresas de pequeno e médio porte da cidade de Assu-RN, na importância de manutenção e segurança dos seus dados, visando em manter a integridade de equipamentos e sistemas. Solicito que leia atentamente o termo de consentimento anexo e, caso concorde, preencha, assine e retorne-o. Agradeço antecipadamente pela sua participação e contribuição para o desenvolvimento deste TCC. Estou à disposição para esclarecer quaisquer dúvidas adicionais.

Eu, Simone Emanuelle R. de S. Silva concedo meu consentimento para a utilização de informações do ambiente fisico e lógico da empresa com o objetivo de criar uma cartilha de boas práticas da segurança fisicas e lógicas da empresa ao estudo intitulado "Segurança da informação em empresas de pequeno e médio porte na cidade de Assu-RN: vulnerabilidades físicas e lógicas.". Declaro que obtive todas as informações necessárias, bem como todos os eventuais esclarecimentos quanto às dúvidas por mim apresentadas.

Este termo tem o propósito de estabelecer o consentimento informado e esclarecido sobre a coleta, armazenamento e uso dos meus dados para a finalidade mencionada acima.

Estou ciente que:

I) Dados Coletados: Os dados coletados incluíram informações sobre a qualidade de suporte técnico, níveis de conhecimento de informática dos usuários, histórico manutenção de equipamentos, sistemas e informações de backup.

II) Propósito da Utilização: Os dados coletados serão utilizados exclusivamente para criar uma cartilha que fornecerá informações para manter a integridade da empresa. A cartilha terá o objetivo de conscientizar a importância na regularidade de manutenção dos equipamentos, sistemas e dados, e outras atividades relacionadas à melhoria da operações da empresa.

III) Retenção dos Dados: Os dados serão retidos pelo período necessário para atingir a finalidade mencionada acima, a menos que eu solicite sua exclusão antecipada por escrito. Após o término do período de retenção, os dados serão devidamente descartados de forma segura.

IV) Concordo que meu nome e assinatura estejam presentes no trabalho de conclusão de curso submetida à UFERSA (Universidade Federal Rural Semi-Árido), como prova da minha participação do estudo.

Angicos, 28 de Setembro de 2023.

Nome: Simone Emanuelle R. de Souza Silveira

CPF: 059.600.444-39

Telefone: 84-99620-0187

gov.br Documento assinado digitalmente
FRANCISCO DE ASSIS PEREIRA VASCONCELOS
Data: 04/10/2023 10:57:09-0300
Verifique em https://validar.iti.gov.br

Responsável pelo projeto: Francisco de Assis Pereira Vasconcelos de Arruda (Orientador)

Em caso de dúvidas com respeito deste estudo, poderei consultar:

Pesquisador principal: Noilton Wilson da Silva

Orientador: Francisco de Assis Pereira Vasconcelos de Arruda

Contatos: 85 9 9834-1212 | noilton.silva@alunos.ufersa.edu.br | xico@ufersa.edu.br

ANEXO A – CONTROLE DO SUPORTE

Prontuário de Manutenção

Nome da empresa
Av. Senador João Câmara
Assu - RN
Código postal

Fone: 0000 0000
nomedaempresa@email.com

Técnico (a)	Tipo de manutenção	Descrição do serviço	Data / Hora
Nome do Técnico	Corretiva	Substituição de peça	DD/MM/AAAA
Nome do Técnico	Inspeção	Verificação de segurança	DD/MM/AAAA
Nome do Técnico	Preventiva	Limpeza geral	DD/MM/AAAA

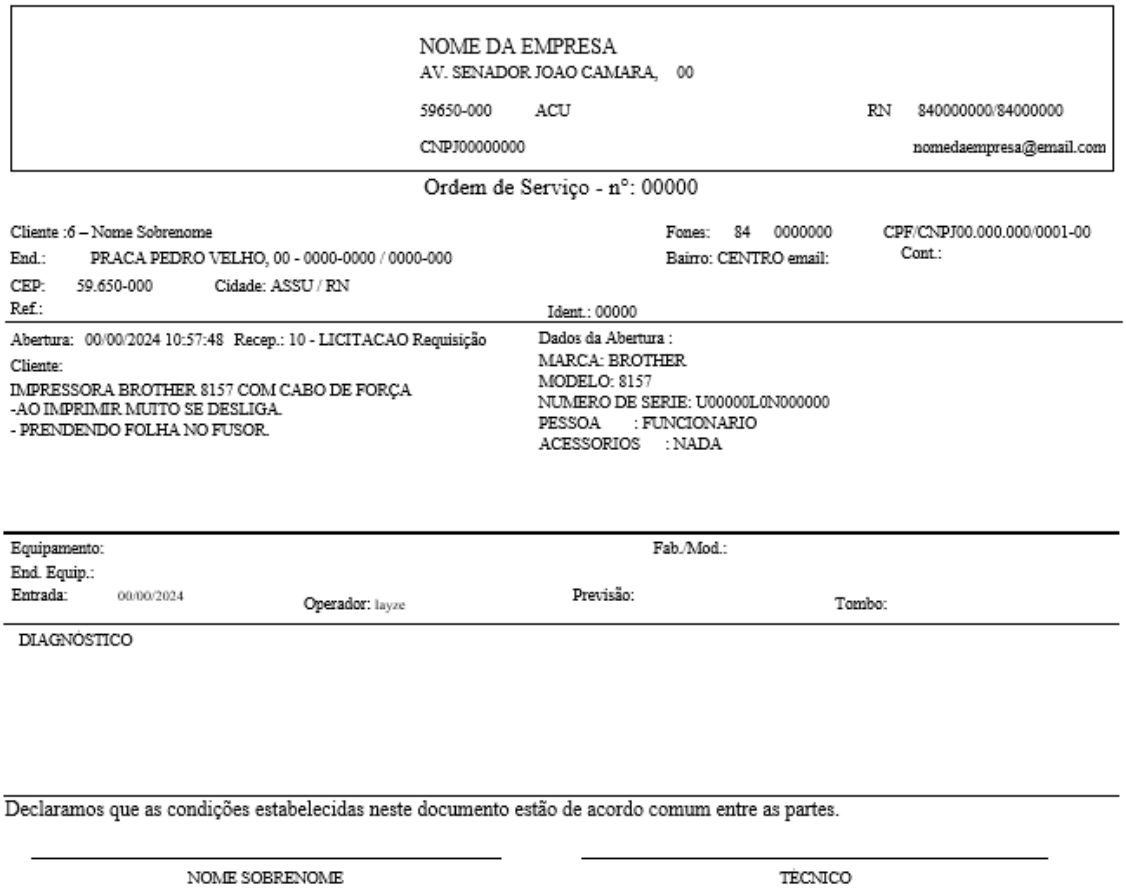
Manutenção Preventiva
☐ Mensal ☐ Trimestral

☐ Limpeza de componentes
☐ Teste de funcionamento
☐ Outros:

Observações:

Fonte: Autoria própria (2024)

ANEXO B – ORDEM DE SERVIÇO



NOME DA EMPRESA
AV. SENADOR JOAO CAMARA, 00
59650-000 ACU RN 840000000/84000000
CNPJ00000000 nomedaempresa@email.com

Ordem de Serviço - n°: 00000

Cliente :6 – Nome Sobrenome
End.: PRACA PEDRO VELHO, 00 - 0000-0000 / 0000-000
CEP: 59.650-000 Cidade: ASSU / RN
Ref.:
Fones: 84 0000000 CPF/CNPJ00.000.000/0001-00
Bairro: CENTRO email: Cont.:
Ident.: 00000

Abertura: 00/00/2024 10:57:48 Recep.: 10 - LICITACAO Requisição
Cliente:
IMPRESSORA BROTHER 8157 COM CABO DE FORÇA
-AO IMPRIMIR MUITO SE DESLIGA.
- PRENDENDO FOLHA NO FUSOR.

Dados da Abertura :
MARCA: BROTHER
MODELO: 8157
NUMERO DE SERIE: U00000L0N000000
PESSOA : FUNCIONARIO
ACESSORIOS : NADA

Equipamento:
Fab./Mod.:
End. Equip.:
Entrada: 00/00/2024
Operador: layze
Previsão:
Tombo:

DIAGNOSTICO

Declaramos que as condições estabelecidas neste documento estão de acordo comum entre as partes.

NOME SOBRENOME

TECNICO

Fonte: Autoria própria (2023)