Instituto Federal do Sertão Pernambucano (IFSERTÃOPE)

Campus Floresta (CFLO)

Graduação em Tecnologia da Informação (GTI)

Girlene Maria Pereira

Política de Segurança da Informação e Comunicação - PoSIC: Uma análise sobre a utilização das normas de segurança do IF Sertão-PE no Campus Floresta

Trabalho de Conclusão de Curso

Floresta-PE, dezembro de 2019.

Instituto Federal do Sertão Pernambucano (IFSERTÃOPE)

Campus Floresta (CFLO)

Graduação em Tecnologia da Informação (GTI)

Girlene Maria Pereira

Política de Segurança da Informação e Comunicação - PoSIC: Uma análise sobre a utilização das normas de segurança do IF Sertão-PE no Campus Floresta

Orientador: Jair Galvão de Araújo

Monografia apresentada ao Instituto Federal do Sertão Pernambucano, Campus Floresta, como parte dos requisitos para conclusão do curso de Gestão de Tecnologia da Informação.

Floresta-PE, dezembro de 2019.

Dados Internacionais de Catalogação na Publicação (CIP)

P436p Pereira, Girlene Maria
Política de segurança da informação e comunicação – PoSIC: uma análise sobre a utilização das normas . / Girlene Maria Pereira - Floresta, 2020.

42 f. il.

Orientador: Jair Galvão de Araújo
Trabalho de Conclusão de Curso – Tecnólogo em Gestão da Tecnologia da Informação Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta.

1. Tecnologia da informação. 2. Segurança da informação. 3. PoSIC.

I. Araújo, Jair Galvão de. II. Título.

CDD: 005.8

Elaborada pela bibliotecária Ednaene de Menezes CRB4/2133

Agradecimentos

Agradeço primeiramente a Deus, pelas oportunidades que Ele me deu, pela sabedoria e paciência, pois graças a Ele, eu cheguei até aqui. Sou grata, não só pela conquista da faculdade, mas por tudo, pois com ajuda de Deus, eu venci cada desafio que surgiu na minha vida e segui em frente de cabeça erguida, sabendo que tenho um Deus que cuida de mim.

Agradeço também a minha família que sempre me apoiou e acreditou em mim, em especial, aos meus pais Maria e Geraldo. Sempre me incentivaram e me apoiaram em cada momento que precisei. Aos meus irmãos Givanilson, Gildenilson, Gildevan e Gilsevânia.

Sou grata aos meus professores pelos ensinamentos, conselhos e desafios, pois cada um deles me ajudou a crescer cognitivamente, e me ajudou também a me superar a cada dia. Sou grata em especial ao meu orientador Jair Galvão, pela paciência, incentivo, compreensão e por todos os ensinamentos repassados.

Agradeço ao meu namorado Jelson pelo apoio dado quando precisei, tanto no decorrer da trajetória acadêmica, quanto na vida.

Sou grata também ao IF Sertão - Campus Floresta, pelas oportunidades que me deu, por cada momento de aprendizagem, pelos amigos que fiz na faculdade, pelas experiências que obtive durante minha graduação. Agradeço também a todas as pessoas que de forma direta ou indireta me apoiaram, me incentivaram e fizeram parte da minha formação acadêmica.

Muito obrigada!

Resumo

A Tecnologia da Informação trouxe grandes avanços para as organizações, uma vez que os recursos tecnológicos são essenciais, proporcionando mais facilidade e agilidade na transmissão, armazenamento e manipulação de informações. Dessa forma, uma Política de Segurança da Informação e Comunicação (PoSIC) é indispensável para o sucesso de uma organização. Entretanto, não adianta ter uma PoSIC se os funcionários da organização não cumprem, nem ao menos conhecerem suas diretrizes e normas para então poder cumprí-las.

Este trabalho busca fazer uma análise no Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - Campus Floresta, em relação a utilização das normas e diretrizes estabelecidas na PoSIC do IF Sertão-PE pelos servidores e comparar a PoSIC do IF Sertão-PE com as PoSICs do IFPE e IFPB buscando ter uma visão mais ampla do que comtepe a PoSIC do IF Sertão-PE com relação a outras PoSICs.

A metodologia usada para esta pesquisa, foi promover um questionário contendo 19 questões, elaboradas com base na PoSIC do IF Sertão. O questionário foi aplicado no período entre o dia 23/10/2019 ao dia 31/10/2019, o questionário foi respondido por 41 pessoas de um total de 92 servidores. Através dos resultados, foi possível perceber que aproximadamente 80% dos servidores entrevistados do Campus Floresta não conhecem as normas de segurança que foram estabelecidas na PoSIC.

Palavras-chave: Tecnologia da Informação, Segurança da Informação, PoSIC.

Abstract

Information Technology offers great advancements to organizations as essential technology resources make it easier and faster to transmit, store and manipulate information. Thus, an Information and Communication Security Policy (PoSIC) is indispensable for the success of an organization. However, there is no point in having a PoSIC if the employees of the organization do not comply, nor know their guidelines and norms to be able to meet them.

This paper seeks to make an analysis at the Federal Institute of Education, Science and Technology of Sertão Pernambucano - Campus Floresta, in relation to the use of the rules and rules applicable in the IF Sertão-PE PoSIC by the servers and comparisons in the IF Sertão-PoSIC. PE with as IFPE and IFPB PoSICs looking for a broader view than IF Sertão-PE PoSIC with respect to other PoSICs.

The methodology used for this research was promoted to a questionnaire containing 19 questions, elaborated based on IF Sertão's PoSIC. The questionnaire was applied between 10/23/2019 and 10/31/2019, the questionnaire was answered by 41 people from a total of 92 servers. Through the results, it was possible to realize that approximately 80 % of the servers interviewed in Campus Floresta do not know the security standards that were used in PoSIC.

Keywords: Information Technology, Information security, PoSIC.

Lista de Figuras

Lista de Tabelas

Sumário

1

Introdução

A Tecnologia da Informação(TI) é entendida como tudo que implica nos processos realizados por meios computacionais. Gobbo em 2013 [1] incluiu a TI nos processos de geração de conhecimento para as organização, além de incluir também o armazenamento e processamento de dados e informações na definição de TI.

A adoção da TI trouxe uma grande contribuição na execução das tarefas diárias nas organizações, pois, comparando o tempo que se levava para fazer os processos manuais com o tempo que se gasta nos processos computacionais, é notável a diferença de tempo. Azevedo (2015) [2]

A utilização de equipamentos tecnológicos abrangem toda a organização. É importante adotar políticas de segurança para que através das normas nela estabelecidas os funcionários saibam como fazer bom uso das ferramentas tecnológicas, como também, possam estar preparados para as situações de risco que podem ameaçar a segurança da informação da organização.

O Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IF Sertão-PE) possui uma política de segurança que é aplicada em todos os campi. Esse documento é conhecido como Política de Segurança da Informação e Comunicação (PoSIC).

Este trabalho tem como objetivo avaliar o conhecimento das normas e diretrizes de segurança e o uso dos equipamentos de Tecnologia da Informação no IF Sertão Campus Floresta pelos servidores e comparar a PoSIC do IF Sertão-PE com as PoSICs do IFPE e IFPB buscando ter uma visão mais ampla do que comtepe a PoSIC do IF Sertão-PE com relação a outras PoSICs.

1.1 Organização do trabalho

Além desse capítulo da introdução, este trabalho é constituído por outros quatro capítulos que estão descritos a seguir.

No Capítulo 2 são apresentados os conceitos e a importância da Tecnologia da Informação. O Capítulo 3 discorre sobre a metodologia utilizada no trabalho. No Capítulo 4 são apresentados os resultados obtidos por meio da pesquisa que foi realizada. No Capítulo 5 são apresentados a conclusão do trabalho e as propostas para trabalhos futuros.

2

Referencial Teórico

2.1 Tecnologia da Informação

Rios et.al. em 2017 [3] interpreta a informação como sendo algo de grande importância para toda e qualquer organização, independentemente do seu tamanho e do tipo de atividade que exerce. Segundo Paiva em 2017 [4] um dos principais ativos das organizações é a informação. Paiva [4] ainda define os ativo, como tudo aquilo que representa valor para organização.

Sendo assim, por meio dessa classificação, podemos ver a informação como algo essencial para as organizações.

A transmissão, o processamento e o armazenamento de informações se dá principalmente por meio da Tecnologia da Informação. A TI é de extrema importância para as organizações, a utilização de equipamentos tecnológicos fazem parte da rotina de trabalho, proporcionando auxílio e agilidade na execução das tarefas.

Para Gomes em 2019 [5] todo o processo de transmissão do conhecimento por meio da tecnologia no ambiente organizacional faz parte da TI, ou seja, o tratamento de dados e informações, o armazenamento, e as tecnologias que propagam as informações são consideradas como tecnologia da Informação. Munhoz em 2015, [6] define a Tecnologia da Informação de uma forma mais geral, como sendo um conjunto de procedimentos e respostas fornecidas por meios computacionais onde é possível armazenar, acessar, e também gerenciar as informações.

A TI auxilia nas mudanças nas organizacionais. As formas como a TI têm se expandido nas empresas mudou, consideravelmente, o modo como as organizações trabalham Gomes em 2019 [5]. Tal afirmação também é confirmada por Fenando em 2017 [7] quando diz que os recursos de TI possibilitam inúmeras transformações para uma organização, uma vez que através desses recursos é possível obter organização, armazenamento e gerenciamento de imensas quantidades de dados. Essas modificações envolvem tanto uma grande mudança na forma de administrar e impulsionar os negócios como também as coisas mais simples como a automatização de processos.

As ferramentas tecnológicas estão em todos os setores das organizações e isso trouxe avanços, mas também faz com que as informações estejam mais vulneráveis. Silva (2016) [8] diz que o elo mais fraco da segurança da informação nas empresas é o ser humano, pois, segundo Silva, as pessoas estão suscetíveis a disponibilizar informações a terceiros quando são atacados por meio da engenharia social, num momento em que a pessoa confia ingenuamente ou, de modo geral, somente desconhece ou desconsidera os padrões de segurança da organização. A engenharia social é a forma pela qual se consegue informações a respeito de algo através da persuasão. Silva em 2016 [8].

Sendo assim, entende-se que não é somente a ingenuidade das pessoas de modo geral que influenciam na fragilidade humana no que tange a Segurança da Informação (SI), pois, o desconhecimento de normas de segurança também podem comprometer a segurança da informação da empresa, é necessário o conhecimento e treinamentos dos funcionários para lidar com os recursos de TI dentro da organização sem comprometer a segurança por falta de conhecimento ou por ingenuidade.A melhor maneira de evitar que informações caiam em mãos erradas é conscientizando os funcionários da organização da importância da Segurança da Informação. Silva (2016) [8]

Para Silva em 2016 [8], investir em equipamentos tecnológicos e em ações de segurança sem um plano de conscientização pode ser perigoso para a organização, pois se o funcionário não está ciente dos riscos, das vulnerabilidades e das ameaças, tem grandes chances da segurança dessa organização ser comprometida. Segundo De Paula e Cordeiro em 2016 [9], empresas ainda possuem dificuldades ou desconhecem a importância da SI, fato este que se torna ainda mais debilitado em instituições públicas, por causa de obstáculos como interferência política e a cultura organizacional existente.

2.1.1 Tecnologia da Informação e Comunicação

A Tecnologia da Informação e Comunicação (TIC), vem a ser a área que faz uso de ferramentas tecnológicas cujo objetivo é simplificar a comunicação e a obtenção de um objetivo comum. Além de trazer benefícios para a produção industrial, a TIC, consegue também ser bastante proveitosa no aprimoramento dos métodos de comunicação e na renovação das pesquisas científicas. Castilho (2018) [10]

As TICs são o resultado da junção de três aspectos técnicos: a informática, as telecomunicações e as mídias eletrônicas. O papel principal das TICs desde a sua criação foi de facilitar a comunicação entre pessoas e também torná-la mais acessível, bem como poder solucionar também alguns problemas sem que seja necessário se deslocar até um determinado local naquele instante.

As TICs são vistas como sinônimo da TI. Entretanto, as TICs vão mais além, por consistir em todos os meios técnicos usados para tratar a informação e auxiliar na comunicação. Assim, podem ser definidas como uma soma de recursos tecnológicos incorporados mutuamente. Oliveira (2015) [11] Toda tecnologia torna possível a comunicação e a disseminação de informações, pode ser entendida como TIC.

2.1.2 Segurança da Informação

A "Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". ABNT ISO/IEC 17799: 2005 [12].

Entender o conceito de Segurança da Informação, é muito importante para as organizações, entretanto, se as pessoas não entenderem contra o quê a informação precisa ser

protegida, não adianta falar de segurança.

Paiva em 2017 [4], define ameaças como sendo acontecimentos ou ações que possivelmente tragam problemas para a organização. Existem vários tipos de ameaças que cercam as organizações, principalmente a parte tecnológica, podendo ser softwares maliciosos como vírus, exposição ou falta de cuidados com senhas anotando em papéis que podem ser facilmente encontrados, vazamento de informações importantes para a organização, acessos que não foram devidamente autorizados, proporcionando dados à organização.

Sendo assim, as organizações devem preparar-se para evitar possíveis ataques das ameaças que a cercam, conscientizando os funcionários sobre a importância da segurança da informação, falando dos riscos e o que fazer para evitá-los, buscando também se fazer cumprir os princípios da segurança da informação.

Paiva [4] ainda define os princípios básicos da segurança da informação, sendo que para ele a confidencialidade das informações é o princípio que busca garantir que pessoas que não foram devidamente autorizadas, não acessem determinadas informações. Enquanto o princípios da disponibilidade é garantir o acesso a determinadas informações a pessoas autorizadas sempre que precisar. A Integridade, tem por objetivo garantir que as informações que sejam acessadas ou enviadas por um meio de comunicação, quer seja de um empresa, quer seja de um indivíduo, irão permanecer inalteradas, mantendo a sua originalidade.

Por meio da utilização da internet tornou-se possível fazer a junção das muitas áreas que hoje existem no mundo dos negócios, no entanto, a utilização da internet contém certas vulnerabilidades que podem causar um efeito negativo dentro da organização quando os funcionários não estão preparados. Para que as empresas consigam entrar no mercado e consigam se destacar das demais, é necessário disponibilizar as suas informações, tanto internamente com os funcionário da organização e quanto externamente. Mas, nem sempre esse processo se dá de maneira correta, e quando isso acontece, as informações disponibilizadas tanto internamente quanto externamente, tornam-se frágeis a segurança, pois não cumpriu os princípios básicos da segurança da informação: disponibilidade, integridade e confidencialidade. Paiva(2017) [4]

2.1.3 Ameaças e Vulnerabilidades

Segundo a NBR ISO/IEC 27002:2013 [13], ameaças à segurança da informação podem ser consideradas como tudo aquilo que pode causar danos as informações da organização, desde causas naturais como incêndios e inundações, até problemas causados por pessoas como espionagem, burlagem, fraudes e vandalismos. Para Costa (2019) [14], as ameaças à segurança da informação não causa danos somente a aos computadores ou as informações, mas pode prejudicar tanto a parte tecnológica quanto física e até mesmo prejudicar pessoas.

As principais ameaças causadas por pessoas são a inserção de *malwares* em computadores buscando danificar o computador ou as informações contidas nele. *Malwares* são softwares maliciosos criados com a intenção de causar danos ou qualquer outra atividade maliciosa a um computador [15] Ferreira em 2017. Cada *malwares* podem infectar o computador de formas diferentes.

Os códigos maliciosos podem infectar um computador são por meio de:

- Vírus – o vírus é um software malicioso que ao infectar um computador torna-se parte de um programa ou arquivo, gerando cópias de si mesmo quando o programa ou arquivo for executado. Seu principal meio de propagação são mídias removíveis, mas também pode pode ser encontrado em e-mails [16].
- Worms - é um código malicioso cuja função é semelhante ao vírus, mas ele é capaz de se multiplicar automaticamente sem necessitar ser executado pelo usuário. Além de ser independente de outros programas, os worms podem carregar consigo outros tipos de *malwares* como se fossem parte dele [17].
- Bot e Botnet - O Bot é um malware que é semelhante aos worms, porém, além de se propagar automaticamente, o Bot pode ser acessado pelo invasor remotamente. Assim, o invasor pode enviar comandos para o Bot, para que ele execute ações que causem danos ao computador. O Botnet é uma rede de computadores infectados com o Bot. Com uma rede de computadores controlada pelo invasor, ele potencializa seus resultados. Os computadores infectados com o Bot são chamados de zumbis [4].
- O Ransomware - é um código malicioso cuja função é invadir um sistema computacional e bloquear o sistema invadido para que o usuário não consiga ter acesso ao computador ou a determinados dados que estejam contidos nele. O invasor deter-

mina um valor para liberar o acesso ao sistema computacional, e quando a vítima para o valor, o acesso é concedido pelo invasor [18].

- Spyware - É um software de espionagem cujo objetivo é monitorar as atividades realizadas pelo usuário no sistema, enviando esses dados para a pessoa que irá monitorar tais atividades. O spyware pode ser encontrado em forma de keylogger (capta tudo que for digitado no teclado físico), screenlogger (registra a área onde foi clicado com o mouse) é adware (exibe propagandas escondendo um malware por trás) [16].
- Trojan Horse - É um código malicioso que aparece ao usuário em forma de "presente" onde o malware está oculto por trás de uma aplicação. Um exemplo são e-mails oferecendo coisas gratuitas para que o usuário clique e sem perceber instale a ameaça no computador. Cândido et. al. (2017) [19] O objetivo do trojan horse ou cavalo de tróia é ter controle sobre as informações do computador da vítima, ou também, controlar a máquina física remotamente. O trojan horse, além de ser baixado disfarçadamente, ele vem acompanhado por outros softwares maliciosos, os quais ajudam a disfarçar sua presença no computador da vítima e ajuda também a retornar ao computador invadido sem que a vítima saiba que está sendo atacada [16].
- Backdoor - É um software que permite manutenção de acesso e dá garantia de retorno ao sistema invadido, pois, ele deixa portas abertas permitindo que o invasor possa acessar remotamente e retornar ao sistema sem ser preciso fazer uma nova invasão [17].
- Rootkit - É um software utilizado para ocultar a presença do invasor no computador que foi comprometido. Este programa também pode vir junto de outro [17].

Segundo Gasparini (2018) [20], "uma vulnerabilidade é uma fraqueza que torna um alvo suscetível ao ataque". Os tipos de vulnerabilidades podem ser classificados da seguinte maneira: físicas, naturais, de hardware e software, comunicação, humana [4].

A vulnerabilidade física refere-se a área de TI da organização. Ele deve ser protegida tanto de acessos indevidos quanto de desastres naturais [4]. A vulnerabilidade natural está ligada aos desastres naturais, contra os quais as organizações devem se proteger o máximo possível [16]. As vulnerabilidades de hardware e software segundo Souza 2017,

são fragilidades em equipamentos de hardware ou softwares mal desenvolvidos facilitando assim a invasão de uma pessoa mal intencionada ao sistema computacional tendo acesso aos dados e informações contidas nesse sistema [16].

Comunicação - Trata-se das redes de comunicação que a empresa utiliza, mantendo controle dos computadores que estão ligados a rede para evitar possíveis invasões [4]. A vulnerabilidade humana está relacionada ao que uma pessoa pode causar de dano à organização, deixando ela mais suscetível a ataques ou exposições, sendo ou não de forma intencional [8].

2.2 Tecnologia da Informação nos Órgãos Públicos

A inserção de recursos tecnológicos na gestão pública ocasionou grandes mudanças no setor público, na economia global houve grandes mudanças, alterando também a maneira de se trabalhar no setor público, fazendo com que as empresas encontrem um novo jeito de trabalhar com eficiência e prestando serviços de qualidade. Souza (2013) [21]

A utilização de aparelhos tecnológicos nas organizações têm ajudado na execução das tarefas, na comunicação e nos processos. Azevedo em 2015 [2] tanto os os notebooks, quanto os tablets e, principalmente, os celulares estão entre os itens tecnológicos mais conhecidos e utilizados nos processos organizacionais.

A praticidade desses aparelhos tecnológicos e a grande capacidade de resolver inúmeras tarefas fazem com que aumente cada vez mais a utilização desses equipamentos nas organizações. Corroborando com este fato, Azevedo [2] afirma que: "Com o auxílio da Tecnologia da Informação, principalmente com a utilização da internet, é possível estar conectado (em tempo real) com quase tudo que acontece numa administração pública e além de suas fronteiras"

Diante disso, é perceptível a importância da tecnologia nas organizações públicas. A TI nos órgão públicos tem crescido a cada dia e isso faz com que aumente a agilidade na execução das tarefas, contudo, se não houver normas a serem seguidas e treinamentos adequados para os funcionários a informação fica mais vulnerável devido a falta de conhecimento das pessoas no que diz respeito a Segurança da Informação.

Apesar de toda essa revolução tecnológica ter cooperado para um bem comum à so-

ciedade principalmente influenciando em como as pessoas se relacionam e também na forma como se comunicam, as tecnologias presentes nas organizações têm sido um fator determinante para uma nova situação de ameaças, de forma a expor as pessoas a um novo conjunto de fraudes e em virtude disso, gerando perdas materiais ou morais.Teodoro em 2014 [22]. Assim, nota-se a importância de investir não só em tecnologia mas também na Segurança da Informação. Para Paiva em 2017 [4] Segurança da Informação "é a proteção de dados, informações, sistemas e demais ativos de uma organização". Sendo para ele ainda os ativos, tudo aquilo que representa valor para a organização. A Segurança da Informação não tem como objetivo proteger somente os ativos físicos e tecnológicos da organização, mas visa proteger também por onde a informação passa e onde é armazenada. Manduca em 2014 [23] afirma que a função da Segurança da Informação é proteger a informação e os sistemas de informação contra eventos que possam trazer riscos e acessos não autorizados.

Rios et. al. em 2017 [3] afirma que:

"As organizações públicas enfrentam o desafio de proteger suas informações, considerando que são ambientes onde há crescente complexidade, interconexões, incertezas e dependência da tecnologia, tendo ainda que realizar suas respectivas missões sem deixar de se submeter às normas e diretrizes provenientes dos órgãos centrais do governo. Contudo, é necessário que algumas medidas sejam tomadas para que tais informações sejam mantidas seguras e invioláveis".

Souza em 2013 [21], afirma que foi percebida pela administração pública a importância de promover aos funcionários públicos treinamentos para que assim, pudessem ter o domínio quanto a manuseio das tecnologias que vão surgindo a cada dia, de forma a adquirir as competências necessárias para a um melhor desenvolvimento quanto a prestação de serviços e também melhorar o seu conhecimento.

Nos dias de hoje, em uma organização pública o acesso às ferramentas de Tecnologia da Informação e Comunicação é essencial para seu funcionamento e seu melhor desempenho, todavia, é necessário que normas e diretrizes sejam estabelecidas para o uso adequado das Tecnologias da Informação.

2.3 Tecnologia da Informação no IF Sertão

O IF Sertão-PE preocupado o uso dos recursos tecnológicos criou uma Política de Segurança da Informação e Comunicação (PoSIC).

Para que o processo de segurança da informação pudesse ser criado, estabelecido e mantido, faz parte das boas práticas da segurança da informação que qualquer organização tenha sua PoSIC. Rios et. al. (2017) [3]

O Comitê de Gestão de Segurança da Informação (CGSI) [24] no capítulo I da PoSIC do IF Sertão, nos dá uma visão geral desta política onde diz que a PoSIC é um documento cujo objetivo é proporcionar diretrizes, normas e apoio administrativo.

Essa política dará o direcionamento necessário para que as organizações definam as regras, os procedimentos e os controles que serão implantados na proteção da informação. É neste documento, onde contém as normas e diretrizes que ensinam os servidores sobre como devem comportar-se diante da tecnologia da informação e comunicação que está presente no seu ambiente de trabalho.

A utilização da TIC tem aumentado muito nos últimos anos com a utilização de e-mails e mídias sociais, fazendo com que a afluência de dados e informações sejam mais intensos, mas ao mesmo tempo mais dinâmicos, de forma a facilitar o os métodos de tomada de decisão no que diz respeito aos gerentes e gestores da organização.Pinto e Rocha (2016) [25]

Dessa forma, é necessário que haja um controle, por isso, a PoSIC no capítulo II, no Art. 1 determina as normas, os direitos e também as condições principais para o uso do e-mail institucional no âmbito do IF SERTÃO-PE, no qual são mostradas definições importantes para que o documento fique mais fácil de ser compreendido. Nele também, são mostrados quais são as obrigações e cuidados que o usuário deve ter, como também mostra as penalidades.

Assim também, no capítulo III da PoSIC no Art. 1fala que esta regulamentação tem por objetivo "estabelecer responsabilidades e requisitos básicos de utilização da Internet no Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IF SERTÃO-PE".

Para Lyra em 2015 [26] pessoas representam uma forte influência no que diz respeito aos princípios da SI (confidencialidade, a integridade e a disponibilidade), pois, o usuá-

rio que não manter a sua da senha de modo confidencial por exemplo, evitando anotar em papéis, compartilhar com terceiros, ou não fazer uso de senhas seguras, podem estar comprometendo a segurança da informação. Por conseguinte, a um dos principais problemas que a SI deve zelar é da segurança em pessoas,pois, a colaboração dos usuários é primordial para o êxito da segurança.

Assim, CGSI aborda no capítulo IV da PoSIC no Art. 1 a respeito dos regulamentos para para que o servidor utilize a sua de estação de trabalho na rede corporativa do IF SERTÃO-PE.

A PoSIC do IF Sertão-PE, possui em seu capítulo V no Art. 1º as normas para a administração dos domínios, subdomínios, sítios e também os serviços eletrônicos na internet do IF Sertão-PE, que são gerenciados por este documento.

Backups podem ser definidos como cópias de segurança garantindo que se uma houver uma falha nos computadores, servidores ou demais equipamentos do usuário ou da organização, que seus dados não serão perdidos. Paiva (2017) [4].

No capítulo VI, art. 1º da PoSIC do IF Sertão-PE normas que regem a política de backup e restauração de dados corporativos armazenados que existem nos servidores de rede no parque tecnológico do IF SERTÃO-PE são estabelecidos.

Ainda há desafios existentes quanto a utilização das TICs nas escolas, porque ainda há aqueles que consideram que as tecnologias que já temos são a bastante para exercer um bom papel na educação. Outro desafio é que devemos aprender a utilizar as tecnologias que vão surgindo, e nem tudo vem com um "manual de instruções", o que faz com que a escola reflita quanto ao uso das TICs de forma coletiva, na medida que principal objetivo das TICS é o de fazer o ensino evoluir. Ramos (2012) [27]

Todos os campi do IF Sertão-PE possuem laboratórios de informática. E além disso, a PoSIC ainda regulamenta a utilização dos laboratórios de informática do IF Sertão-PE, dando orientações e as condições de uso, no art.1º do capítulo VII da PoSIC.

E por fim, o capítulo VIII da PoSIC, onde trata-se das normatizações do regimento interno da CGSI, o art. 1º fala que essa regulamentação tem por objetivo, determinar os aspectos de organização e de funcionamento do CGSI junto ao Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – IF SERTÃO-PE.

3

Metodologia

Neste trabalho foi realizada uma pesquisa sobre o nível do conhecimento que os servidores do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano Campus Floresta (IF Sertão-PE) têm a respeito da sua Política de Segurança da Informação e Comunicação (PoSIC) como também o cumprimento de suas normas.

Inicialmente, foi aplicado um questionário sobre o uso de Tecnologia da Informação no Campus Floresta por meio da internet, utilizando a ferramenta de criação de formulários (Google Formulários). O objetivo foi analisar se o que os servidores do Campus Floresta sabem das normas de uso definidas na PoSIC do IF Sertão-PE. O questionário foi elaborado com base nas normas e diretrizes estabelecidas na PoSIC do IF Sertão-PE.

No questionário aplicado, contém 19 perguntas que foram elaboradas sobre os seguintes tópicos: Conhecimento sobre Tecnologia da Informação, e-mail institucional e backup, os quais são abordados pela PoSIC do IF Sertão-PE.

A Tabela 3.1 mostra as perguntas aplicadas aos servidores do Campus Floresta.

Tabela 3.1: Perguntas e respostas aplicadas aos servidores quanto ao uso e normas das Tecnologias da Informação.

Perguntas	**Respostas**
1-Você sabe o que é tecnologia da informação?	Sim Não
2-Você conhece as políticas e normas de segurança do IF Sertão?	Sim Não
3-Você teve treinamento sobre as normas de uso de tecnologias da informação no IF Sertão?	Sim Não
4-Você já participou de algum programa de conscientização sobre segurança da informação no Instituto?	Sim Não
5-Você usa o e-mail institucional?	Sim Não
6-Você acessa o e-mail institucional pelo seu computador ou pelo computador da instituição?	Meu computador.O computador da Instituição.Não acesso o e-mail institucional.
7-Você já leu o termo de responsabilidade de uso do e-mail institucional?	Sim Não
8-Você sai do seu e-mail institucional ao deixar o campus?	Sim Não
9-Você usa caracteres especiais (% @ * ! ; : .) em suas senhas?	Sim Não
10-Você usa o e-mail institucional para uso pessoal?(exemplo: enviar e-mail para familiares ou amigos)	Sim Não
11- Você acessa redes sociais (Facebook, Instagram, etc) com o e-mail institucional?	Sim Não
12- Você faz compras em sites com o e-mail institucional?	Sim Não
13-Você recebe e-mails de remetente desconhecidos ou de conteúdo duvidoso	Sim Não
14-Ao receber e-mails de remetente desconhecido ou propagandas, você comunica ao setor de TI?	Nunca recebi Já recebi e informei Já recebi mas não informei
15-Você já necessitou que outra pessoa acessasse seu e-mail institucional por você?	Sim Não
16-Você sabe o que é um backup de arquivos?	Sim Não
17-Você faz backup de arquivos do trabalho?	Sim Não
18-Você faz backup no computador ou em outro repositório fora do computador?	No computador Outro repositório
19-Quais ferramentas você utiliza para fazer backup?	No computador da instituição. Google Drive. ICloud Drive. Dropbox. No meu computador pessoal. Não faço backup. Não tenho computador institucional. HD Externo. Nuvem. Outros.

Foi comparado a estrutura das normas e diretrizes da Política de Segurança da Informação e Comunicação do IF Sertão-PE com as PoSICs do Instituto Federal de Pernambuco (IFPE) e o Instituto Federal da Paraíba (IFPB).

A tabela 4.1 apresenta a comparação das normas e diretrizes das PoSICs.

4

Resultados

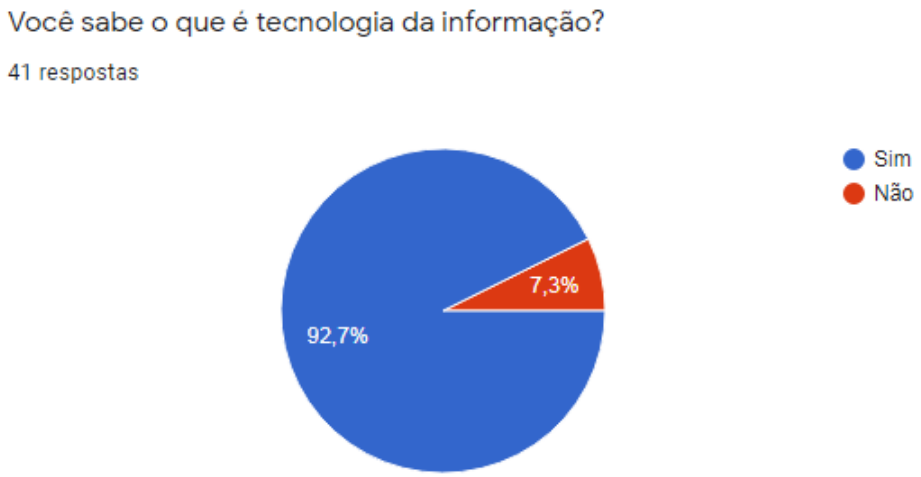
Nesta seção serão apresentados os resultados que foram obtidos por meio do questionário aplicado aos servidores do IF Sertão - Campus Floresta.

4.1 Resultado da pesquisa

A partir das respostas obtidas no questionário aplicado no Campus Floresta sobre o uso de Tecnologia da Informação, realizado no período entre o dia 23/10/2019 até o dia 31/10/2019, dos 92 servidores do campus Floresta, 41 responderam ao questionário.

A respeito do conhecimento que os servidores têm sobre Tecnologia da Informação, 92,7% responderam quem tem o conhecimento como mostra na figura 4.1.

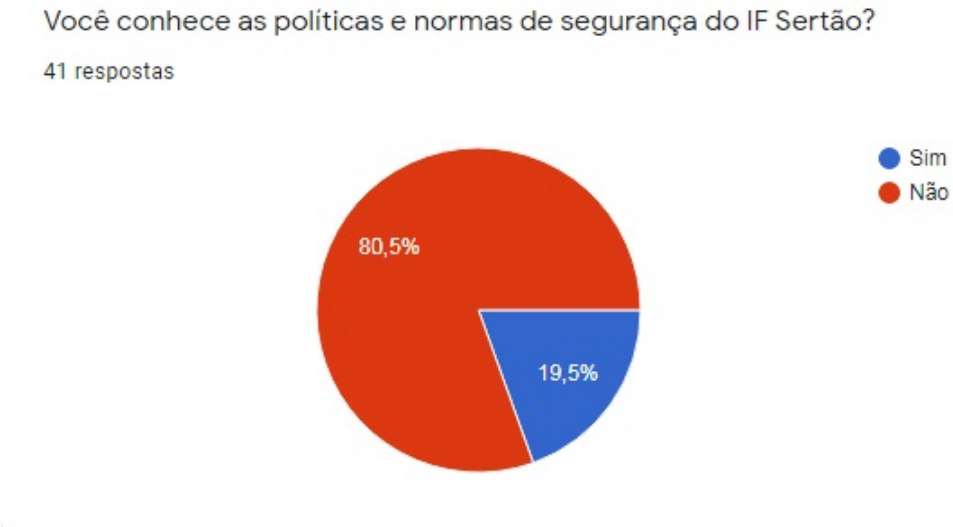
Figura 4.1: Quantitativo de respostas sobre o que é tecnologia da informação.



Fonte: Elaborado pela autora

Em relação ao conhecimento que os servidores têm sobre as normas de segurança do IF Sertão-PE, 80,5% das pessoas entrevistadas responderam que não conhecem as políticas e normas de segurança como mostra na figura 4.2

Figura 4.2: Quantitativo de respostas sobre o conhecimento acerca das políticas de segurança do IF Sertão-PE.



Fonte: Elaborado pela autora

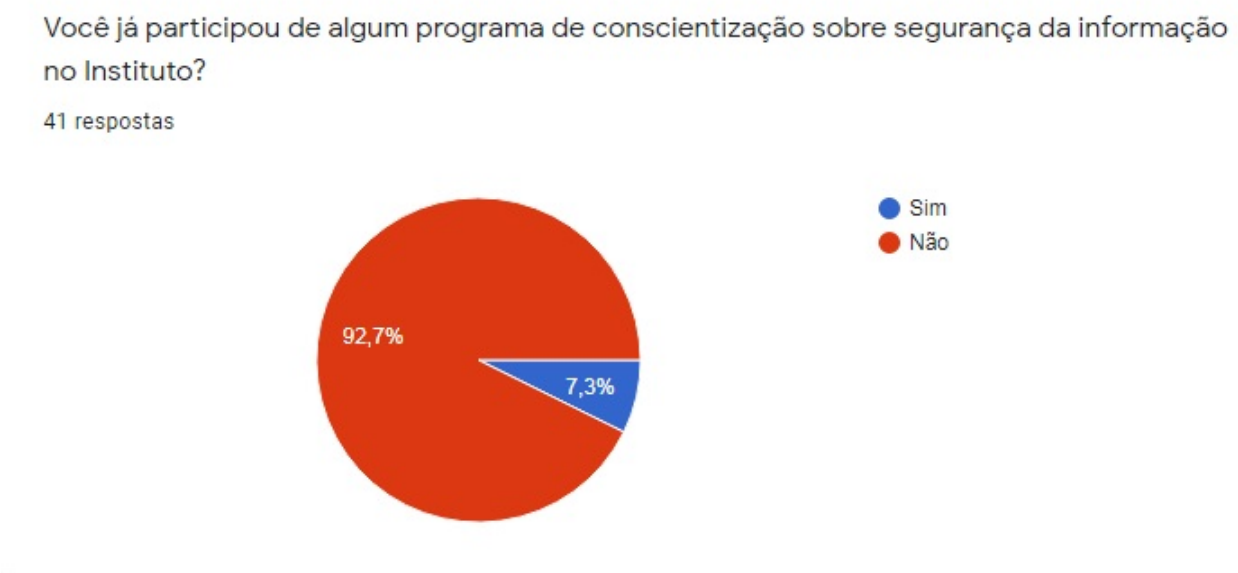
Quanto aos possíveis treinamentos sobre as normas de uso de tecnologias da informação no IF Sertão-PE, 97,6% responderam que nunca passaram por esse tipo de treinamento. A figura 4.3 mostra esse resultado.

Figura 4.3: Quantitativo de respostas sobre treinamentos a respeito das normas de uso da tecnologia da informação.

Fonte: Elaborado pela autora

Sobre a participação de algum programa de conscientização a respeito da segurança da informação no Instituto, 92,7% responderam que nunca participaram de nenhum programa de conscientização sobre segurança da informação. A figura 4.4 mostra esse resultado:

Figura 4.4: Quantitativo de respostas sobre a participação em programas de conscientização sobre Segurança da Informação no Instituto.

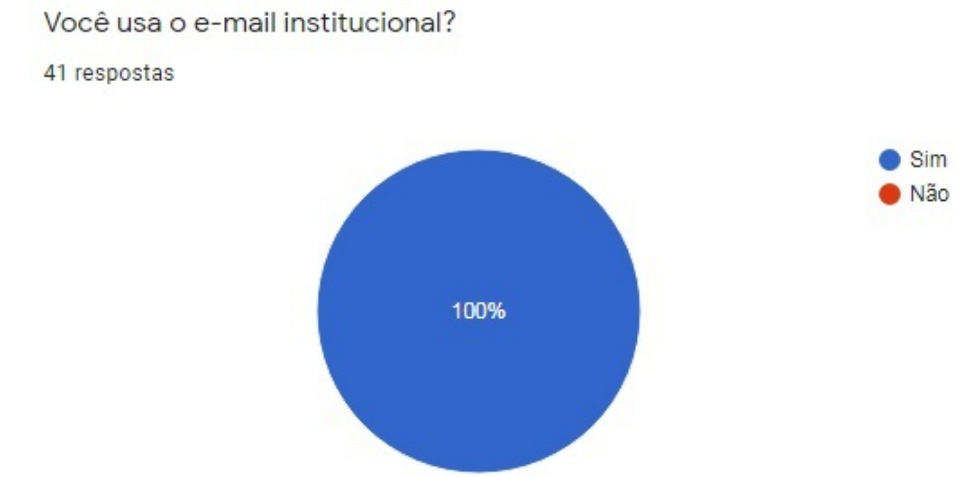


Fonte: Elaborado pela autora

A respeito da utilização do e-mail institucional, 100% dos entrevistados responderam

que fazem uso. É possível ver esse resultado na figura 4.5.

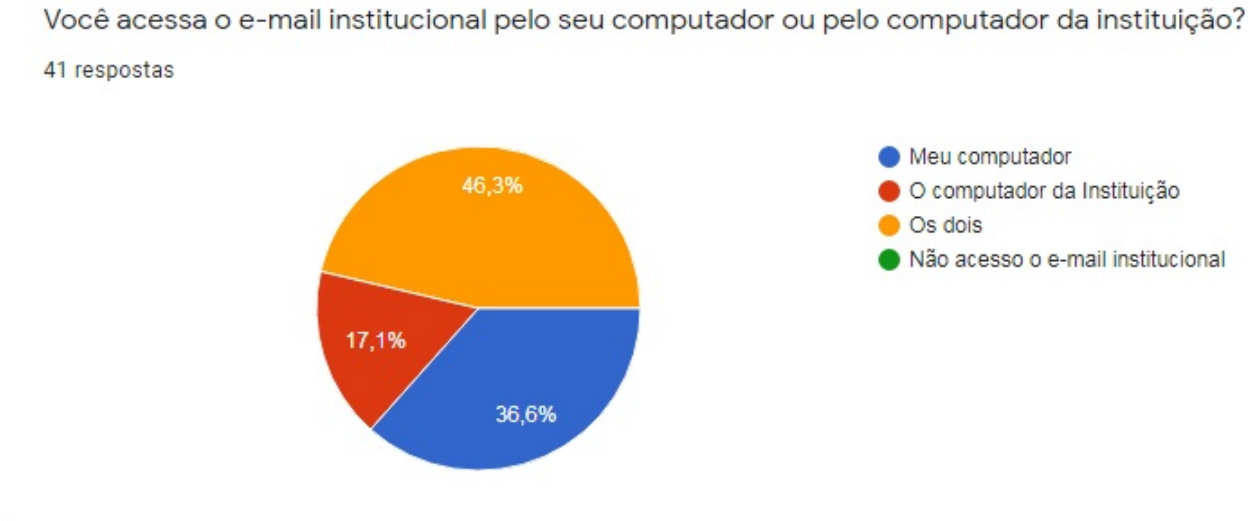
Figura 4.5: Quantitativo de respostas sobre a utilização do e-mail institucional.



Fonte: Elaborado pela autora

Com relação aos computadores onde é acessado o e-mail institucional pelos servidores. As respostas foram divididas, 43,3% das pessoas responderam que utilizam o e-mail institucional tanto em seu computador pessoal, quanto no computador da instituição. Já 17,1% das pessoas responderam que utilizam o e-mail institucional apenas no computador da instituição. Mais detalhes sobre esse resultado, é possível ver na figura 4.6.

Figura 4.6: Quantitativo de respostas sobre qual computador o servidor acessa o e-mail institucional.



Fonte: Elaborado pela autora

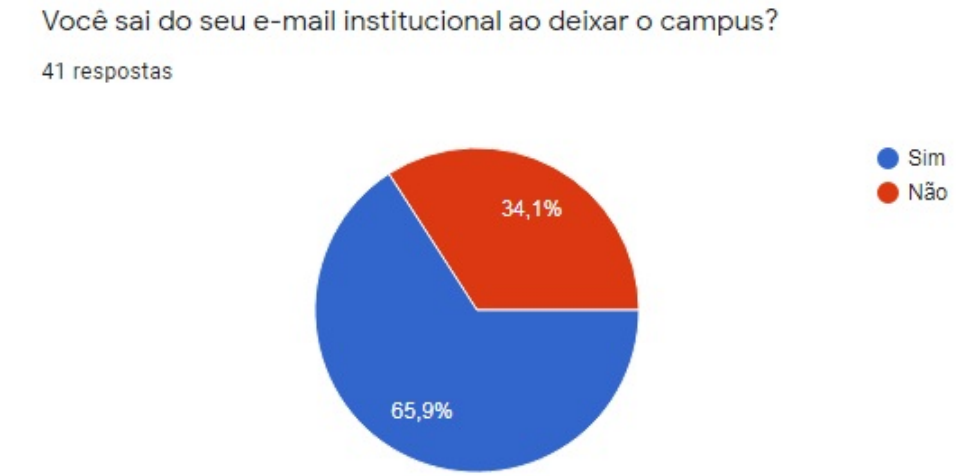
A cerca do termo de responsabilidade que é assinado por todos os servidores ao serem cadastrados no e-mail institucional, 61% das pessoas afirmaram ler o termo de responsabilidade antes de assinar. As respostas que indicam esse resultado estão na figura 4.7.

Figura 4.7: Quantitativo de respostas sobre o termo de responsabilidade de uso do e-mail institucional.

Fonte: Elaborado pela autora

Sobre os cuidados com a o e-mail institucional, perguntando se o usuário fecha o e-mail ao se ausentar do campus, 65,9% dos entrevistados responderam que sim. A figura 4.8 mostra esse resultado.

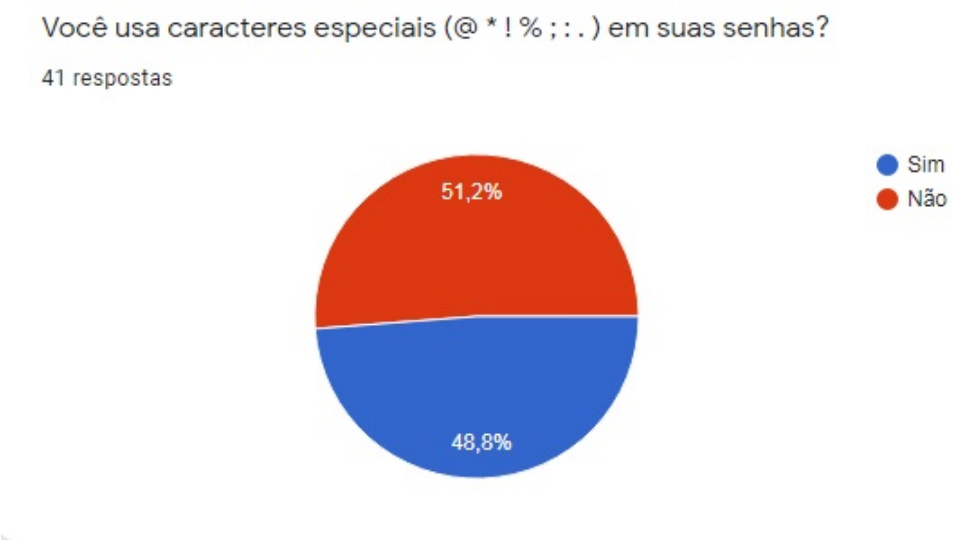
Figura 4.8: Quantitativo de respostas sobre logout do e-mail institucional ao deixar o campus.



Fonte: Elaborado pela autora

A respeito da segurança das senhas do e-mail institucional, quanto ao uso de caracteres especiais, 51,2% responderam que não utilizam caracteres especiais em suas senhas do e-mail institucional. Na figura 4.9 vemos esse resultado.

Figura 4.9: Quantitativo de respostas sobre a utilização de caracteres especiais nas senhas.



Fonte: Elaborado pela autora

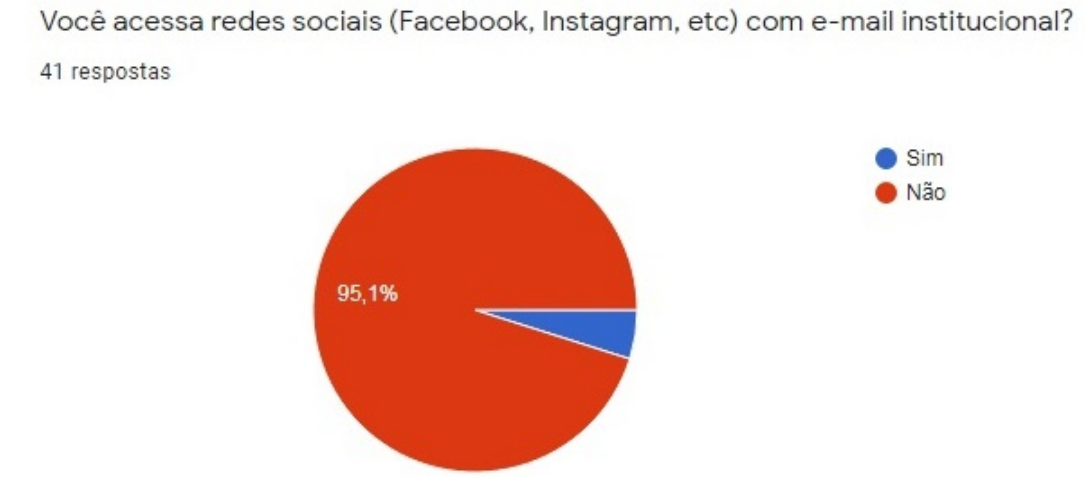
Referente ao uso do e-mail institucional para coisas pessoais, 100% das pessoas que responderam ao questionário, respondeu que não.A figura 4.10 mostra esse resultado.

Figura 4.10: Quantitativo de respostas sobre a utilização do e-mail institucional para uso pessoal.

Fonte: Elaborado pela autora

Sobre a utilização do e-mail institucional para acessar redes sociais na conta pessoal, 95,1% dos entrevistados responderam que não acessam redes sociais com o e-mail institucional. Figura 4.11

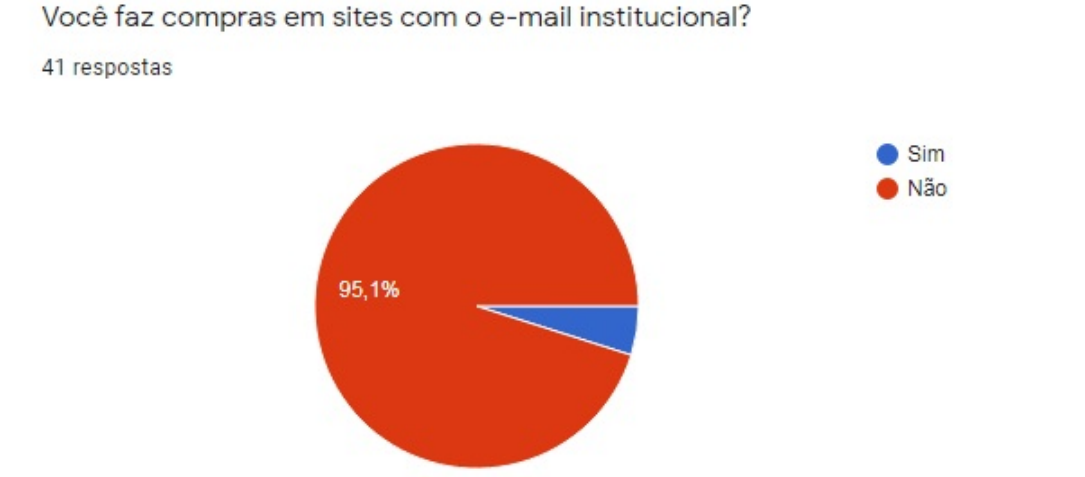
Figura 4.11: Quantitativo de respostas sobre o acesso às redes sociais com e-mail institucional



Fonte: Elaborado pela autora

A respeito de realizar compras em sites com o e-mail institucional, de acordo com as respostas 95,1% responderam que não fazem compras pela internet utilizando o e-mail institucional. Veja a figura 4.12

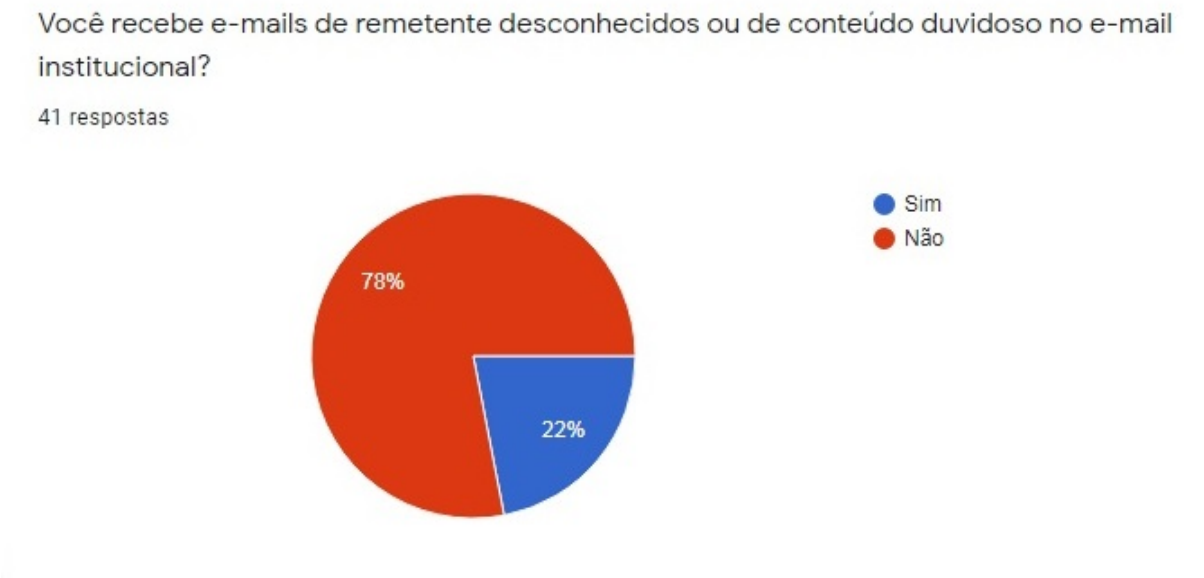
Figura 4.12: Quantitativo de respostas sobre compras em sites com o e-mail institucional.



Fonte: Elaborado pela autora

Sobre o recebimento de e-mails de remetente desconhecidos ou de conteúdo duvidoso no e-mail institucional, o gráfico a seguir mostra que 78% dos entrevistados nunca receberam esse tipo de e-mail na sua conta de e-mail institucional. Veja a figura 4.13 onde consta esse resultado.

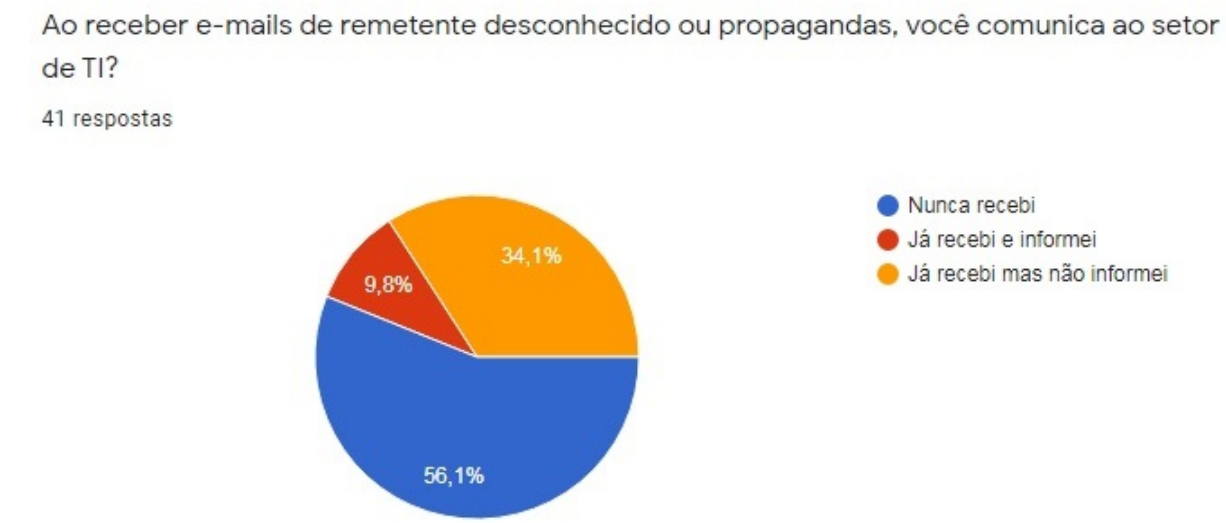
Figura 4.13: Quantitativo de respostas sobre o recebimento de e-mails de remetente ou conteúdo de caráter duvidoso.



Fonte: Elaborado pela autora

Sobre a comunicação ao setor responsável quando recebe e-mail desconhecido, 56,1% afirmou nunca receber esse tipo de e-mail, mas há também uma quantidade de pessoas que receberam, e 9,8% afirmaram não informaram ao setor responsável. Na figura 4.14 é possível ver mais detalhes desse resultado.

Figura 4.14: Quantitativo de respostas sobre informar ao setor de TI o recebimento de e-mails desconhecidos.



Fonte: Elaborado pela autora

A respeito do servidor necessitar que outra pessoa acessasse o seu e-mail institucional em seu lugar, 97,6% responderam que não. O resultado dessa resposta está na figura 4.15.

Figura 4.15: Quantitativo de respostas sobre a necessidade de disponibilizar o acesso ao e-mail institucional por terceiros.

Fonte: Elaborado pela autora

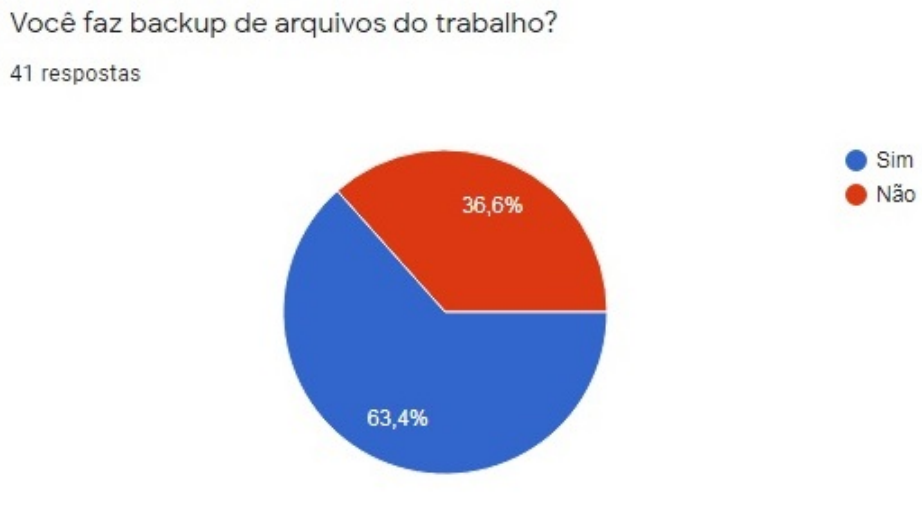
Com relação ao entrevistado saber o que é um backup de arquivos, 97,6% dos entrevistados responderam que sim. A figura 4.16 confirma esse resultado.

Figura 4.16: Quantitativo de respostas sobre o que é um backup de arquivos.

Fonte: Elaborado pela autora

Sobre o servidor fazer backup dos arquivos de trabalho, 63,4% dos entrevistados respondem que sim. Esse resultado é mostrado na figura 4.17.

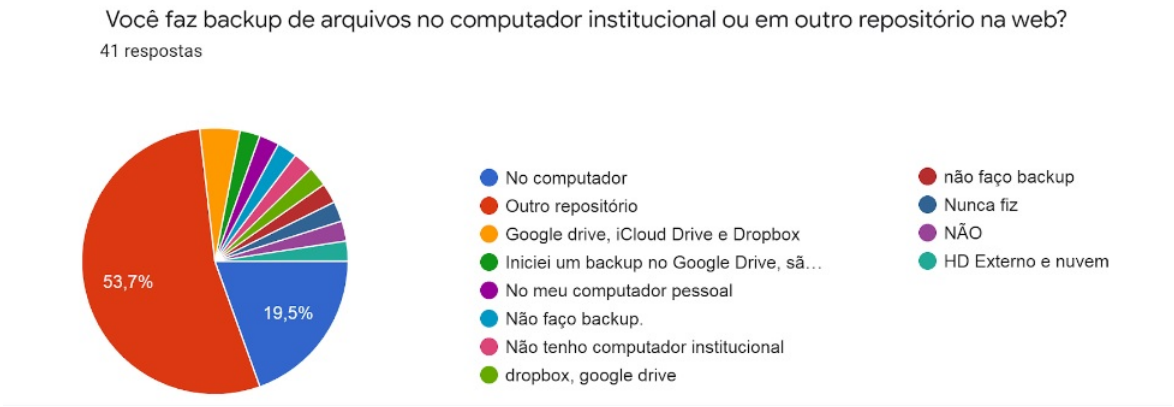
Figura 4.17: Quantitativo de respostas sobre fazer backup de arquivos de trabalho.



Fonte: Elaborado pela autora

Referente ao local onde o servidor faz o backup de arquivos, se é no computador institucional ou em outro repositório na web, dando também outras opções de respostas, dos entrevistados, 53,7% responderam que fazem o backup dos arquivos em outro repositório, enquanto 19,5% fazem no computador da instituição. A figura 4.18 mostra todas as respostas desse resultado.

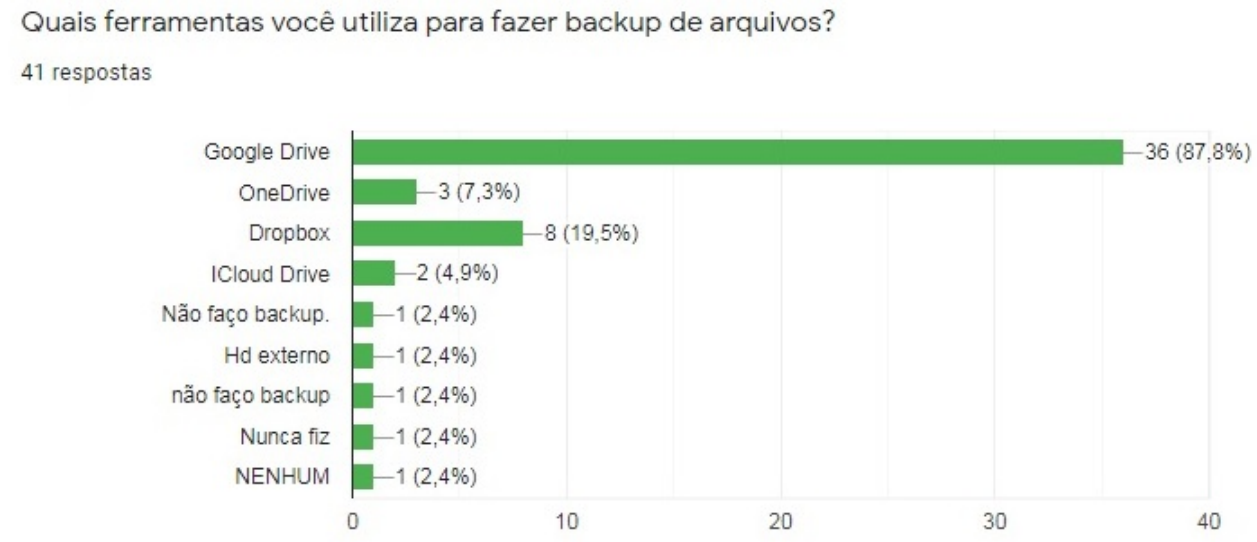
Figura 4.18: Quantitativo de respostas sobre o local onde esse backup de arquivos seria feito.



Fonte: Elaborado pela autora

Em referência a quais ferramentas o servidor utiliza para fazer o backup de arquivos, 87,8% das pessoas entrevistadas responderam que utilizam o Google Drive, 19,5% utilizam o Dropbox e 7,3% utilizam o OneDrive. As demais respostas é possível ver no gráfico a seguir da figura 4.19.

Figura 4.19: Quantitativo de respostas sobre as ferramentas usadas para fazer o backup dos arquivos de trabalho.



Fonte: Elaborado pela autora

4.2 Resultado da comparação entres as PoSICs do IF Sertão-PE, IFPE e IFPB

Após a análise das respostas do questionário aplicado, foi feita também uma análise comparativa entre a política de segurança do Instituto Federal do Sertão Pernambucano (IF Sertão-PE) [24], Instituto Federal do Pernambuco (IFPE) [28] e o Instituto Federal da Paraíba(IFPB) [29], onde será mostrado os principais tópicos contidos nesses documentos.

A tabela 4.1, faz mostra o resultado desta comparação.

Tabela 4.1: Comparação da estrutura de normas e diretrizes da POSIC dos institutos IFSertão-PE, IFPE e IFPB.

PoSIC	IF Sertão	IFPE	IFPB
Objetivo	X	X	X
Fundamento Legal da PoSIC	X	X	X
Conceitos e Definições	X	X	X
Política de Segurança da Informação e Comunicação		X	X
Competências e Responsabilidades é Estrutura da Gestão de Segurança da Informação	X	X	X
Diretrizes	X	X	X
Penalidades	X	X	X
Disposições Gerais		X	X
Atualização	X	X	X
Vigência		X	X
Princípios	X	X	
Gestão de Risco		X	X
Gestão de Continuidade do Negócio		X	X
Controle de Acesso		X	X
Correio Eletrônico	X	X	X
Declaração de Comprometimento	X		
Abrangência	X	X	
Política de Backup	X		
Utilização dos Laboratórios de Informática	X		
Tratamento de Incidentes		X	
Criptografia		X	

Através da tabela 4.1 é possível ver que há uma diversificação na composição dessas PoSICs. Entretanto, isso não significa dizer que uma ou outra esteja errada, mas de acordo com a realidade das instituições para as quais foram criadas essas políticas.

Em comparação aos outros Institutos, o IF Sertão-PE em sua PoSIC possui uma quantidade menor de recomendações, normas e procedimentos. Por exemplo, o controle de acesso e o tratamento de incidentes.

Enquanto o IFPE e o IFPB possui documentos complementares à sua PoSIC como Gestão de Risco e um Plano de Continuidade do Negócio. A PoSIC do IF Sertão-PE também se destaca dos demais, por ser o único entre os três a possuir uma política de backup e normas para a utilização dos laboratórios de informática.

5

Conclusão

Diante dos resultados, é possível ver que aproximadamente 80% dos servidores entrevistados não possuem o conhecimento acerca das diretrizes e normas estabelecidas na PoSIC do IF Sertão, do qual é de extrema importância para os servidores quanto ao uso dos equipamentos de Tecnologia da Informação.

Os resultados obtidos mostram que os servidores não conhecem as normas de segurança do seu ambiente de trabalho, logo, não sabem como utilizar de maneira adequada seguindo as normas, as tecnologias que utilizam no seu dia-a-dia.

A pesquisa mostrou o quanto é importante buscar meios de fazer com que os servidores conheçam as orientações contidas na PoSIC, considerando o fato de que todos deveriam estar cientes das normas estabelecidas neste documento. Entretanto, através das respostas, somente duas pessoas afirmaram passaram por treinamentos, assim, pode-se deduzir que somente os servidores da área de TI passaram por esses treinamentos.

Os resultados mostram que há pessoas que acessam suas redes sociais usando o e-mail

institucional, mesmo sendo um número pequeno de pessoas, mas segundo a PoSIC do IF SERTÃO-PE, é inadmissível uso do e-mail institucional para acessar redes sociais, bem como para qualquer outra utilização que não estejam associadas às funções institucionais.

A falta de conhecimento das boas práticas de segurança, pode tornar mais fácil um acesso indevido a determinada área ou informação. No que se refere a utilização de senhas, segundo os dados coletados na pesquisa, mais de 50% dos servidores entrevistado não utilizam caracteres especiais em suas senhas, o que torna uma senha mais frágil e insegura. E é importante que a Direção Geral de Tecnologia da Informação (DGTI) possa ressaltar a importância de ter uma senha segura e orientar os servidores no momento da criação de uma conta do e-mail institucional, pois, a DGTI é o órgão executivo da Pró-reitora de Desenvolvimento Institucional (PRODI), que é responsável pelo planejamento, direção, avaliação e execução das políticas de tecnologia da informação comunicação (TIC) em todo o Instituto.

A comparação feita entre as PoSICs do IF Sertão-PE, IFPE e IFPB mostrou que apesar da singularidade de cada PoSIC, todos eles possuem um objetivo comum, promover a segurança da informação através de normas e diretrizes para a utilização de equipamentos tecnológicos nos campi de cada região que as PoSICs abrangem.

5.1 Trabalhos Futuros

Como trabalhos futuros:

• Elaboração de uma cartilha informativa sobre o uso das Políticas de Segurança da Informação e Comunicação

• Comparar a PoSIC dos outros Institutos Federais que não foram contemplados do trabalho em relação as normas e diretrizes.

• Ampliar a pesquisa para avaliar o conhecimento dos servidores sobre as normas e diretrizes da PoSIC dos demais campi

Referências Bibliográficas

[1] J. A. G. Júnior, "Adoção da tecnologia da informação nas micro e pequenas empresas de taquarituba–sp," 2013.

[2] F. C. d. Azevedo, "Tecnologia da informação na gestão pública: um estudo de caso sobre a divulgação de conteúdo nas páginas da transparência eletrônica ativa da prefeitura municipal de jardim do seridó-rn," B.S. thesis, Universidade Federal do Rio Grande do Norte, 2015.

[3] O. K. L. Rios, J. G. de Almeida Teixeira Filho, e V. P. da Silva Rios, "Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação," *NAVUS-Revista de Gestão e Tecnologia*, vol. 7, n. 2, pp. 49–65, 2017.

[4] S. Paiva, "Segurança e auditoria de sistemas," 2017.

[5] S. C. Gomes, K. R. M. Negrão, T. da Silva Lima, C. M. Martins, e M. C. d. S. de Carvalho, "Adoção de tecnologia da informação como estratégia para melhorar o desempenho da gestão de micro e pequenas empresas," *REMIPE-Revista de Micro e Pequenas Empresas e Empreendedorismo da Fatec Osasco*, vol. 5, n. 1 Jan-Jun, pp. 24–45, 2019.

[6] J. P. Munhoz, "Gestão da tecnologia da informação," 2015.

[7] S. M. H. M. C. W. M. Spagnuolo, Fernando de Oliveira, "A importância da tecnologia da informação no suporte à tomada de decisões."

[8] E. F. Da Silva, "Vulnerabilidade humana – recomendção para conscientizção do aspecto humano como elo mais fraco da segurança da informção nas empresas," *São Paulo: USP*, 2016.

[9] L. P. de Paula e D. F. Cordeiro, "Políticas de segurança da informação em instituições públicas," *Revista Eletrônica de Sistemas de Informação e de Gestão Tecnológica*, vol. 6, n. 2, 2016.

[10] L. B. CASTILHO, "O uso da tecnologia da informação e comunicação (tic) no processo de ensino e aprendizagem em cursos superiores," *Projetos e Dissertações em Sistemas de Informação e Gestão do Conhecimento*, vol. 4, n. 2, 2018.

[11] C. de Oliveira, "Tic's na educação: a utilização das tecnologias da informação e comunicação na aprendizagem do aluno," *Pedagogia em Ação*, vol. 7, n. 1, 2015.

[12] A. N. ISO, "Iec 17799: 2005: Tecnologia da informação–técnicas de segurança–código de prática para a gestão da segurança da informação," *Rio de Janeiro, Associação Brasileira de Normas Técnicas*, 2005.

[13] ——, "Iecc 27002:2013 tecnologia da informação–técnicas de segurança–código de prática para a gestão da segurança da informação," *Rio de Janeiro, Associação Brasileira de Normas Técnicas*, 2013.

[14] M. C. F. COSTA, "O bibliotecário no contexto da segurança da informação." 2019.

[15] L. d. M. Ferreira, "Os riscos do sequestro de informações pelos ransomwares," *Gestão da Segurança da Informação-Unisul Virtual*, 2017.

[16] R. A. Souza, "Segurança da informação no serviço público: a realidade da segurança da informação no instituto federal de educação, ciência e tecnologia do rio de janeiro," *Tecnologia em Gestão da Tecnologia da Informação-Unisul Virtual*, 2017.

[17] R. F. Diorio, E. Serafim, K. R. Alves, e M. C. Meira, "Segurança da informação e de sistemas computacionais: Um estudo prático sobre ataques utilizando malwares," *Anais SULCOMP*, vol. 9, 2018.

[18] D. R. d. Brito, "Combatendo a ameaça ransomware aplicando a norma iso/iec 27001: 2013 na gestão da segurança da informação," 2016.

[19] J. W. Candido, J. H. G. Borges, e F. Florian, "Segurança da informação com foco na propagação iminente de ransomware nas corporações," 2017.

[20] L. H. Gasparini, "O usuário como o elo mais frágil da segurança da informação: uma analise para os batalhões de comunicações em 2018," 2018.

[21] E. S. de Sousa, "A gestão da ti dentro do serviço público," *Curitiba*, 2014.

[22] E. Teodoro, "Protótipo de um sistema em java para atender os principais processos de gestão administrativa de uma micro ou pequena empresa," *Revista Technologies Faculdades Network–Revista da Faculdade de Sistemas de informação ISSN-1677-7778*, p. 24, 2014.

[23] F. A. Manduca, "Segurança da informção em ambientes organizacionais: Uma abordagem bibliográfica," *Curitiba*, 2014.

[24] "Política de segurança da informação e comunicação do if serão-pe," *Petrolina-PE*, 2016.

[25] L. F. Pinto e C. M. F. Rocha, "Inovações na atenção primária em saúde: o uso de ferramentas de tecnologia de comunicação e informação para apoio à gestão local," *Ciência & Saúde Coletiva*, vol. 21, pp. 1433–1448, 2016.

[26] M. R. Lyra, "Governança da segurança da informaçao," *Brasília: nd*, 2015.

[27] F. A. RAMOS e P. E. R. CARMO, "As tecnologias de informação e comunicação(tics) no contexto escolar," 2012.

[28] "Política de segurança da informação e comunicação do ifpe," *Recife-PE*, 2017.

[29] "Política de segurança da informação e comunicação do instituto federal de educação, ciência e tecnologia da paraíba," *Paraíba-PB*, 2011.