Instituto Politécnico de Santarém

Escola Superior de Educação
Mestrado em Ciências da Educação/Administração Educacional

Política de segurança da informação e o acesso à internet: o caso de um Instituto Federal do Brasil

Edimária Cerqueira Rodrigues Lamounier

Orientadora: Professora Doutora Susana Isabel Gueifão Colaço

Coorientadora: Professora Doutora Maria Cristina Madeira da Silva

2019, julho

Instituto Politécnico de Santarém

Escola Superior de Educação
Mestrado em Ciências da Educação/Administração Educacional

Política de segurança da informação e o acesso à internet: o caso de um Instituto Federal do Brasil

Trabalho de projeto realizado para obtenção do Grau de Mestre em Ciências da Educação/Administração Educacional.

Edimária Cerqueira Rodrigues Lamounier

Orientadora: Professora Doutora Susana Isabel Gueifão Colaço

Coorientadora: Professora Doutora Maria Cristina Madeira da Silva

2019, julho

“*Mesmo que já tenha feito uma longa caminhada, sempre haverá mais um caminho a percorrer***”**

Santo Agostinho

Agradecimentos

Detalhista que sou, fiquei preocupada em como apresentar meus agradecimentos sem deixar de mostrar a importância de cada pessoa nesse processo que eu vivenciei. Depois de muito pensar, descobri que não teria como fazê-lo apenas sendo sucinta, seguindo regras e modelos. Não seria eu mesma se assim o fizesse. Portanto, sem me prender a formatos e discursos adequados, mas com o coração cheio de alegria, gratidão, entusiasmo e até de saudade do que ainda não foi, sigo.

Agradeço a Deus sempre e por tudo! Agradeço a Ele por eu ter...

- … os melhores pais do mundo e que, ainda hoje, apoiam as minhas “boas loucuras” e me dão colo quando preciso;
- … o posto de filha caçula, no qual até hoje me faz “sofrer as consequências” do cuidado e do amor de um irmão mais velho;
- … nascido numa família linda, acolhedora, onde os mais velhos são minha referência; os da minha geração, meus amigos de/para a vida; e os mais novos meus “xodós”;
- … sido presenteada com um esposo amigo, parceiro, companheiro e que se entregou ao máximo, morrendo para si mesmo um pouquinho a cada esforço extra a mim dedicado nesse período, para que pudesse me dar tranquilidade na construção deste trabalho;
- … conhecido o amor incondicional, por meio da minha filha. Esse “serzinho” que é o meu bem maior e que, por muitas vezes nesta etapa, encheu-me de beijos, de massagens e de apoio dizendo “mamãe, fique tranquila! Vai dar certo!”;
- … numa mesma pessoa, um amigo e um diretor espiritual, o qual me fez entender que nos momentos difíceis é preciso aprender a “andar sobre a morte, assim como Pedro andou sobre as águas do mar”;
- … amigos fiéis que estão sempre disponíveis tanto para um brinde (tim-tim) quanto para me oferecerem o ombro nos momentos difíceis;
- … sido “vítima” do maravilhoso esforço da Profª. Drª. Maria Cristina Madeira, que defendeu com a máxima dedicação os servidores técnicos para que estes pudessem participar das turmas de Mestrado em Ciência da Educação/Administração Escolar. Não por acaso fiz o convite para que esta mulher fantástica fosse minha coorientadora e fui presenteada com o seu sim. Cris, a você minha gratidão sempre!
- … recebido da instituição em que trabalho a oportunidade de vivenciar a experiência do Mestrado numa turma excepcional em convívio e em contribuição mútua e, ainda, com o apoio incondicional do meu amigo (há época meu chefe) e dos

demais colegas de equipe. Em especial Cláudia e João que, também estudantes do mestrado, foram parceiros nos momentos de desespero e também nos de risadas. Ficou mais fácil com vocês por perto.

… bebido do conhecimento e da vasta experiência dos doutores educadores que vieram de Portugal especialmente para nos fazer compreender que educar é o nosso compromisso mas, para além disso, uma linda e transformadora missão;

… recebido como orientadora a Profª Drª Susana Colaço, uma mulher que me inspira por quem é, pelo que representa profissionalmente e pela postura que tem. Ela que por muitas vezes me acompanhou noites adentro, dando-me força, contribuindo com o trabalho e, mesmo em meio a tanto cansaço, ainda me incentivava a continuar firme e assim se forçava a ficar também. Susana, a você serei eternamente grata por todo apoio e parceria durante essa trajetória do Mestrado. Sentirei saudades;

… conversado com meu amigo Leôncio e, numa dessas conversas, ele me fez pensar no tema que resultou o meu trabalho de projeto;

… conseguido perceber, mesmo um pouco tarde, que aqui não é uma autobiografia e sim, uma página de agradecimento e, portanto, corro para finalizar.

Mas antes, preciso registrar um agradecimento especial aos docentes parceiros que foram a campo comigo em busca de angariar respondentes ao meu instrumento de coleta de dados. Professores Paulo Wanderley, Fábio Ferraz, Leôncio Dutra e Professora Ana Cláudia Vilarinho, com a ajuda de vocês deu certo! Gratidão!

Também não posso deixar de agradecer aos colegas que me ajudaram a validar o instrumento de coleta de dados, bem como a todos os docentes que se predispuseram a respondê-lo, compartilhando comigo sua visão e sua experiência sobre o tema Segurança da Informação. Vocês me forneceram insumos e me deram condições para construir este projeto. Muito obrigada!

Dedico este trabalho a todos que, de uma forma ou de outra, fizeram parte desta etapa da minha vida, seja presencial seja espiritualmente.

Índice de Conteúdo

Índice de Tabelas

Índice de Quadros

Índice de Gráficos

Lista de Abreviaturas e Siglas

ABNT: Associação Brasileira de Normas Técnicas

APF: Administração Pública Federal

ARPANET: *Advanced Research Projects Agency Network* ou Rede da Agência para Projetos de Pesquisa Avançada

BS7799: *British Standard 7799*

CAIS: Centro de Atendimento a Incidentes de Segurança

CCSC: *Commercial Computer Security Centre*

CERT: *Computer Emergency Response Team* ou Centro de Estudos para Resposta e Tratamento de Incidentes em Computadores

CID: confidencialidade, integridade e disponibilidade

CRFB: Constituição da República Federativa do Brasil

CSIRTs: *Computer Security Incident Response Teams*

DES: *Data Encryption Standard*

DF: Distrito Federal

DoD: U.S.Department of Defense

DSIC: Departamento de Segurança da Informação e Comunicações

DTIC: Diretoria de Tecnologia da Informação e Comunicação

ECA: Estatuto da Criança e do Adolestete

FIC: Formação Inicial e Continuada

FW: *Firewall*

IEC: *International Electrotechnical Commission* (Comissão Eletrotécnica Internacional) significa International Engineering Consortium.

IF: Instituto Federal

ISO: *International Organization for Standardization* (Organização Internacional de Normalização).

GSI: Gabinete de Segurança Institucional

LAI: Lei de Acesso à Informação

LDB: Lei de Diretrizes e Bases da Educação Nacional

MCTIC: Ministério da Ciência, Tecnologia, Inovações e Comunicações

MD5: *Message-Digest algorithm 5*

MEC: Ministério da Educação

NASA: *National Aeronautics and Space Administration* ou Administração Nacional da Aeronáutica e Espaço

NBR: Norma Brasileira

NIC.BR: Núcleo de Informação e Coordenação do Ponto BR

ONU: Organização das Nações Unidas

POSIC: Política de Segurança da Informação

PSI: Política de Segurança da Informação

RNP: Rede Nacional de Ensino e Pesquisa

SCCS: *Security Controls for Computar Systems*

SETEC: Secretaria de Educação Profissional e Tecnológica

SHA: *Secure hash algorithm* ou algoritmo de dispersão seguro

SI: Segurança da Informação

SIC: Segurança da Informação e Comunicação

SIGEPE: Sistema de Gestão de Pessoas

SUAP: Sistema Unificado da Administração Pública

TCP/IP: *Transmission Control Protocol/Internet Protocol*

TCSEC: *Trusted Computer System Evaluation Criteria*

TCU: Tribunal de Contas da União

TI: Tecnologia da Informação

TIC: Tecnologia da Informação e Comunicação

Política de segurança da informação e o acesso à internet: o caso de um Instituto Federal do Brasil

Resumo

Este estudo analisou em que medida as Políticas de Segurança da Informação (PSI), pautadas nas diversas legislações, podem ferir o direito à informação no ambiente académico.

Os docentes de um Instituto Federal Brasileiro constituíram o público para o *design* metodológico escolhido: Estudo de Caso com abordagem de natureza qualitativa e quantitativa.

Muitos docentes defendem que não cabe à escola cercear o acesso à informação e sim, preparar cidadãos críticos e conscientes, mas essa defesa perde força ao se depararem com o risco de responsabilização por uso indevido da internet nas suas aulas.

Apesar de muitos desconhecerem a PSI, a maioria dos docentes é favorável a ela e afirmam que o fator impeditivo para dinamização das aulas não está nas restrições de acesso, mas na dificuldade em conseguirem liberar sítios bloqueados, que considerem úteis para desenvolver um determinado conteúdo em sala de aula.

O Projeto de intervenção apresenta o escopo de uma metodologia de criação de um Sistema de Gestão de Segurança da Informação para a instituição onde foi realizado o estudo.

Palavras-chave: Política de Segurança da Informação; Internet; Acesso à informação, Ambiente Académico, Sistema de Gestão de Segurança da Informação

Information security policy and internet access: the case of a Brazilian Federal Institute

Abstract

This study examined the extent to which Information Security Policies (ISPs), based on different laws, may harm the right to information in the academic environment.

The teachers of a Brazilian Federal Institute constituted the public for the chosen methodological design: Case Study with a qualitative and quantitative approach.

Many teachers argue that it is not up to the school to curtail access to information, but to prepare critical and conscientious citizens, but this defense loses its strength when faced with the risk of liability for misuse of the internet.

Although many are not aware of the PSI, most teachers are in favor of it and affirm that the factor impeding the dynamization of classes is not in the access restrictions, but in the difficulty in being able to release blocked sites that they consider useful to develop a certain content in classroom.

The Intervention Project presents the scope of a methodology for creating an Information Security Management System for the institution where the study was carried out.

Keywords: Information Security Policy; Internet; Access to information, Academic environment, Information Security Management System

Introdução

Este estudo teve o intuito de analisar em que medida as políticas de segurança da informação, restringindo o acesso à Rede Mundial de Computadores – Internet, dentro de uma instituição educacional brasileira, podem ter implicações, na opinião dos docentes, no ensino-aprendizagem no âmbito da lecionação das suas disciplinas.

Muitos docentes defendem que é prerrogativa do ambiente académico constituir um espaço democrático propício para a formação de cidadãos conscientes, em que o acesso à informação não deve ser cerceado sob qualquer hipótese.

Contrárias a essa defesa, aparecem legislações e órgãos regulamentadores que impõem requisitos de segurança da informação que, por vezes, tendem a restringir ou mesmo negar o acesso a alguns tipos de informação em prol da proteção das informações institucionais e, principalmente, das pessoas que nela atuam.

Cabe ressaltar que com a internet rompem-se as barreiras nacionais e individuais e as pessoas são apresentadas ao livre acesso ao conhecimento e à informação em quantidades nunca antes experimentadas. Neste ambiente abrem-se espaços para novas discussões e novos conflitos, além de muitos questionamentos.

Nesse contexto conflitante, mas também desafiante, torna-se necessário analisar as garantias fundamentais à luz do princípio da proporcionalidade para que se chegue a um equilíbrio entre os direitos, pois o abuso de um, pode prejudicar o outro. E ambos configuram direitos dos quais não se pode abdicar.

Como proceder nos casos em que as imagens ou publicações ofensivas estão hospedadas em outro país cuja legislação não as considera como tal?

Como avaliar o potencial ofensivo de certos discursos antes que eles se espalhem?

Como reparar os danos causados pelo abuso da liberdade de expressão e, ainda, em tempo razoável?

O que é direito de liberdade de expressão e o que é ofensa contra a imagem ou a dignidade de um grupo de pessoas?

Quando a liberdade de expressão e o direito à informação extrapolam seu limite e tornam-se discurso de ódio e promoção da intolerância?

Enfim, são infindáveis os questionamentos, mas o que se pretende com eles é dar destaque ao uso abusivo da internet, que é, certamente, um dos problemas mais controversos que foi imposto pela sociedade em rede e que suscita uma reflexão importante para a dualidade imposta: a imposição de restrições à liberdade à informação e de expressão na Internet versus a tutela dos direitos da personalidade, em especial quando analisados sob a égide do princípio da dignidade humana.

Desta forma, o virtual torna-se realidade jurídica, na medida em que novas relações se constituem, tanto no âmbito privado como no público. O choque de direitos torna-se inevitável e os direitos fundamentais vêm protegidos no âmbito constitucional brasileiro, sendo perfeitamente adequado ao universo do ciberespaço.

Assim, faz-se necessário conhecer essa realidade social e jurídica para que se possam enfrentar tais conflitos e buscar soluções efetivas para tais incompatibilidades, sem desconsiderar os direitos individuais tão bem definidos na Constituição Brasileira, mas sim buscando a proporcionalidade e a razoabilidade entre eles, pois o respeito a estes direitos é característica fundamental do Estado Democrático de Direito.

Cabe ao Estado zelar para que todos possam conviver de forma civilizada e respeitosa neste ambiente. Portanto é necessário que as pessoas que abusam do direito à informação e da liberdade de expressão, estejam conscientes que são passíveis de responsabilização.

Foram essas diferentes visões sobre como deve ser o acesso à internet dentro de uma mesma instituição que acabaram por motivar este estudo, uma vez que enquanto profissional que atua na área de Tecnologia da Informação e Comunicação dentro de uma instituição de ensino, posso permear os dois lados de defesa, entendendo e concordando com ambos.

Porém, mais que entender, concordar ou discordar, o importante é descobrir se essas ações interferem na dinamização do ambiente de sala de aula ou ainda no processo de ensino-aprendizagem dos estudantes, e esse foi o objetivo principal deste trabalho.

A metodologia de investigação científica escolhida para a realização do trabalho de pesquisa foi o Estudo de Caso, sendo ele realizado a partir de uma abordagem com natureza essencialmente qualitativa, embora dados quantitativos também puderam ser recolhidos e analisados.

Este Estudo de Caso, portanto, restringiu-se aos docentes de um Instituto Federal Brasileiro, uma autarquia vinculada ao Ministério da Educação – MEC e criada em dezembro de 2008, por meio da lei nº 11.892, no qual passou a compor a Rede Federal de Educação Profissional, Científica e Tecnológica, existente em todo o Brasil.

A partir do cenário proposto, os instrumentos de recolha de dados utilizados para a realização do Estudo de Caso foi inquérito por questionário e a análise documental, os quais juntos permitiram uma significativa coleta de dados que serviu de insumo para a análise proposta e consequentemente a triangulação de alguns dados.

Em termos de estrutura, este trabalho está organizado em cinco capítulos. No primeiro capítulo, intitulado Enquadramento Teórico, fez-se uma varredura por histórico, conceitos e legislações que abarcam os temas abordados e que fundamentaram a compreensão da temática.

Portanto, aborda desde o conceito primeiro de “Informação” até suas nuances a depender do contexto utilizado e ainda ao longo da história. Também traz uma abordagem que passa pelo Direito à Informação – que é muito ligado à Liberdade de expressão – e às legislações que o amparam, até chegar às questões ligadas à Segurança da Informação.

No segundo capítulo é apresentada a Metodologia, ressaltando os objetivos, as opções metodológicas, os participantes do estudo, os instrumentos de recolha de dados e como a análise de dados foi realizada.

A análise e discussão dos resultados são apresentadas no terceiro capítulo. As conclusões e a proposta de projeto de intervenção são trazidas no capítulo quarto.

O capítulo cinco aborda as limitações do estudo realizado e apresenta a delineação de possibilidades de estudos posteriores a este trabalho.

Objetivos de Investigação

O objetivo principal deste trabalho consiste em analisar em que medida a aplicação das políticas de segurança da informação impacta o trabalho do docente no momento em que este busca a dinamização das aulas por meio do acesso à internet.

Para responder ao objetivo principal foi necessário definir outros objetivos específicos:

- Verificar se a Política adotada na instituição está de acordo com o que os órgãos regulamentadores nacionais ditam quanto às políticas de segurança da informação na Administração Pública Federal;
- Identificar se os docentes conhecem a política de segurança da informação da instituição;
- Analisar como os docentes veem a política de segurança da informação no âmbito da utilização das ferramentas WEB 2.0 no processo de ensino e aprendizagem.

I – ENQUADRAMENTO TEÓRICO

Informação

A informação é o elemento básico para a humanidade desde o seu surgimento. As pessoas, constantemente, trocam informações com elementos internos e externos ao meio em que vivem. Portanto, nas sociedades humanas, a informação tem um impacto nas relações entre diferentes indivíduos e, ao longo da história, a forma de armazenamento e acesso à informação sofreu variações, além do crescimento de seu volume.

Na chamada Idade Média, eram nas bibliotecas dos mosteiros que se encontrava o acervo principal de informação. A imprensa nasceu na Idade Moderna e a partir de então os livros começaram a ser fabricados em série. Nesse período também surgiu o jornal. E estava instalada a evolução das formas de informação.

Os meios de comunicação de massas, como o rádio, a televisão e as ferramentas digitais, apareceram no século passado e alavancaram o surgimento e o desenvolvimento da internet. Com a globalização, essa troca de informação cresceu exponencialmente. Sobre o volume de conhecimento, Wurman (1991) diz que uma única edição do jornal americano *The New York Times* há mais informação do que um cidadão comum da Inglaterra do século XVII poderia receber durante toda sua vida.

No ambiente da informação, permeiam alguns conceitos, nos quais encontramos definições específicas para dados, informação, conhecimento e inteligência. Esses conceitos alcançam áreas específicas, como, por exemplo, a militar, cuja atividade de inteligência está voltada para defesa do Estado, e a empresarial, que direciona essa atividade para os negócios.

Para Chiavenato (1999), informação é o conjunto de dados com um significado, ou seja, que reduz a incerteza ou que aumenta o conhecimento a respeito de algo. Aparecem dois outros conceitos: dado e conhecimento.

Para Davenport e Prusak (2000), dados são simples observações sobre o estado do mundo, é facilmente estruturado, facilmente obtido por máquinas, frequentemente qualificado e facilmente transferível. Para eles conhecimento é uma informação valiosa da mente humana. Inclui reflexão, síntese e contexto. De difícil estruturação, difícil captura em máquinas, frequentemente tácito e de difícil transferência.

Além dos três conceitos acima (informação, dado e conhecimento), há outro que muito se confunde com conhecimento, mas que está acima deste: a inteligência ou, para alguns, sabedoria que, segundo Greenberg (1963), é a capacidade de fazer o uso correto do conhecimento.

Portanto, para consolidar esses conceitos, Cardoso (2005) diz que os dados compreendem a classe mais baixa da informação. A informação propriamente dita são os dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível. O conhecimento é a informação cuja relevância, confiabilidade e importância foram avaliadas, e é obtido pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação. A inteligência é a informação com oportunidade, ou seja, é a parte do conhecimento que habilita a tomada das melhores decisões.

A partir disso, buscou-se trazer para este estudo o conceito de informação sob vários enfoques, conforme apresentados a seguir.

Informação no âmbito da Comunicação

Para a comunicação, informação é a mensagem trocada entre dois ou mais interlocutores. É a mensagem codificada, transmitida, decodificada e interpretada. (Castells, 2009).

A informação atribui significado a realidade mediante seus códigos e o conjunto de dados. Ela é capaz de dar origem à formação do pensamento humano, além de permitir a resolução de problemas e a tomada de decisões, com base no uso racional deste conhecimento adquirido através dela.

Portanto, comunicação é a base da Informação e quanto mais precisa for a informação melhor será a comunicação.

Informação no âmbito do ambiente de ensino

No ambiente de ensino a busca pela informação que gera conhecimento é crescente, e tanto o acesso quanto o uso da informação vêm modificando as estruturas escolares.

Nessa linha, se a informação faz parte da construção do conhecimento, o acesso a ela não deve estar sujeito a qualquer forma de censura ideológica, política ou religiosa, nem às barreiras económicas.

A Constituição da República Federativa do Brasil de 1988 - CRFB (88) defende que todos os cidadãos, independente de raça, religião, sexo, idade, têm direito ao acesso à informação e o de expressar suas opiniões publicamente e a escola deve oferecer ambiente favorável ao processo de construção do conhecimento, às ideias e à manifestação do processo criativo.

É, portanto, papel da instituição de ensino desenvolver as competências na busca, recuperação, disseminação e no uso da informação. A escola deverá ser capaz de guiar os estudantes, orientando-os para selecionar e contextualizar o que é relevante neste universo de informações disponíveis.

Informação e conhecimento estão relacionados, mas não são sinónimos. O fato dos estudantes terem acesso à informação não significa que possuam conhecimento sobre um determinado assunto. O papel do docente aí é fundamental para ajudar o estudante, a partir da informação, a construir o conhecimento e a desenvolver competências.

Libâneo (2007) afirma que: “o grande objetivo das escolas é a aprendizagem dos estudantes, e a organização escolar necessária é a que leva a melhorar a qualidade dessa aprendizagem”. Libâneo (2007, p.309)

Informação no âmbito da Gestão Institucional

De acordo com a Brasileira de Normas Técnicas – ABNT – NBR ISO/IEC 17799 (2003), a informação é um ativo que, como qualquer outro importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido.

Gonçalves (2015) corrobora com esse pensamento ao afirmar que a informação é um elemento crítico para as organizações. Sem informação, nenhuma instituição sobrevive e consegue se manter em seu mercado de atuação.

Na mesma linha, Dias (2003) defende que a informação é o principal património da empresa e está sob risco permanente. É a essência da inteligência competitiva e deve ser administrada, diferenciada e salvaguardada. Ela funciona como um recurso fundamental para a obtenção de estratégias alternativas e para organização flexível, onde o aprendizado é constante.

De acordo com Rezende e Abreu (2000) a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. Ela ajuda na identificação das ameaças e das oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente. Com a evolução dos sistemas de informação, ganhou-se mobilidade, inteligência e real capacidade de gestão.

Portanto, a informação, em conjunto com recursos tecnológicos, é uma necessidade para o funcionamento tático, estratégico e operacional de qualquer instituição. Isso porque possibilita que a alta gestão elabore seu planejamento estratégico-tático e que as atividades operacionais sejam realizadas e controladas, atuando assim como ferramenta estratégica de competitividade.

Informação no âmbito da Informática

Os rápidos avanços da Tecnologia da Informação (TI) se refletem no cenário de constantes mudanças característico da sociedade moderna. No mundo marcado por rápidas e profundas transformações, estudos sobre a TI e a educação tornam-se fundamentais para

compreender e acompanhar as novas demandas educacionais contemporâneas (Wang, 2006).

A Tecnologia da Informação - TI, é uma área que utiliza a computação como um meio para produzir, transmitir, armazenar, acessar e usar diversas informações. Ela pode ser utilizada em diversos contextos, tendo uma definição bem complexa e ampla.

A tecnologia é usada para fazer o tratamento da informação, auxiliando o utilizador a alcançar um determinado objetivo, por meio dos sistemas de informação, que constituem um modelo de processos responsáveis por coletar e transmitir dados que sejam úteis ao desenvolvimento de produtos ou serviços das organizações.

O uso de sistemas da informação pode facilitar a comunicação e os processos administrativos, bem como apoiar a gestão na tomada de decisões estratégicas e com maior agilidade. A exemplo dos sistemas administrativos, financeiros, de folha de pagamento, bem como painéis de gerenciamento de informações, os *dashboards* gerenciais.

Da mesma forma, as Tecnologias da Informação podem ser úteis ao processo de ensino-aprendizagem. Os sistemas de gestão académica e ambientes virtuais de ensino são exemplos desse apoio.

1. Direitos e responsabilidades envolvidos no uso da Informação

A Constituição da República Federativa do Brasil de 1988 (CRFB/88) em seu artigo 5º abriga, em alguns dos seus dispositivos sob a forma de direitos e garantias fundamentais, um mister sobre a liberdade de imprensa, liberdade de expressão e também a liberdade de informação:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

Ainda no artigo 5º, a Constituição garante a todos de forma explícita o acesso à informação, inclusive preservando o sigilo da fonte, quando necessária ao sigilo profissional. Importante destacar o artigo 1º da Lei de Imprensa 5.250/67: “É livre a manifestação do pensamento e a procura, o recebimento e a difusão de informações ou ideias, por qualquer meio, e sem dependência de censura, respondendo cada um, nos termos da lei”.

Observa-se que o direito positivo brasileiro garante o direito de informar, e ao mesmo tempo, a tutela ao acesso às informações e comunicações. Esse direito antes concebido como um direito individual, atualmente é concebido como um direito de interesse coletivo à informação.

A Declaração dos Direitos do Homem e do Cidadão, estabelecida na França em 1789, aborda esse direito por meio do artigo 11, que traz explicitamente essa garantia: "*a livre manifestação do pensamento e das opiniões é um dos direitos mais preciosos: todo cidadão pode, portanto, falar, escrever e imprimir livremente, à exceção do abuso dessa liberdade pela qual deverá responder nos casos determinados por lei.*"

A Organização das Nações Unidas publicou, em 1948, a Declaração Universal dos Direitos Humanos que estabelece que *"toda pessoa tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras"*.

Da mesma forma, a Convenção Americana de Direitos Humanos, em 1969, afirma no artigo nº 13:

> Liberdade de pensamento e de expressão:
> 1. Toda pessoa tem o direito à liberdade de pensamento e de expressão. Esse direito inclui a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, sem considerações de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha.
> 2. O exercício do direito previsto no inciso precedente não pode estar sujeito à censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente previstas em lei e que se façam necessárias para assegurar:
> a) o respeito dos direitos e da reputação das demais pessoas;
> b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.
> 3. Não se pode restringir o direito de expressão por vias e meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões.
> 4. A lei pode submeter os espetáculos públicos a censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2.
> 5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitamento à discriminação, à hostilidade, ao crime ou à violência.

A Convenção Europeia de Salvaguarda dos Direitos do Homem e suas Liberdades Fundamentais, de 1950, também trata desse assunto em seu artigo 10, 1º:

> Toda a pessoa tem direito à liberdade de expressão. Esse direito compreende a liberdade de opinião e a liberdade de receber ou de comunicar informações ou ideias, sem que possa haver a ingerência da autoridade pública e se consideração de fronteiras. O presente artigo não impede os Estados de submeterem as empresas de radiodifusão, cinema ou televisão a um regime de autorização prévia.

Para Barroso (2011), a liberdade de informação, de expressão, e a liberdade de imprensa, não são direitos absolutos, encontrando limites na própria Constituição. Basta considerar os próprios direitos da personalidade como a honra, a intimidade, a vida privada e

a imagem (arts. 5º, X e 220, § 1º), a segurança da sociedade e do Estado (art. 5º, XIII), a proteção da infância e da adolescência (art. 21, XVI62), dentre outros.

Portanto, é indiscutível que o arcabouço legislativo defende a liberdade à informação. Todavia, há possibilidade de se delinear conflitos entre a liberdade à informação e de expressão com o direito à privacidade, direito à honra, direito à intimidade, direito à imagem e o próprio direito a vida.

Para minimizar esses conflitos, a Constituição Brasileira de 1988 (CRFB/88) preocupou-se em estabelecer limites para esses direitos. Em seu art. 53, por exemplo, buscou responsabilizar civil ou penalmente aqueles que agiram de forma a abusar de suas garantias, lesando o direito do outro.

Quando as restrições à Liberdade de Expressão ou a outros direitos fundamentais não estiverem estipuladas em lei, ou ainda, havendo desacordo entre previsões legais, far-se-á necessário recorrer aos princípios de ponderação entre os direitos envolvidos.

Serão apresentados neste tópico alguns desses direitos, sem nenhuma intenção de esgotá-los em sua totalidade, mas apenas buscando trazer todo o contexto que envolve a liberdade à informação e os cuidados com a segurança da informação.

1.1 Direito à Informação – Liberdade de Expressão

A necessidade de manter-se informado é uma questão de sobrevivência tanto individual (física, emocional, psíquica) quanto social e política.

Os direitos compreendidos no pensamento liberal dos séculos XVII e XVIII, assegurados pela Declaração Universal dos Direitos do Homem e no ordenamento jurídico português e brasileiro, a ideia de liberdade de expressão está profundamente ligada à ideia de liberdade à informação e, conforme esclarece Rodrigues (2009, p.61), compreende:

> Direito de **informar**: consiste na faculdade de comunicar informações a outrem sem impedimentos;
> Direito de **se informar**: consiste na faculdade de obter informações sem impedimentos;
> Direito de **ser informado**: consiste na liberdade de receber informações íntegras, verdadeiras e continuas, sem impedimentos*. (grifos do autor).*

Esse direito provém da ideia que permitindo que os cidadãos se manifestem livremente produz autonomia e variedade de discursos o que finalmente resultaria em uma sociedade mais transparente e representativa, características fundamentais a um modelo de governo democrático e estável.

A liberdade de expressão se relaciona com autorrealização a fim de que o homem possa desenvolver plenamente suas capacidades. Para tanto, o Estado deve defender o direito a troca de informações entre as pessoas, bem como garantir que elas possam livremente escolher que ideais desejam seguir e ou conhecer, ainda que o Estado propriamente dito não apoie tais posicionamentos.

Outro viés da liberdade de expressão é sua função de autogoverno, que atende a finalidade de proteger o processo democrático, uma vez que fomenta a discussão sem a dominância do poder político vigente. Nesse sentido não protege um direito individual, mas da coletividade.

A liberdade de expressão também pode ser utilizada como mecanismo de “controle” da sociedade sobre atos de agentes públicos, desta forma membros do povo podem denunciar ou expor atos ilícitos desses agentes sem que seja necessário temer represálias ou cerceamento. Nesse sentido a liberdade de expressão funcionaria como uma forma de verificação da atuação destes agentes.

Liberdades de informação e de expressão são diferenciadas pela doutrina brasileira. A primeira se refere ao direito do indivíduo de exprimir fatos sem cerceamento e ainda ao direito difuso de recebê-los sem censura prévia. Já a liberdade de expressão seria a garantia de expressar ideias, juízos de valor, opiniões ou qualquer outra manifestação de pensamento pessoal.

Em seu sentido mais amplo, a liberdade de expressão abarca a liberdade de informação, e sua diferenciação se faz necessária uma vez que a informação, diferentemente da opinião ou da crença, não pode prescindir da verdade.

Ainda que seja desconsiderada a ideia de verdade absoluta, a informação deve ser fundamentada em algo mais factível do que uma simples opinião ou ideia. O que não se aplica à liberdade de expressão, mesmo que o autor esteja passível de responsabilização pela difusão de ideias e de argumentos. (Barroso, 2011, p. 6)

Ainda que não seja possível controlar o pensamento é possível controlar aquilo que se manifesta e nessa seara a lei procurou garantir que seja possível identificar quem expressa o quê, o que sustenta a vedação do anonimato, o que torna possível responsabilizar na esfera jurídica aqueles que abusam do seu direito à liberdade de expressão.

1.2 Direito da Personalidade

A partir de um conceito tradicional, pode-se afirmar que todas as pessoas físicas ou jurídicas de um determinado país, são dotadas de personalidade jurídica, pois são sujeitos do direito.

O artigo 52 do Código Civil brasileiro dita que “aplica-se às pessoas jurídicas, no que couber, a proteção dos direitos da personalidade”, não conferindo direitos de personalidade aos entes despersonalizados. Para Godoy (2008, p.15):

> A personalidade consiste no conjunto de caracteres próprios da pessoa. A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apoia os direitos e deveres que dela irradiam, é o objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para

> sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens.

Portanto, o direito à personalidade (também denominado direito fundamental ou individual da pessoa, direito personalíssimo e direito sobre a própria pessoa) é considerado essencial para o desenvolvimento da pessoa humana e é configurado como direito absoluto, do qual nem a própria pessoa tem a faculdade de dispor dele.

Esse direito resguarda a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte de outros indivíduos.

Admite-se no Brasil um conceito geral para o direito da personalidade, com previsão no artigo 1º da Constituição Federal, adquirido pela tutela de bens específicos como a honra, a intimidade, a imagem das pessoas, entre outras, bem como pelo Novo Código Civil, quando relacionado o artigo 12 (eventualidade da violação), artigos 13 e 15 (direito ao próprio corpo, vivo ou morto), artigo 17 (direito ao nome), artigo 20 (direito à imagem) e artigo 21 (direito à privacidade).

1.3 Direito à Honra

Segundo Godoy (2008, p.28): “a honra compreende em seu significado, noções como a da autoestima, da consideração, da boa fama, do bom nome, da reputação que ao indivíduo se atribui”.

É possível analisar o conceito de honra sob a óptica subjetiva e objetiva. Sob o prisma interno, subjetivo, a honra pode ser relacionada com autoestima, amor próprio, sentimento da própria dignidade, consciência do próprio valor moral e social. Já pela óptica externa, a honra se refere ao conjunto de qualidades que os terceiros veem em uma pessoa, à forma como ela é vista pelos outros, pela sociedade, ou seja, traz a preocupação com apreço, respeito que a pessoa recebe; com a fama e a reputação que ostenta.

Destarte, a honra deve ser entendida sempre considerando os paradigmas sociais estabelecidos, portanto, seu valor é mutável ao longo do tempo, uma vez que tende a acompanhar as mudanças comportamentais da sociedade e os valores apreciados por um determinado grupo, num intervalo de tempo específico.

É interessante enfatizar que a forma como a pessoa é vista na sociedade influencia nas oportunidades que surgem para ela na comunidade. Se uma pessoa goza de confiança e respeito, esta terá mais consideração social e receberá oportunidades mais amplas, quando comparadas àquelas que são desprestigiadas. Estas, por sua vez, tendem a sofrer prejuízos não só nas relações pessoais, mas em seu poder econômico.

É possível inferir que essa diferenciação social descrita no parágrafo anterior justifica o fato de a honra ser um dos valores que o ser humano mais aprecia e defende enquanto direito fundamental à dignidade da pessoa humana.

1.4 Direito à Informação - Lei Brasileira de Acesso à Informação (Lei 12.527/11)

A Lei nº 12.527, sancionada pela Presidenta da República em 18 de novembro de 2011, tem o propósito de regulamentar o direito constitucional de acesso dos cidadãos às informações públicas e seus dispositivos são aplicáveis aos três Poderes da União, Estados, Distrito Federal e Municípios, inclusive aos Tribunais de Conta e Ministério Público. Entidades privadas sem fins lucrativos também são obrigadas a dar publicidade a informações referentes ao recebimento e à destinação dos recursos públicos por elas recebidos.

A publicação da Lei de Acesso a Informações significa um importante passo para a consolidação democrática do Brasil e também para o sucesso das ações de prevenção da corrupção no país. Por tornar possível uma maior participação popular e o controle social das ações governamentais, o acesso da sociedade às informações públicas permite que ocorra uma melhoria na gestão pública.

No Brasil, o direito de acesso à informação pública foi previsto na Constituição Federal, no inciso XXXIII do Capítulo I - dos Direitos e Deveres Individuais e Coletivos – o qual dispõe que:

> Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

A Constituição também tratou do acesso à informação pública no Art. 5º, inciso XIV, Art. 37, § 3º, inciso II e no Art. 216, § 2º. São estes os dispositivos que a Lei de Acesso a Informações regulamenta, estabelecendo requisitos mínimos para a divulgação de informações públicas e procedimentos para facilitar e agilizar o seu acesso por qualquer pessoa.

No Governo Federal, a Lei de Acesso à Informação foi regulamentada pelo Decreto nº 7.724/2012.

2 Decreto nº 7.724 de 16 de maio de 2012 da Presidência da República

Este decreto regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 18 de novembro de 2011.

De modo geral, o decreto reforça os pontos mais importantes da Lei de Acesso à Informação (LAI), como a obrigação da transparência ativa (a divulgação de informações de interesse público independentemente de solicitações), o direito de todos os cidadãos a pedir informações públicas e o fim do sigilo eterno de documentos oficiais. Mais relevante, entretanto, é que ele mitiga algumas dúvidas que ainda pairavam sobre certos dispositivos e

especifica as condutas e procedimentos que a esfera federal deve seguir para efetivar o cumprimento da Lei.

O decreto detalha como os pedidos de informação deverão ser feitos – sobretudo, como deverão ser processados e respondidos pela entidade pública. O decreto reitera e reforça a intenção de encerrar o segredo sobre papéis relacionados a práticas de tortura e morte de membros da oposição ao regime militar (1964-1984).

Mesmo os documentos que forem mantidos sob sigilo deverão ter algum nível de transparência. Os órgãos públicos deverão publicar na Internet, até o dia 1º de junho de todo ano, lista das informações desclassificadas nos últimos doze meses e lista das informações classificadas em cada um dos 3 graus de sigilo (detalhando o código de indexação do documento, categoria em que ele se encaixa e data de produção e classificação).

A publicação dessas listas anuais de documentos classificados e desclassificados foi incluída na lei por pressão da sociedade civil, porque se considerou que essa é uma ferramenta essencial para aferir o bom funcionamento da nova regra de transparência.

2.1 Crimes Virtuais

Os cibercrimes (em inglês, *cybercrimes*), e-crime, crime eletrônico, crime cibernético, crime informático, crime virtual ou crime digital são termos aplicáveis a práticas criminosas realizadas por meio de um computador ou de uma rede de computadores.

O termo *cybercrime* apareceu em uma reunião de um subgrupo do G-8 (grupo composto pelos sete países mais ricos do mundo, mais a Rússia, por sua importância histórica e militar) próximo do final dos anos 90. Essa reunião abordava exatamente as maneiras e os métodos utilizados para combater as práticas ilícitas da internet.

Segundo dados divulgados pela Norton, empresa especializada em segurança digital, a prática do cibercrime é tão comum que aproximadamente 65% dos internautas já foram vítimas de alguma forma de crime virtual.

Essas práticas podem envolver invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais, violação de marcas e muitos outros como ameaças, calúnias, difamação, injúria, terrorismo, pornografia infantil, pedofilia e tantos mais.

Publicar ofensas em redes sociais não se confunde com o direito à liberdade de expressão. A falsa sensação de anonimato tem levedo centenas de internautas a publicar conteúdos ofensivos de todo tipo para milhares de pessoas, famosas ou não.

Portanto, quando se trata de liberdade de expressão na internet, deve-se levar em consideração o potencial lesivo que esta nova plataforma trouxe para as manifestações da liberdade, uma vez que uma simples opinião pode ser entendida como verdade absoluta e esta é passível de gerar danos difíceis de serem reparados.

O “*cyberbullying*” é um exemplo. Considerado o “*bullying*” virtual, geralmente é praticado nas redes sociais e representa uma forma de intimidação, humilhação e até mesmo violência física praticada contra alguém. Por vir caracterizado em palavras, fotos, discursos, que depreciam um indivíduo, é considerado assédio moral e tem impactos danosos na vida da pessoa ofendida.

A maior dificuldade para combater esses crimes é a falta de leis e punições eficientes em diversos países na luta contra os transgressores, frente à vasta variedade deles. Porém, todas as pessoas que são atingidas podem recorrer à Justiça para garantir o seu direito de reparação. Apesar de não estar num estágio ideal, a legislação tem avançado com textos específicos para cada propósito.

A defesa é que os bens jurídicos (tudo aquilo que é objeto do Direito) são os mesmos tanto no mundo real como no virtual. Ao se tratar de crimes eletrônicos, há apenas uma mudança de meio. Ou seja, se uma ação for caracterizada como crime ou infração, mesmo sendo praticada na Internet, ela está sujeita às penas impostas pela lei.

Um avanço na luta contra os crimes eletrônicos veio com o Marco Civil da Internet (Lei 12.965/2014 da Presidência da República), sancionado em 2014 e regulou os direitos e deveres dos internautas. Ter uma lei que garanta direitos e deveres no ambiente virtual foi um passo importante, e culturalmente relevante para o país, uma vez que trouxe à tona questões sobre privacidade e proteção das pessoas na Internet que, por consequência, levou a sociedade a se preocupar com o assunto.

Algumas leis surgiram de acordo com as demandas da sociedade, a exemplo da Lei 12.737 de 2012 da Presidência da República, também conhecida como Lei Carolina Dieckmann, por ter sido criada após o vazamento de imagens íntimas da atriz em 2012.

Esta lei tipifica como crime a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita e imputa a penalidade de três meses a um ano de detenção, além da multa.

Apesar de ganhar espaço na mídia com o caso da atriz, o texto da Lei 12.737/12 já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela internet.

É interessante ressaltar que essa lei coloca na mesma condição de crime aquele que reduz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática de cibercrimes.

Outro exemplo nesse sentido é a Lei do *Bullying* (Lei 13.185/15), que traz medidas específicas inclusive para o *cyberbullying.* A lei determina que escolas, clubes e agremiações

assegurem medidas de conscientização, prevenção e combate à violência, e que criem meios de intimidar sistematicamente a prática do *bullying.*

A Lei 13.663/2018 veio para reforçar a regulamentação anterior de Combate ao *Bullying* (Lei 13.185/2015) com foco na conscientização e prevenção do *bullying*. A lei institui o Programa de Combate à Intimidação Sistemática, no qual exige que as escolas promovam medidas de conscientização e combate a todos os tipos de violência.

3 Educação Digital

A Internet revolucionou o mundo e a educação. O uso das tecnologias trouxe grandes avanços e foi determinante para o sistema social, econômico e educacional. Nasce a Sociedade da Informação. Termo oriundo do século XX.

O uso de tecnologias na escola mais que uma realidade, constitui uma necessidade. Sua utilização como instrumento de ensino trouxe à educação mudanças estruturais e funcionais, além de um duplo desafio: o social, referente à formação e o pedagógico, no sentido de facilitar o acesso aos conteúdos. (Lopes, 2004).

Portanto, educação digital é um dos novos papéis da escola na Sociedade da Informação. Não basta apenas colocar o equipamento na escola e "treinar" o estudante. A escola deve considerar a formação humana e que tipo de cidadãos ela quer conceber.

Para isso, a escola precisa conscientizar o estudante sobre cidadania, ética, propriedade intelectual, privacidade e segurança virtual, preparando indivíduos adaptáveis e criativos que lidam facilmente com a rapidez na fluência de informações, mas, principalmente, cidadãos digitais éticos para um novo mercado de trabalho cujas exigências tendem a ser cada vez maiores.

Não é novidade que na internet veicula uma infinidade de informações. Porém, nem toda informação é conhecimento, mas podem ser transformadas se formalmente organizadas em conteúdo escolar. Diante da facilidade e ampliação no acesso às informações, cabe à escola o papel de orientar os jovens sobre como utilizar tais informações para que se transformem em conhecimento. (Jordão, 2009, p. 1).

Além disso, sendo a internet livre, é necessária, aos jovens e às crianças que ainda estão em formação, orientação para saberem selecionar informações que possam ser úteis e relevantes para eles.

Da mesma forma, a escola deve ter atenção quanto aos problemas com crimes virtuais. Se a escola oferece a acesso à Internet, cabe a ela também a responsabilização por todo acesso realizado dentro de seu espaço, uma vez que é dela a responsabilidade da orientação de uso.

Questões como assédio digital, conteúdos inapropriados a menores, desinformação sobre as consequências legais do mau uso da Internet, crimes cometidos sob a falsa

impressão de anonimato, inabilidade de pensamento crítico quanto a informações falsas e verdadeiras disponíveis na rede, plágio, pirataria, e até uso indevido da marca da instituição são alguns temas que a escola precisa desenvolver com seus estudantes para minimizar esses riscos.

Conforme dispõe o Estatuto da Criança e do Adolescente (ECA), em seu artigo 241:

> Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
> Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.
> § 1° Incorre na mesma pena quem:
> I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
> II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
> III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.

Em meio aos riscos, a escola deve refletir se já se dedicou a conferir o conteúdo ao qual expões aos estudantes; se os laboratórios de informática devem ser ou não bloqueados; se a escola precisa incentivar o uso de redes sociais; se está expondo seus estudantes menores de idade a conteúdos inapropriados; se algum tipo de acesso liberado leva a mensagens convidativas a grupos de sexo, o que, dependendo do caso, pode caracterizar crime de pornografia infantil ou exploração sexual; dentre vários outros questionamentos.

Enfim, a escola precisa abrir um espaço de reflexão sobre os perigos aos quais os estudantes estão sujeitos na internet. A partir daí, terá condições de desenvolver esses temas com seus estudantes, instruindo-os adequadamente quanto às consequências dos crimes virtuais tanto para a vítima quanto para o criminoso, propiciando aos estudantes uma experiência positiva no uso da internet.

3.1 Segurança da Informação: preocupação com a segurança ao longo da história

Desde a mais remota antiguidade, há uma preocupação com as informações e com os conhecimentos atrelados a elas. Egípcios e romanos, por exemplo, deixaram registrado na história sua preocupação com o trato de certas informações, especialmente as de valor estratégico e comercial.

Desde então, o ser humano vem buscando controlar as informações que julga serem importantes. Essa atenção especial pode ser observada no processo de escrita de alguns povos. Conforme relaciona Schneier (2001), na antiga China, a própria linguagem escrita era usada como uma forma de criptografia na medida em que somente as classes superiores podiam aprender a ler e a escrever. Assim, a escrita foi uma das várias formas utilizadas pelos antigos de proteger e, ao mesmo tempo, perpetuar o conhecimento.

Ao percorrer a história, percebe-se que nos EUA, a criação de novas tecnologias para tratamento e recuperação da informação foi largamente acelerada em agências de inteligência governamentais durante a Segunda Guerra Mundial (como o *Office of Strategic Service*), sendo essas tecnologias e métodos transpostos para serviços de documentação científica e tecnológica no pós-guerra, como os cartões perfurados para a recuperação da informação por assunto (Shera & Cleveland, 1977).

Tanto para o Estado norte-americano quanto para o soviético (primeiro com a industrialização leninista e posteriormente na guerra fria stalinista) as atividades ligadas à informação passam a ser encaradas como assunto estratégico de Estado.

Questões geopolíticas como o tratamento de informações estratégicas durante a guerra e o lançamento do Sputnik soviético em plena guerra fria, trouxeram à tona o poder político e estratégico da informação, cujas primeiras referências datam do pós-guerra americano.

O tema passou a ter importância no âmbito governamental, levando à criação de agências civis e militares, com o apoio do Congresso, de empresas (IBM, GE, Eastman Kodak etc.) e instituições universitárias.

Com o choque do Sputnik, os EUA se lançaram numa corrida frenética por programas de educação científica e exploração espacial, passando o governo a encarar a informação científica e tecnológica como ponto focal de esforço (Shera & Cleveland, 1977; Bowles, 1999; Hayes, 1999).

Os anos de 1960, nos EUA, marcaram o início da implantação de vários sistemas de informação de âmbito nacional por agências governamentais devotadas à informação científica e tecnológica (NASA, Energia Atômica, Saúde Mental e Medicina) ou serviços especializados (*Science Information Exchange, National Referral Center e Committee on Scientifc and Technical Information*).

Portanto, a questão da segurança como estratégia para a gestão da informação e dos dados organizacionais ganhou ênfase, com a Segunda Guerra Mundial, na medida em que sistemas automáticos, eletromecânicos foram criados tanto para criptografar como para efetuar a criptoanálise e quebrar a codificação (Schneier, 2001). O que, de certo modo, trouxe uma valorização do uso de sistemas de segurança enquanto mecanismos de proteção da informação.

Certo dessa valorização da informação, Deresky (2004) afirma que a “segurança passa a ser crítica na gestão da informação organizacional” e, portanto, constitui recurso de valor e precisa de proteção contra o uso e acesso criminoso.

Mudou-se aqui o foco das organizações que, tradicionalmente, dedicavam grande atenção para com seus ativos tangíveis físicos e financeiros, mas relativamente pouca atenção aos ativos de informação que possuíam. A partir de então, a informação assumiu

importância vital para manutenção dos negócios, marcados pela dinamicidade da economia globalizada e permanentemente *on-line*, de forma que o comprometimento do sistema de informações por problemas de segurança possa vir a causar grandes prejuízos ou mesmo levar a organização à falência (Caruso e Steffen, 1999).

Dessa forma, o tema Segurança da Informação veio se consolidando ao longo do tempo, baseado nas necessidades de cada época, conforme pode ser verificado na Tabela 1, no qual é apresentada uma breve sequência histórica sobre o assunto.

Anos 50 e 60	**1950:** Surge o primeiro padrão de segurança: *Transient Electromagnetic Pulse Surveillance Technology* (Tempest), criado pelo governo dos EUA. • Estudo da escuta de sinais eletromagnéticos que emanam dos computadores. • Vulnerabilidade: obtenção de dados por radiação eletromagnética. **1967:** criação da força-tarefa do DoD (*Departament of Defense* - Departamento de Defesa americano). • Realizou estudos sobre potenciais ameaças a computadores, identificou vulnerabilidades, introduziu métodos de controle de acesso para computadores, sistemas de rede e informações. • O DoD foi um dos órgãos que mais contribuiu para o desenvolvimento de projetos não só na área de segurança como, inclusive, ao que deu origem à internet, o Arpanet. • Contribuiu com o *Security Controls for Computar Systems* (SCCS) e também com o *Trusted Computer System Evaluation Criteria* (TCSEC), mundialmente conhecido como *Orange Book* (Livro Laranja), referência mundial para sistemas seguros de computação. **1969:** Surge a Arpanet (futura internet), rede de computadores descentralizada que conectava: • *Stanford Research Institute*. • *University of Utah*. • *University of California* (Los Angeles). • *University of California* (Santa Barbara).
Anos 70	**1970:** Publicação pelo DoD do *Security Controls for Computar Systems* (SCCS). • SCCS: documento importante na história da segurança de computadores. • Em 1976, esse documento deixou de ser confidencial. • Iniciativas oriundas da parceira do DoD com a indústria:

	• *Tiger teams*.
	• Estudos sobre segurança e desenvolvimento de sistemas operacionais seguros.
	• Surgiram conceitos de segurança como:
	  • Política de segurança.
	  • Modelos de segurança.
	  • Modelos matemáticos de segurança.
	1975: Arpanet completamente funcional; o Unix torna-se o sistema operacional oficial.
	1977: Adotado o *Data Encryption Standard* (DES), padrão de criptografia que durou 20 anos, quando foi substituído pelo MD5 e pelo SHA (algoritmos de hash criptografado).

Anos 80	**1982:** Adotado o protocolo TCP/IP como padrão da Arpanet. **1983:** Lançado o *Trusted Computer System Evaluation Criteria* (TCSEC): • Cognominado *Orange Book*, bíblia do desenvolvimento de sistemas de computação seguros. • Classificação feita em níveis D, C, B e A, na ordem crescente de segurança. **1985:** Primeira vez em que o nome “internet” foi usado para definir a Arpanet. **1986:** *Computer Fraud and Abuse Act*: • Proibia acesso não autorizado a computadores do governo. • Pena pecuniária de cinco mil dólares ou o dobro do valor obtido pelo acesso. • Pena de cinco anos de prisão. **1987:** O departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o CCSC (*Commercial Computer Security Centre*) que dentre suas atribuições tinha a tarefa de criar uma norma de segurança das informações para companhias britânicas que comercializavam produtos para segurança de TI (Tecnologia da Informação) através da criação de critérios para avaliação da segurança. Outro objetivo do CCSC era a criação de um código de segurança para os usuários das informações. **1988:** *Computer Security Act*: • Computador do governo que guardasse dados confidenciais deveria ter plano de segurança para administração e uso do sistema.

	• Exigia que pessoal envolvido recebesse treinamento periódico sobre segurança. • O estudante da Universidade de Cornell escreveu um programa capaz de se autoreplicar e se autopropagar, denominado de "*worm*", justamente por rastejar pela rede. Esse programa explora vulnerabilidades conhecidas dos servidores *sendmail* e *fingerd*. À época, esse programa infectou e indisponibilizou milhares de servidores. • Umas das consequências mais importantes desse ataque (além de Robert T. Morris, o autor do ataque, ter sido condenado por violação do *Computer Fraudand Abuse Act*, por três anos de prisão, 400 horas de serviços comunitários e multa de U$ 10.050,00) foi a criação do *Computer Emergency Response Team* (CERT). • O CERT até hoje é uma das entidades mais importantes na coordenação e informação sobre problemas de segurança. **1989:** O *Commercial Computer Security Centre* publicou a primeira versão do código de segurança, denominado PD0003 - Código para Gerenciamento da Segurança da Informação.
Anos 90	**1995:** O PD0003 foi revisado e publicado como uma norma britânica (BS), a BS7799:1995. **1996:** A BS7799:1995 foi proposta ao ISO (*International Organization for Standardization*) para homologação mas foi rejeitada. Uma Segunda parte desse documento foi criada posteriormente e publicada em novembro de 1997 para consulta pública e avaliação. **1998:** O documento citado no tópico anterior foi publicado como BS7799-2:1998. **1999:** Depois de revisado, esse documento foi publicado junto com a primeira parte em abril de 1999 como BS7799:1999.
Anos 2000	**2000:** O "*The Orange Book*" representou o marco "zero", do qual nasceram vários padrões de segurança, cada qual com a sua filosofia e métodos proprietários, contudo visando uma padronização mundial. Houve um esforço para a construção de uma nova norma, mais atual e que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação. Este esforço foi liderado pela "*International Organization for Standardization* (ISO). No final do ano de 2000, o primeiro resultado desse esforço foi apresentado, que é a norma internacional de Segurança da Informação "ISO/IEC-

	17799:2000", a qual já possui uma versão aplicada aos países de língua portuguesa, denominada "NBR ISO/IEC-17799".
Segurança no Brasil	
Anos 80	**1988:** *The Academic Network at* São Paulo (ANSP), via Fapesp, conectou-se com a internet em Chicago (*Fermi National Laoratory*), nos EUA. **1989:** O Ministério da Ciência e Tecnologia criou a Rede Nacional de Ensino e Pesquisa (RNP), com o objetivo de construir uma infraestrutura de rede internet nacional de âmbito académico.
Anos 90	**1995:** A internet comercial teve início no Brasil. Na mesma época foi criado o Comitê Gestor da Internet no Brasil. A partir disso surgiram: • NIC.BR: Responsável por registros de domínios e associação de endereços IP, também é responsável por receber, revisar e responder à relatos de incidentes de segurança envolvendo a internet brasileira. • O CAIS (Centro de Atendimento a Incidentes de Segurança) atua na detecção, resolução e prevenção de incidentes de segurança na rede académica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes. • Criação de vários Grupos de Respostas a Incidentes de Segurança (CSIRTs) no Brasil.
Anos 2000	**2000:** O Decreto nº 3505, de 13 de junho deste ano instituiu a política de segurança da informação nos órgãos e entidades da administração pública federal. **2001:** A Associação Brasileira de Normas Técnicas (ABNT), que é a responsável pelo Fórum Nacional de Normalização, em abril de 2001, disponibilizou para consulta pública o Projeto 21:204.01-010, que daria origem a norma nacional de segurança da informação: NBR ISO/IEC 17799:2000. A versão final da NBR ISO/IEC-17799, que é uma "tradução literal" da norma Internacional de Segurança da Informação – ISO/IEC-17799:2000, foi homologada em Setembro de 2001 e sua publicação inclui oficialmente o Brasil no conjunto de países que, de certa forma, adotam e apoiam o uso da norma de Segurança da Informação ABNT2001. E esta versão da ISO/IEC 17799 vem sendo utilizada por vários outros países, como é o caso de Portugal, Angola e outros.

Tabela 1 – Histórico de Segurança da Informação no Brasil e no mundo.

Dentre os vários conceitos específicos que se fazem presentes no ambiente da informação, é importante alinhar aqueles que dizem respeito a dados, informação, conhecimento, inteligência, dentre outros.

Para Cardoso (2005), os dados compreendem a classe mais baixa da informação. A informação propriamente dita são os dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível. O conhecimento é a informação cuja relevância, confiabilidade e importância foram avaliadas e é obtido pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação. A inteligência é a informação com oportunidade, ou seja, é a parte do conhecimento que habilita a tomada das melhores decisões.

Embora se reconheça as diferenças acima, para a segurança da informação, todas essas segregações serão incluídas num único contexto: o da informação. Portanto, dados, informação, conhecimento e inteligência, para o cenário de segurança da informação utilizado neste trabalho, devem ser entendidos como informação.

O próprio conceito de sistema de informação tem suas interpretações. Ralph (1998, p.11) diz que "*sistemas de informação é uma série de elementos ou componentes inter-relacionados que coletam (entrada), manipulam e armazenam (processo), e disseminam (saída) os dados e informações e fornecem um mecanismo de feedback*" para atender um objetivo.

A Norma NBR ISO/IEC 27002 trata o conceito de sistema da informação como a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade, minimizar o risco, maximizar o retorno sobre o investimento e as oportunidades de negócio.

Com base nos dois conceitos apresentados, fica evidente que para a tomada de decisões com vista na competitividade, é indispensável um sistema de informações bem estruturado para a utilização da informação com oportunidade. Benefício esse, fruto da inteligência competitiva, processo pelo qual as informações de múltiplas fontes são coletadas, interpretadas e comunicadas a quem precisa delas para decidir (Cardoso, 2005).

Outros conceitos permeiam o tema de segurança da informação. Segundo a NBR ISO/IEC 17799, a segurança de um ambiente é caracterizada pela manutenção de três fatores primordiais: a Confidencialidade, a Integridade e a Disponibilidade das informações críticas.

Albuquerque e Ribeiro (2002) e Krause (1999) reforçam o que diz a NBR ISO/IEC 17799, quando afirmam que há três princípios básicos para garantir a segurança da informação: confidencialidade (a informação somente pode ser acessada por pessoas explicitamente autorizadas), disponibilidade (a informação deve estar disponível no momento em que esta for necessária) e integridade (a informação deve ser recuperada em sua forma original. É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas).

Abaixo são apresentados os conceitos de forma mais detalhada e, adicionalmente, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade, dentre outras, que também podem estar envolvidas neste contexto.

Confidencialidade: é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (NBR ISO/IEC 27002), ou seja, não significa informação isolada ou inacessível a todos, mas sim que a informação somente deve ser acessada a quem lhe é de direito. Ocorre a quebra da confidencialidade da informação ao se permitir que pessoas não autorizadas tenham acesso ao seu conteúdo. A perda da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

Disponibilidade: este conceito tem despertado maior interesse depois que as organizações passaram a depender mais da informação para serem geridas. Afinal, de nada adiantará uma completa infraestrutura tecnológica, com recursos que garantam a integridade e confidencialidade das informações, se quando for preciso acessá-la, a informação não estiver disponível. A disponibilidade, portanto, é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002). Ocorre a quebra da disponibilidade quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito e do armazenamento da informação.

Integridade: diferente do que possa parecer, o conceito de integridade está ligado ao estado da informação no momento de sua geração e resgate. Ela estará íntegra se em tempo de resgate, estiver fiel ao estado original. A Integridade não se prende ao conteúdo, que pode estar errado, mas a variações e alterações entre o processo de geração e o de resgate. É a garantia da exatidão e completeza da informação e dos métodos de processamento (NBR ISO/IEC 27002). Garantir a integridade é permitir que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente. Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua condição original. Contribuem para a perda da integridade: as inserções, substituições ou exclusões de parte do conteúdo da informação; as alterações nos seus elementos de suporte, que podem ocorrer quando são realizadas alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

O item integridade não pode ser confundido com confiabilidade do conteúdo (significado) da informação. Uma informação pode ser imprecisa, mas deve permanecer íntegra (não sofrer alterações por pessoas não autorizadas). Alguns autores defendem que

para que uma informação seja considera segura, o sistema que o administra ainda deve respeitar os seguintes critérios:

Autenticidade: define-se pela veracidade do emissor e receptor das informações trocadas. É a garantia de que a informação é oriunda da fonte que lhe é atribuída e elaborada por quem tem autoridade para tal.

Confiabilidade: é a garantia de que a informação é confiável, oriunda de uma fonte autêntica e que expressa uma mensagem verdadeira. A autenticidade e confiabilidade estão interligadas. A primeira diz respeito à idoneidade da fonte e a segunda ao seu conteúdo. A avaliação da fonte para a sua autenticidade pode ser feita com relação à sua idoneidade, como, por exemplo: completamente idônea, regularmente idônea, inidônea e cuja idoneidade não se pode avaliar. E a avaliação da confiabilidade pode ser feita com relação ao seu conteúdo, como, por exemplo: confirmação por outras fontes, por ser verdadeira, duvidosa ou improvável.

Não repúdio (ou Irretratabilidade): trata-se da garantia de que o emissor de algum dado ou informação ou o autor de alguma ação sobre a informação não possa posteriormente negar que tenha enviado ou alterado alguma informação. Ou seja, é a propriedade que garante a impossibilidade de negar (no sentido de dizer que não foi feito) a autoria em relação a uma transação anteriormente realizada.

Responsabilidade: é a coparticipação de responsabilidades por todos os que produzem, manuseiam, transportam e descartam a informação, seus sistemas e redes de trabalho.

Para ficar mais claro, pode-se, até aqui, dizer, resumidamente, que a autenticidade do emissor é a garantia de que quem se apresenta como remetente é realmente quem diz ser. A confiabilidade é a garantia de que a informação está completa e igual à sua forma original quando do envio pelo remetente, e expressa uma verdade. O não repúdio é a garantia de que o emissor ou receptor não tem como alegar que a comunicação não ocorreu, e a responsabilidade diz respeito aos deveres e proibições entre remetente e destinatário.

Todavia, outros critérios também são considerados, como:

Legalidade: Garante a legalidade (jurídica) da informação; a aderência de um sistema à legislação; e as características das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação nacional ou internacional vigente.

Privacidade: Foge do aspecto de confidencialidade, pois uma informação pode ser considerada confidencial, mas não privada. Uma informação privada deve poder ser vista / lida/alterada somente pelo seu dono. Garante ainda, que a informação não será disponibilizada para outras pessoas (neste caso é atribuído o caráter de confidencialidade à

informação). É a capacidade de um usuário realizar ações em um sistema sem que seja identificado.

Auditoria: Rastreabilidade dos diversos passos de um negócio ou processo, identificando os participantes, os locais e horários de cada etapa. A auditoria aumenta a credibilidade da empresa e é responsável pela adequação da empresa às políticas legais e internas.

A todas estas ponderações acerca de critérios para a segurança da informação soma-se outra como estratégia de gestão da informação: a veracidade. Isto é, a informação deve estar calcada em acontecimentos verídicos ou argumentos lógicos compatíveis com a necessidade da organização. Nesse sentido, não basta que a informação seja autêntica, pois sua fonte pode ser desonesta.

Portanto, não basta a confiabilidade, mas também deve existir veracidade. A combinação em proporções apropriadas dos itens confidencialidade, disponibilidade e integridade facilitam o suporte para que as empresas alcancem seus objetivos, pois seus sistemas de informação serão mais confiáveis.

A segurança passa, assim, a ser uma estratégia de gestão da informação aplicável a toda a organização. A veracidade da informação é um critério a ser contemplado nos sistemas de segurança para que se possa fomentar uma gestão da informação estratégica para toda a instituição.

Antigamente, a atenção sobre a segurança da informação estava focada na tecnologia. Hoje, o desafio é construir uma relação de confiabilidade com clientes e parceiros. Conforme Rezende e Abreu (2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório.

Neste contexto, a segurança visa também a aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática e viabilizando o uso de aplicações de missão crítica.

Outros conceitos recorrentes e permeiam o universo de Segurança da Informação:

Ativo: qualquer coisa que manipule direta ou indiretamente uma informação. A NBR/ISO/IEC 13335-1:2004 trata a informação como “um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para organização e consequentemente necessita ser adequadamente protegido”. Portanto, um ativo é qualquer coisa que tenha valor para a organização.

Vulnerabilidade: tem-se por “vulnerável” um ambiente que não fornece a garantia adequada à informação no que diz respeito à sua segurança. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, o CERT, vulnerabilidade é uma

falha em software ou sistema operacional que reflete na violação da segurança quando explorada por um atacante.

Ameaça: algo que possa provocar danos à segurança da informação, prejudicar as ações da organização e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade. Define-se ameaça por qualquer fato que possa ir contra os princípios da tríade CID (confidencialidade, integridade e disponibilidade) em um sistema de informação. Podem ser acidentais ou propositais. As acidentais são aquelas que acontecem por forças da natureza, falhas de software, hardware ou operação, erros humanos ou erros de infraestrutura. Já as ameaças propositais são aquelas oriundas de espionagem, ações humanas propositais ou ataques.

Risco: é a probabilidade de uma ameaça acontecer e o dano que este pode causar. A ideia de risco está diretamente associada à definição de ameaça. Risco é a possibilidade de determinada ameaça se concretizar em algo que comprometa a informação por meio de uma vulnerabilidade. Risco = Probabilidade x Impacto, ou seja, um risco existe somente se a probabilidade de uma vulnerabilidade ser explorada resultar no impacto sobre a segurança da informação. Devido a isso, um risco é classificado de acordo com os três seguintes fatores: grau de importância da vulnerabilidade, probabilidade de exploração dessa vulnerabilidade e o impacto causado devido aos dois outros fatores.

Incidente: qualquer fato inesperado quer seja ele confirmado ou sob suspeita que possa oferecer ameaça à segurança da informação. Segundo CERT.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores. Em geral, toda situação onde uma informação está sob risco é considerada um incidente de segurança.

É indiscutível, portanto, que algumas informações são centrais para a organização e sua divulgação, parcial ou total, pode acarretar repercussões cuja complexidade pode ser pouco ou nada administrável pela organização. Uma informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.

Entretanto, cabe ressaltar que nem toda informação é crucial ou essencial a ponto de merecer cuidados e investimentos especiais.

Assim, é necessário um esforço para uma correta classificação dos dados para que se proteja o que de fato é importante e não se gaste nem esforços nem recursos financeiros preservando informações que não são cruciais para a instituição. Uma vez classificadas, as informações consideradas importantes precisam ser protegidas.

A classificação da informação contribui para a manutenção das principais características da informação (confidencialidade, integridade, disponibilidade, autenticidade e não repúdio). A NBR ISO 27002 não estabelece classificação para as informações, apenas

recomenda que a informação seja classificada considerando-se o seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Verifica-se que é mais comum a classificação da informação quanto ao sigilo; contudo, esta pode ser efetuada com base em outros critérios. Boran (1996), Wadlow (2000) e Abreu (2001) classificam a informação em níveis de prioridade, de acordo com a necessidade de cada instituição, bem como observando a importância da classe de informação para a manutenção das atividades da organização. Dessa forma, segundo eles, a informação pode ser classificada como:

Pública: Informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da organização e cuja integridade não é vital.

Interna: O acesso livre a este tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital.

Confidencial: Informação restrita aos limites da instituição, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.

Secreta: Informação crítica para as atividades da instituição, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia. Independente da relevância ou do tipo da informação, a gestão dos dados organizacionais é estratégica porque possibilita a tomada de decisões em qualquer âmbito institucional.

Já Beal (2005) classifica os dados de forma a atender aos requisitos de confidencialidade, integridade e disponibilidade.

Para ele, dentro dos requisitos de confidencialidade, a informação pode ser confidencial cuja divulgação para pessoas não autorizadas pode causar danos graves à organização; reservada: aquelas que devem ser de conhecimento restrito e cuja revelação não autorizada pode frustrar o alcance de objetivos e metas; e pública: as consideradas de livre acesso.

No que tange aos requisitos de disponibilidade, Beal (2005) orienta que a informação deve ser classificada de acordo com o impacto que a sua falta pode provocar para a empresa, classificando-as por tempo de recuperação em: curto, médio, sem exigência e com exigência (sazonalidade).

Para os requisitos de integridade, Beal (2005) classifica as informações em alta, média e baixa exigência de integridade. Também apresenta a classificação de acordo com requisitos de autenticidade, classificando-as quanto à exigência da verificação da autenticidade ou não, a exemplo do uso de senha para acesso a um sistema de informação.

Em outra linha, Toigo (2003) classifica as informações em crítica, vital, sensível e não sensível com base no grau de importância destas para os principais processos de negócios e o custo para a recuperação das informações no caso da ocorrência de um evento ou desastre.

Crítica: informações que devem ser mantidas por razões legais, para uso nos processos-chave do negócio, ou para uma mínima restauração aceitável nos níveis de trabalho em um evento ou desastre.

Vital: informações que devem ser mantidas para uso nos processos normais, e que representam um investimento substancial de recursos da companhia, que podem dificultar ou impossibilitar a sua recuperação, mas que podem não ser necessárias numa situação de recuperação de desastre. Informações que necessitam de sigilo especial podem ser incluídas nessa categoria.

Sensível: informações necessárias às operações normais, mas para os quais existem fornecimentos alternativos disponíveis em um evento de perda. Informações que podem ser reconstruídas rapidamente, por completo, mas que possuem algum custo.

Não crítica: informações que podem ser reconstruídas facilmente com custo mínimo, ou cópias de dados críticos, vitais e sensíveis, que não necessitem de pré-requisitos de proteção.

Outro esquema de classificação pode ser feito considerando os níveis estratégico, tático e operacional da organização. Essa opção pode levar em conta que as informações do nível estratégico sejam classificadas como confidenciais (críticas ou vitais), as do nível tático como restritas (sensíveis), e as do nível operacional como sensível (algumas) e públicas ou ostensivas (não críticas).

O Decreto Federal nº 4.553/2002 disciplina, no âmbito da administração pública federal, a salvaguarda de dados, informações, documentos e materiais sigilosos, estabelece em seu art. 2º, que são considerados sigilosos os dados ou informações cujo conhecimento irrestrito ou divulgação possa acarretar qualquer risco para a segurança da sociedade e do Estado, bem como aqueles necessários ao resguardo da inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas, e o seu acesso é restrito e condicionado à necessidade de conhecer.

No Art. 5º desse decreto as informações são classificadas quanto ao grau de sigilo em quatro categorias:

Ultrassecretos: aqueles cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado;

Secretos: aqueles cujo conhecimento não autorizado possa causar dano grave à segurança da sociedade e do estado;

Confidenciais: aqueles que, no interesse do poder executivo e das partes, devam ser de conhecimento restrito, e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado; e

Reservados: aqueles cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

De modo geral e com base nas linhas apresentadas, o objetivo da classificação da informação é possibilitar um nível adequado de proteção, no qual os requisitos fundamentais estabelecidos pela organização para a segurança das informações sejam preservados durante o seu ciclo de vida.

Por essa especificidade, a classificação da informação pode variar de organização para organização, seja pública ou privada, uma vez que cada uma define a linha de classificação a ser adotada e como suas informações devem ser protegidas.

3.2 Política de Segurança da Informação

É primordial que a informação seja protegida de maneira profissional, a partir de um processo organizacional de segurança da informação que estabelece, dentre outros elementos, as regras para a utilização da informação.

Para que o processo em questão seja desenvolvido, implantado e mantido, é necessário que exista uma estruturação de como este ocorrerá, devendo ser similar tanto para as informações físicas quanto para as lógicas.

Com essa preocupação, a *International Standartization Organization* (ISO) publicou uma norma internacional para garantir a segurança das informações nas instituições. Essa norma foi resultado do esforço que remonta a 1987, quando o departamento de comércio e indústria do Reino Unido (DTI) criou um centro de segurança de informações, o *Commercial Computer Security Centre* (CCSC).

O CCSC tinha como uma de suas atribuições criar uma norma de segurança das informações para companhias britânicas que comercializavam produtos para segurança de TI (Tecnologia da Informação) por meio da criação de critérios para avaliação da segurança (SOLMS, 1998). Além disso, cabia a ele a criação de um código de segurança para os usuários das informações.

Cumprindo seu papel, foi publicada em 1989 a primeira versão do código de segurança, denominado PD0003 - Código para Gerenciamento da Segurança da Informação. Esse código foi revisado e publicado como uma norma britânica (BS), a BS7799 em 1995 e, desde então, sofreu uma série de atualizações.

Em 1996, a *International Standartization Organization* recebeu a norma para homologação, porém ela foi rejeitada (Hefferan, 2000). Posteriormente, uma segunda parte

desse documento foi criada e, em novembro de 1997, foi publicada para consulta pública e avaliação.

A norma BS7799-2 foi publicada em 1998 e após sua revisão, teve sua primeira parte publicada em abril de 1999 como BS7799:1999 (Hefferan, 2000). Ainda em 1998 a lei britânica, denominada “Ato de Proteção de Dados”, recomendou a aplicação da norma na Inglaterra, o que só se concretizou em 1º de março de 2000.

Em outubro de 2000, na reunião do comitê da ISO em Tóquio, a norma foi votada e aprovada pela maioria dos representantes. Em dezembro deste mesmo ano, a norma foi homologada como ISO/IEC 17799:2000.

O objetivo fundamental da norma ISO e da norma brasileira (ABNT), nela baseada, é assegurar a continuidade dos serviços e minimizar o impacto de incidentes de segurança. E define segurança da Informação como uma proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades.

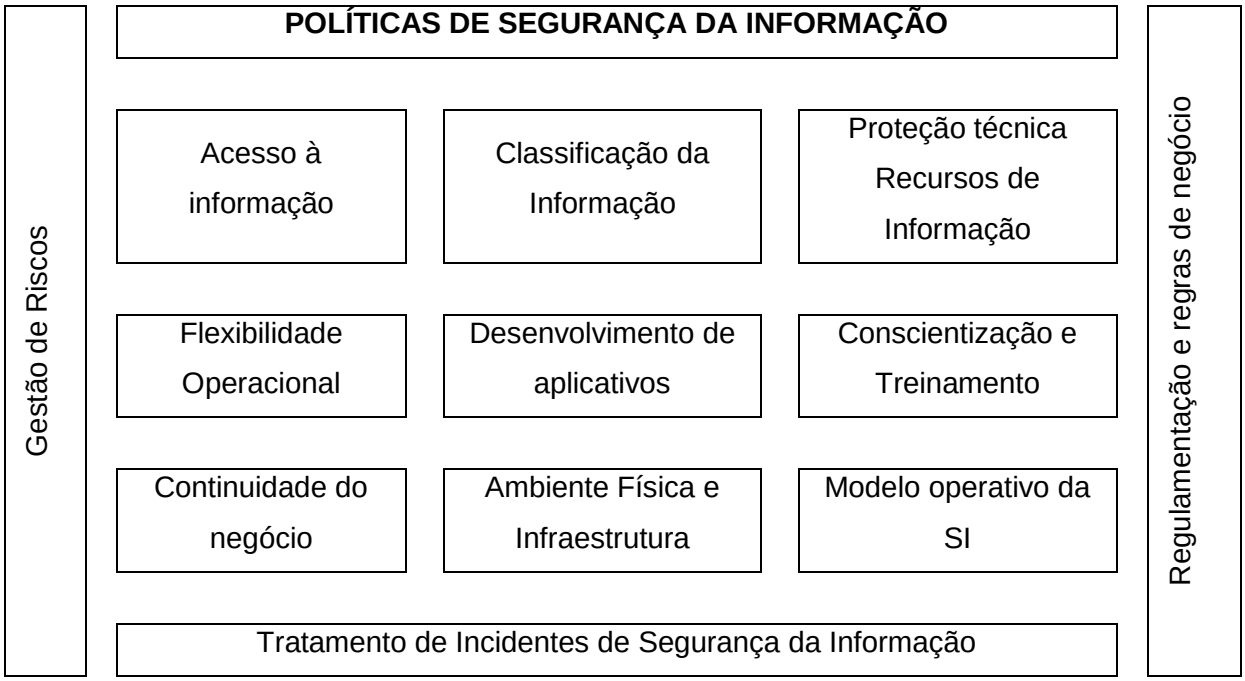
A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos: confidencialidade, integridade e disponibilidade, conforme já citados e conceituados no item 3.1 deste documento. A preservação desses atributos constitui o paradigma básico da Norma Internacional para Gerenciamento da Segurança da Informação, a ISO17799 e de toda a ciência da Segurança da Informação.

A ISO17799 é bem abrangente e contempla a maioria, se não todos, os aspectos da segurança da informação, passando por termos e definições, política de segurança, segurança organizacional, classificação e controle dos ativos de informação, segurança em pessoas, segurança ambiental e física, gerenciamento das operações e comunicações, controle de acesso, desenvolvimento de sistemas e manutenção, gestão de continuidade do negócio, até tratar os aspectos de conformidade.

A ABNT (Associação Brasileira de Normas Técnicas), operando em sintonia com a ISO e atenta às necessidades nacionais quanto à segurança da informação, disponibilizou o projeto na versão brasileira da norma ISO.

Portanto, as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 são a base de Segurança da Informação (SI) e descrevem uma família de controles que devem ser considerados para a existência do Processo Organizacional de Segurança da Informação.

Os controles são agrupados no que se denominam Dimensões da Segurança da Informação, os quais constituem um conjunto de regulamentos referentes a um mesmo tema, a uma mesma dimensão, conforme mostra o Quadro 1:



Quadro 1 – Dimensões da Segurança da Informação

Vale ressaltar que não existe uma dimensão mais importante que a outra. A importância de cada dimensão é igual para todo o processo. Não adianta ter uma dimensão avaliada como excelente e outra como fraca. É muito provável que a proteção da informação será afetada justamente no elemento mais sensível.

A Política de Segurança da Informação, para ser efetiva, deve alcançar todas as dimensões citadas. Esses regulamentos definem como a organização deseja que a informação seja utilizada, controlada, tenha foco também em responsabilização e esteja em conformidade com a legislação e demais regras que a organização necessite cumprir.

Nessa linha, muitas instituições governamentais e não-governamentais vêm trabalhando na definição de normas, padrões e recomendações quanto à segurança da informação nas instituições.

O Tribunal de Contas da União (TCU) do Brasil reconhece a importância da informação quando, no seu Manual de Boas Práticas em Segurança da Informação, declara (Brasil, TCU, 2012, pág.10):

> Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações.

É imperativo, portanto, que os órgãos e entidades da Administração Pública Federal (APF) estabeleçam os seus respectivos planejamentos nas áreas de Segurança da Informação e Comunicação, alinhados ao planejamento estratégico institucional.

Esse documento deve contemplar ações para autodiagnóstico anual, bem como para o desenvolvimento de mecanismos internos de acompanhamento e avaliação sistemática do nível de maturidade, objetivando a excelência dessas áreas e, dentre outros resultados, a prevenção e o combate aos crimes cibernéticos no âmbito do Governo Federal.

O Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União - TCU (Brasil, TCU, 2012) enfatiza que a informação é um elemento crítico, fundamental, essencial e muito valioso, por trazer consigo um valor institucional.

O Decreto Nº 3.505, de 13 de junho de 2000, da Presidência da República, institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal do Brasil, no qual estabelece alguns pressupostos básicos. Alguns deles: assegurar o direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações; criação, desenvolvimento e manutenção de mentalidade de segurança da informação; e a conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Dentre outros conceitos, este decreto dá o seguinte significado à Segurança da Informação:

> Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados ou informações armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças ao seu desenvolvimento.

Ainda segundo o Decreto Nº 3.505/00, um dos objetivos da Política da Segurança da Informação é dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis; bem como, estabelecer normas jurídicas e promover as ações necessárias à efetiva implementação e manutenção da segurança da informação.

O planejamento das ações de Segurança da Informação e Comunicação (SIC) no âmbito da Administração Pública Federal (APF) no Brasil é reforçado pela Norma Complementar nº 02/IN01/DSIC/GSI/PR[1].

1 Norma Complementar nº 2 - Instrução Normativa 01 – Emitida pelo Departamento de Segurança da Informação vinculado ao Gabinete de Segurança Institucional da Presidência da República do Brasil.

A observância desta norma é mandatória e de responsabilidade da Alta Administração da APF, conforme concluiu o Acórdão 1.233/2012-TCU-Plenário em relação aos normativos publicados pelo Gabinete de Segurança Institucional (GSI).

O GSI é um órgão essencial da Presidência da República do Brasil o qual, por meio de seu Departamento de Segurança da Informação e Comunicações (DSIC), é responsável por todas as definições acerca de segurança da informação e comunicações, incluídas aquelas que competem à segurança cibernética e aquelas referentes à segurança das infraestruturas críticas da informação do Estado.

O Departamento de Segurança da Informação e Comunicações (DSIC) avalia tratados, acordos ou atos internacionais relacionados à segurança da informação (em especial, ao tratamento e à troca de informação sigilosa) e assessora o Gabinete de Segurança Institucional da Presidência da República no exercício das funções de autoridade nacional de segurança para o tratamento de informação classificada decorrente de tratados, acordos e atos internacionais.

Portanto, o DSIC planeja, coordena, desenvolve e define normativos e requisitos metodológicos para a implementação de ações de segurança da informação e comunicações, bem como acompanha o desenvolvimento da Política Nacional de Segurança da Informação e promove ações para que esta política seja implementada.

O Departamento de Segurança da Informação e Comunicações (DSIC) determina o cumprimento dessas ações por parte de toda Administração Pública Federal, apoiado pelo Acórdão 3.051/2014-TCU-Plenário, que reforça a necessidade de implementar o planejamento de Segurança da Informação e Comunicação na APF.

Este Instituto Federal Brasileiro atento às determinações do Gabinete da Presidência da República, por meio da Resolução 034 de 2011 aprovou a Política de Segurança da Informação – POSIC no âmbito da instituição.

II – METODOLOGIA

O design metodológico escolhido para a realização do trabalho de pesquisa foi Estudo de Caso, sendo ele realizado a partir de uma abordagem com natureza qualitativa e quantitativa.

A escolha baseou-se no fato de que por meio de um estudo de caso é possível obter um conhecimento amplo e detalhado sobre o objeto de estudo, conforme afirma Yin (2001) que caracteriza este tipo de estudo como uma forma de sistematizar dados e agregar informações, com o maior nível de detalhes possível e em grande volume, referentes ao objeto de estudo sem descaracterizar sua especificidade, seu caráter unitário.

Para Triviños (1987, p.133, grifo do autor), o Estudo de Caso "*é uma categoria de pesquisa cujo objeto é uma unidade que se analisa aprofundadamente*". Todavia, é necessário que essa unidade seja significativa e que faça parte de um todo, para assim propiciar a fundamentação de um julgamento ou propor uma intervenção.

Portanto, o Estudo de Caso permite a reflexão acerca de um determinado cenário e, a partir dele, realizar uma análise crítica para embasar uma tomada de decisão ou apresentar uma proposição. E não existe uma única forma para se conduzir um Estudo de Caso. A depender da proposta da pesquisa, diversas técnicas de investigação podem ser combinadas para esse fim.

Yin (2001) ressalta que apesar de o Estudo de Caso parecer, para muitos, uma pesquisa fácil, ela é extremamente complicada, daí a necessidade da identificação das condições da investigação e do preparo do pesquisador. O Estudo de Caso é uma situação única em que se lida com inúmeras variáveis de interesse e não apenas com pontos de dados, por isso deve seguir um conjunto de procedimentos pré-especificados.

Para assegurar a condição de cientificidade do Estudo de Caso, foram considerados diversos aspectos sensíveis: a seleção do caso, a coleta e o registro de dados, sua análise e a interpretação, bem como o planejamento e o preparo do pesquisador.

Portanto, o estudo apresentado é: Política de segurança da informação e o acesso à internet: o caso de um Instituto Federal Brasileiro que oferece Educação Profissional gratuita para aproximadamente dezenove mil e seiscentos estudantes, na forma de cursos e programas de formação inicial e continuada de trabalhadores (FIC), educação profissional técnica de nível médio e educação profissional tecnológica de graduação e de pós-graduação, articulados a projetos de pesquisa e extensão.

Este Instituto Federal está localizado em uma cidade com dois milhões, quinhentos e setenta mil e cento e sessenta habitantes e possui uma estrutura multicampi que faculta à instituição fixar-se em vários eixos tecnológicos, diversificando seu atendimento, em

conformidade com a vocação econômica das regiões atendidas, conforme tabela apresentada no Anexo II deste documento.

A instituição conta com seiscentos e setenta e quatro[2] docentes no quadro de servidores. Destes, quarenta e seis encontram-se afastados do Instituto por motivos diversos, que vão desde aposentadoria até requisição por outro órgão da Administração Pública Federal do Brasil.

Participantes do estudo

O estudo em questão restringiu-se aos docentes do Instituto Federal em questão.

Instrumentos de recolha de dados

A partir do cenário proposto para o Estudo de Caso, foram utilizados dois instrumentos de recolha de dados: inquérito por questionário limitado aos docentes do Instituto Federal escolhido e análise documental, os quais juntos permitiram uma significativa coleta de dados que serviu de insumo para a análise proposta.

Para Birou (1982), o inquérito por questionário caracteriza-se como uma pesquisa sistemática de dados significativos, realizada da forma mais rigorosa possível, a partir de hipóteses já formuladas, de modo a poder oferecer uma explicação.

O inquérito por questionário é uma técnica de observação não participante que se apoia numa sequência de perguntas ou interrogações escritas que se dirigem a um conjunto de indivíduos (inquiridos), que podem envolver as suas opiniões, as suas representações, as suas crenças ou várias informações factuais sobre eles próprios ou sobre o seu meio.

A escolha de se utilizar o inquérito por questionário justifica-se pelo elevado número de docentes da instituição e pela vasta distribuição geográfica da região deste Instituto Federal. A partir do questionário foi possível alcançar um número expressivo de docentes. Esses mesmos motivos eliminaram a efetividade de um inquérito por entrevista para o público deste estudo de caso.

Já a análise documental foi o outro instrumento de recolha de dados utilizado e é uma técnica decisiva e indispensável para a pesquisa, uma vez que a maior parte das fontes escritas é quase sempre a base do trabalho de investigação, isso porque, segundo Oliveira (2007), os documentos são registros escritos que proporcionam informações em prol da compreensão dos fatos e das relações, ou seja, possibilitam conhecer o período histórico e

2 Dados retirados do SIGEPE (Sistema de Gestão de Pessoas da Administração Pública Federal) e do SUAP (Sistema Unificado da Administração Pública) em 10 de janeiro de 2019. Esses dados foram informados pela Pró-Reitoria de Gestão de Pessoas do órgão. Detectou-se na base, 17 registros redundantes, portanto, há 657 docentes na instituição.

social das ações e reconstruir os fatos e seus antecedentes, pois se constituem em manifestações registradas de aspectos da vida social de determinado grupo.

Dessa forma, a análise documental consiste em identificar, verificar e apreciar os documentos com uma finalidade específica e, nesse caso, preconiza-se a utilização de uma fonte paralela e simultânea de informação para complementar os dados e permitir a contextualização das informações contidas nos documentos. A análise documental deve extrair um reflexo objetivo da fonte original, permitir a localização, identificação, organização e avaliação das informações contidas no documento, além da contextualização dos fatos em determinados momentos (Moreira, 2005).

A pesquisa documental pode se dar a partir de documentos, contemporâneos ou retrospectivos, considerados cientificamente autênticos, por meio de fontes como tabelas estatísticas, cartas, pareceres, fotografias, atas, relatórios, obras originais de qualquer natureza – pintura, escultura, desenho), notas, diários, projetos de lei, ofícios, discursos, mapas, testamentos, inventários, informativos, depoimentos orais e escritos, certidões, correspondência pessoal ou comercial, documentos informativos arquivados em repartições públicas, associações, igrejas, hospitais, sindicatos (Santos, 2000).

Por assim ser, a análise documental constitui uma técnica importante na pesquisa qualitativa, seja complementando informações obtidas por outras técnicas, seja desvelando aspectos novos de um tema ou problema (Ludke & André, 1986).

Para este trabalho foram visitados documentos normativos da Instituição estudada bem como os da Administração Pública Federal; legislações nacionais e internacionais; e muitas bibliografias de estudiosos das áreas de Educação e de Segurança da Informação.

Dessa forma, ao adotar dois instrumentos de recolha de dados – inquérito por questionário e análise documental - foi possível realizar uma coleta de dados mais consistente e abrangente para construção deste projeto permitindo também fazer alguma triangulação de dados.

O questionário aplicado era constituído por dez questões sobre Segurança da informação e todas elas dispunham de um campo de resposta aberta para que o docente, além de escolher um dos itens propostos, pudesse dissertar e deixar sua impressão sobre o assunto, abarcando três perspetivas: opinião, vivência do profissional com o tema e como o docente percebe a atuação da instituição nesse contexto.

Nessa linha, nas questões de um a três, buscou-se a visão do docente sobre Segurança da Informação no contexto geral. Da quarta à sexta questão foram trazidas a vivência do docente em situações que envolveram esse tema, no exercício da profissão; e da sétima à décima pergunta, levantou-se informações sobre como a instituição lida com Segurança da Informação, exclusivamente sob a perspectiva do docente.

Análise de Dados

O público objeto deste estudo foi o corpo docente de um Instituto Federal Brasileiro cujo universo era composto por seiscentos e onze docentes efetivos que estão trabalhando ativamente na instituição, ao qual o questionário foi enviado eletronicamente. Destes, cento e trinta e dois responderam ao formulário, o que corresponde a uma taxa de resposta de 21,6% dos docentes do Universo.

A amostragem foi uma amostra por conveniência constituída, tendo como condição única ser docente do Instituto Federal em estudo e ter respondido por e-mail ao questionário.

Por se tratar de uma pesquisa de natureza qualitativa e também quantitativa, a metodologia de análise de dados combinou uma análise de estatística descritiva, correlações, representações gráficas, entre outras, com análise de conteúdo das questões abertas do questionário, com o objetivo de compreender o significado dos dados coletados, bem como apresentá-los de forma sistematizada.

A análise de dados foi baseada nas recomendações de Bardin (2016) e passou pelas fases de organização da análise, categorização, tratamento dos resultados, inferência e a interpretação dos resultados.

Dessa forma, a análise foi dividida em três partes. A primeira traz a visão estritamente quantitativa; a segunda etapa traz o aspeto qualitativo da análise, no qual foram observadas as respostas descritivas de cada respondente; e na última, um cruzamento dos dados oriundos dos dois tipos de análise realizados.

Os blocos de dados foram agrupados considerando os seguintes aspectos:

- Bloco I – Visão/Opinião do docente sobre Segurança da Informação, de um modo geral.
- Bloco II – Vivência/Experiência do docente em situações que envolveram o tema Segurança da Informação no exercício da profissão.
- Bloco III – Como o instituto lida com Segurança da Informação, sob a perspectiva do docente.

III – ANÁLISE E DISCUSSÃO DOS RESULTADOS

O questionário aplicado constava de dez questões sobre Segurança da informação e todas elas dispunham de campo para que o docente, além de escolher um dos itens propostos, pudesse dissertar e deixar sua impressão sobre o assunto, abarcando três perspectivas: opinião do docente sobre Segurança da Informação, de um modo geral; experiência/vivência em situações que envolveram o tema Segurança da Informação no exercício da profissão; e como o instituto lida com Segurança da Informação, sob a perspectiva do docente.

Análise Quali-Quantitativa

Bloco I (Questões de 1 a 3) – Foco na Visão/Opinião do docente sobre Segurança da Informação, de um modo geral.

Q1. Proteger os estudantes em um ambiente virtual é um papel da instituição de ensino. A partir dessa afirmação, os docentes foram questionados se concordavam que a escola definisse critérios para liberar ou negar acesso a ferramentas disponíveis na internet, efetivar a blindagem de certos sites, dentre outras ações.

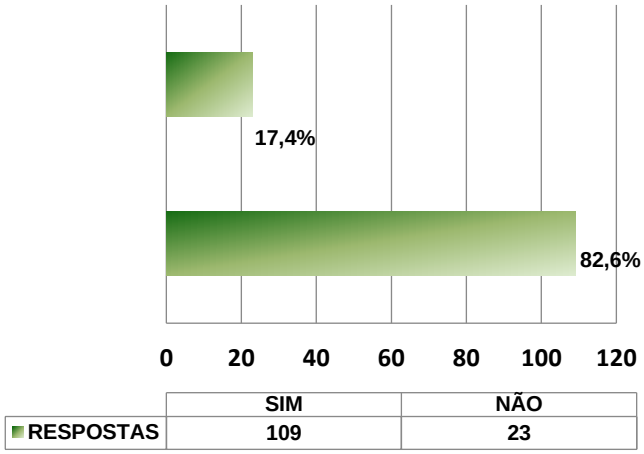
Respostas	Resultados
	A maioria dos docentes concorda com a blindagem de alguns sites. 82,6% dos respondentes entendem que a escola deve estabelecer critérios para navegação na internet, ao passo que apenas 17,4% docentes acreditam que não se devem ter restrições de acesso.

Tabela 2 – Gráfico e resultados referentes à Q1 do questionário.

Análise dos Resultados

Verificou-se que 82,6% dos docentes que responderam “Sim” concordam que a escola estabeleça critérios para navegação na internet e, portanto, que a blindagem de alguns sites se faz necessária.

Mesmo a maioria concordando com o controle de acesso, o motivo exposto não foi único. Por meio da análise das justificativas na perspectiva da resposta “**Sim**”, foi possível

perceber que a preocupação/visão dos docentes girava em torno de alguns temas recorrentes.

Depois de compiladas, as justificativas dos respondentes que optaram pela resposta "Sim", foram classificadas em quatorze temas, conforme apresentado no Gráfico 1.

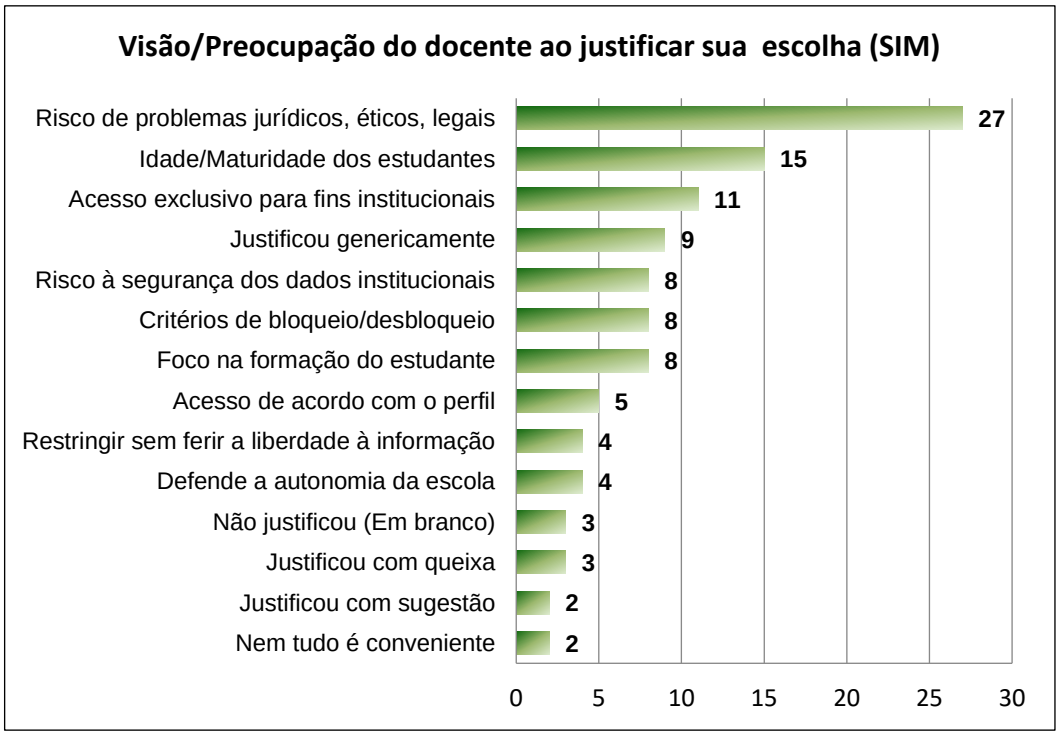


Gráfico 1 – Visão/Preocupação do docente ao justificar sua escolha (SIM)

A partir dos dados apontados pelo Gráfico 1, observa-se que 2,75% dos docentes que responderam "Sim" não apresentaram justificativa para a resposta dada. Como todos os campos do formulário eram obrigatórios, os respondentes preencheram apenas com caracteres especiais (-). Portanto, essas respostas só foram consideradas estatisticamente e classificadas como "***Não justificou*** (***Em branco)***".

Dos docentes que responderam "Sim", 8,25% das justificativas não apresentavam a real visão/preocupação do docente e, ou por serem muito amplas ou pouco elucidativas, foram classificadas como "***Justificou Genericamente***". Seguem alguns exemplos[3] deste tipo de resposta: "*É necessário.*", "*Incontestável.*" "*extremamente necessário*", "*por aí*".

Outros docentes justificaram sua resposta apresentando ***queixas e/ou sugestões*** sobre o assunto. Adicionadas, estas justificativas corresponderam a 4,58% das respostas dos docentes que responderam "Sim". Como exemplo de uma resposta destas tem-se a resposta de um docente que afirma ser dever da instituição de ensino proteger seus estudantes, porém, para ele faltam informação e formação sobre o tema segurança da informação:

[3] As respostas trazidas para o texto estão aqui apresentadas exatamente como foram redigidas, respeitando toda a forma de expressão linguística do respondente. Para melhor identificá-las, estas estão entre aspas ("") e com formatação em itálico.

"*É importante colocar esse ponto como* ***dever da instituição de ensino****. Porém, na minha prática docente, observo que a limitação de acesso dos estudantes está muito mais direcionada a um bloqueio de acesso à páginas consideradas exclusivas para o entretenimento, por exemplo. Não posso afirmar com certeza que todos os campi tenham clareza acerca da proteção dos estudantes nos ambientes virtuais. Falta mais formação e informação a respeito*." docente A

Obtiveram o mesmo percentual aquelas justificativas cuja preocupação do docente girou em torno da ***restrição de acesso às informações com base no nível/perfil do usuário***. Ex.: "*Acho que poderiam haver níveis de acesso. Menores de idade / adultos. Ou algo do tipo*." docente B

Apenas 1,83% dos docentes que responderam "Sim" entenderam que nem todo acesso é **conveniente**, uma vez que nem tudo contribui para o crescimento do estudante, como se pode ver numa das respostas apresentadas: "*Tudo me é permitido, mas nem tudo me convém*!"

A preocupação com a ***liberdade à informação*** foi justificação por 3,67% dos docentes que responderam "Sim". Estes docentes querem certo grau de restrição, mas, ao mesmo tempo, não querem perder a liberdade à informação:

> Sim, é importante que haja limitações relacionadas ao que já está previsto na lei, e que não sejam feitas restrições ou censuras para além do que é considerado crime. É muito complexo definir o que deve e o que não deve ser "próprio para a instituição", sendo que maiores restrições podem implicar em censura prévia, ferindo a liberdade à informação. docente C

Outros 3,67% dos respondentes que responderam "Sim" entendem que cabe à gestão de topo da instituição definir os critérios de restrição de acesso, por acreditarem na ***autonomia da escola***: "*A decisão deve ser do grupo gestor, conselhos ou colegiados que tenham esta atribuição*". docente D

O percentual de 7,34% foi encontrado para três diferentes grupos de respostas dos docentes que responderam "Sim". O primeiro está relacionado com a preocupação dos docentes quanto à segurança dos dados institucionais, o segundo quanto à formação do estudante e o terceiro, traz em voga a efetividade do controle de acesso e a importância da flexibilização dos acessos restritos.

Juntos, os três grupos de justificativas, representam 22% das respostas.

A Tabela 3 apresenta um exemplo de justificativa dada pelos docentes para cada uma das perspectivas por eles apontadas ao responderem que concordam que a instituição deve estabelecer políticas de controle de acesso à informação.

Grupos de justificativas apresentadas pelos docentes que responderam "Sim" ao Controle de Acesso			
Visão do Docente:	**Segurança dos dados institucionais**	**Perspectiva pedagógica voltada para formação do estudante**	**Controle de acesso efetivo e com flexibilização**
Resposta do Docente:	*"... penso que a instituição deve se previnir em relação a sites que possam facilitar/ prejudicar a segurança da informação e prejudicar os equipamentos."* docente E	*"Esse tipo de restrição deve fazer parte da formação do discente."* docente F	*"Com flexibilidade e critérios para liberação de acesso, acredito que as ações de blindagem e segurança sejam primordiais."* docente G
(*) Cada grupo de justificativa corresponde a 7,34% das respostas dos docentes			

Tabela 3 – Grupos de justificativas apresentadas pelos docentes que responderam "Sim" à Q1 e que representam cada um dos grupos, 7,34% das respostas.

A preocupação com a finalidade do acesso à internet foi encontrada na justificativa de 10% dos docentes que responderam "Sim". Para estes, o acesso à internet deve ser voltado apenas para ***fins educacionais***.

Para alguns o acesso livre à internet, ao invés de ajudar faz é atrapalhar os estudantes que, de fato, desejam fazer um trabalho de pesquisa. Portanto, defendem que não há necessidade de navegar em sites que não agreguem na formação do estudante. Segue uma resposta que caracteriza essa visão dos docentes: "*De modo que sejam usados estes recursos somente para fins pedagógicos e não de ócio*." docente H

A ***idade e a maturidade dos estudantes*** frente ao vasto conteúdo disponível na internet foram a segunda maior preocupação apresentada nas justificativas dos docentes que responderam "Sim". Segundo eles, é importante que se estabeleça critérios de navegabilidade para esse público: "*O estudante pode não ter maturidade para o acesso de determinados sites, além do que, se forem menores de idade, a responsabilidade é da instituição*." Foi a afirmação do docente I

A maior preocupação de 24,77% dos docentes que se mostraram favoráveis ao estabelecimento de restrições de acesso à internet, está voltada para o ***risco de problemas futuros sejam eles de esfera legal, ética ou jurídica***.

Isso porque muitos docentes entendem que, enquanto educadores, são responsáveis pelos estudantes dentro do ambiente escolar. Além disso, acesso a conteúdos que trazem temas como pornografia, racismo, homofobia, intolerância, dentre outros que implicam em infrações legais, devem ser acompanhados de perto e só realizados para fins

estritamente de pesquisa e educacional. Nunca para fomentar ou disseminar o assunto enquanto prática discriminatória.

Outra preocupação dos docentes quanto à abordagem dos assuntos descritos no parágrafo acima é a faixa etária e a maturidade do estudante que terá acesso a esse tipo de conteúdo. Mais uma vez ressalta a responsabilidade da escola em promover um acesso consciente e adequado para o público. Portanto, os docentes reforçam que esse acesso não deve ser livre. Deve ser controlado e supervisionado pelos docentes, como refere o docente J:

> Embora a Internet seja a fonte de informação mais utilizada na atualidade e embora o uso de dispositivos eletrônicos na escola seja de fundamental importância para a aprendizagem no século XXI, acredito que seja necessário a utilização de critérios para acesso às ferramentas disponíveis na Internet para proteção dos estudantes e dos servidores em geral, especialmente ferramentas que possam levar à pornografia, estimular a violência, entre outros.

Abaixo segue um quadro resumo com o percentual das diversas perspectivas de alguns dos participantes do estudo ao se posicionarem favoráveis às restrições de acesso dentro da instituição.

Principais justificações dos docentes por concordarem com a existência de controles de acesso à internet na instituição	**Percentagem (%)**
Risco de problemas futuros sejam eles de esfera legal, ética ou jurídica.	**24,7**
Idade e a maturidade dos estudantes.	**13,7**
O acesso à internet deve ser voltado apenas para fins educacionais.	**9,6**
É necessário um controle efetivo e flexível.	**7,3**
Processo de formação do estudante.	**7,3**
Segurança dos dados institucionais.	**7,3**
À alta gestão da instituição deve ter autonomia para definir os critérios de restrição de acesso.	**3,7**
Preocupação com a liberdade à informação.	**3,7**
Nem todo acesso é conveniente.	**1,8**
Restrição de acesso às informações com base no nível/perfil do usuário.	**4,8**
Queixas e/ou sugestões.	**4,8**
Justificou genericamente.	**8,3**
Não justificou (Em branco).	**2,8**

Quadro 2 – Principais justificações participantes que concordam com as restrições de acesso à internet na instituição

Como não houve unanimidade nas respostas, a visão dos 17,4% dos docentes que discordaram das restrições de acesso à internet também foi analisada e buscou-se enquadrá-las de forma similar aos que responderam sim. Isso porque foi possível identificar que havia justificativas comuns nas respostas contrárias dos docentes, o que acaba por se tornar

interessante, pois o mesmo argumento tanto serve para fundamentar o "sim" como o "não" a existência de uma política de restrições.

Relativamente aos docentes que manifestaram a sua opinião contrária ao estabelecimento de restrições de acesso à internet por parte da instituição, o Gráfico 2 mostra o percentual de respondentes para cada grupo de justificativas apresentadas.

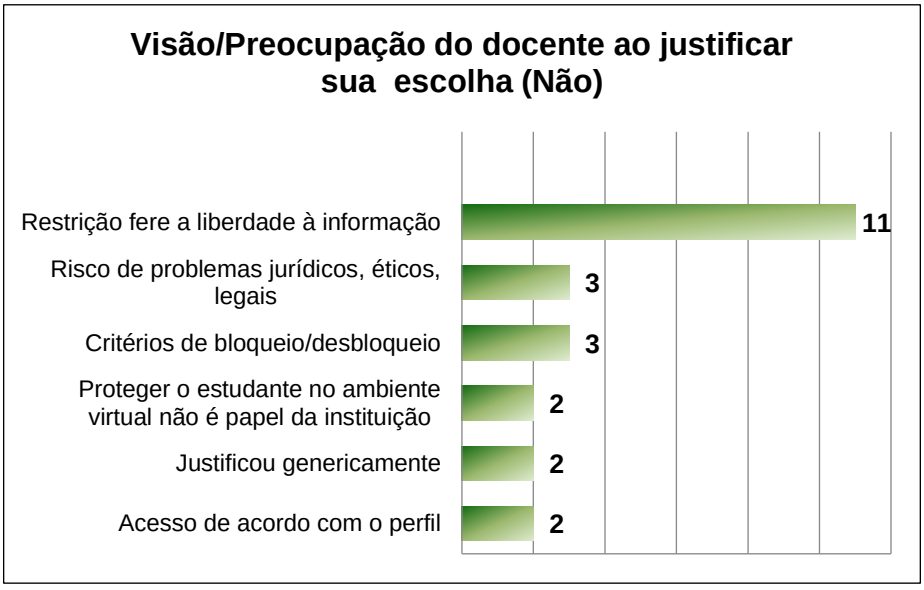


Gráfico 2 – Visão/Preocupação do docente ao justificar sua escolha (NÃO)

Questões como problemas futuros, critérios de bloqueio e de desbloqueio, liberdade à informação e níveis de acesso foram os temas recorrentes nas respostas.

Embora alguns docentes tenham defendido que não se deve ter bloqueios de acesso, os próprios abriram uma exceção para sites que trazem temas como racismo, homofobia, entre outros. Infere-se que, para estes, o bloqueio é necessário em algumas situações, como refere o docente F: "*Não deve haver bloqueio, com exceção do sites racistas, homofóbicos"*

Na mesma linha de pensamento que a anterior, há docentes que por mais que dissessem que não concordavam com restrições de acesso, ao justificarem argumentavam que elas deviam sim existir, mas que deveriam ser acompanhadas das condições de uso para cada perfil de acesso, é o exemplo da resposta do docente K:

> Escolas são também instituições de pesquisa, assim o controle da internet não pode ser único e generalizado para todo o seu público, há que se ter perfis e o controle deve ser definido por perfis, havendo perfis que necessitam de acesso irrestrito, sendo cada um responsável por seus atos. No caso de inimputáveis, os mecanismos de controle podem ser mais rígidos.

Outros docentes que responderam "Não" discordam dos bloqueios por entenderem que a proibição não é educativa e que o importante é educar os estudantes, criar neles uma consciência crítica para que tenham condições de fazer um uso responsável da internet e das ferramentas de Tecnologia da Informação: "*Acredito que o caminho seja discutir com os*

estudantes sobre aspectos benéficos/maléficos dos conteúdos disponíveis, blindar não gera senso crítico.” docente L

Houve também a defesa do livre acesso à informação como direito à cidadania e por entender que a censura não é viável no ambiente de ensino, como refere o docente M: “*A liberdade de conteúdo deve ser um valor de cidadania*”.

Os estudantes, para alguns docentes que responderam “Não”, devem ser estimulados a usar a internet para realizar pesquisas relacionadas aos temas das aulas. O bloqueio cria nos estudantes a necessidade de burlar as regras. Mais uma vez, o importante é preparar o estudante para o uso da internet, como refere o docente N:

> É impossível filtrar todo tipo de informação. O mais importante é educar os estudantes. A proibição por si só não educa. Deve-se explicar por que não se deve acessar determinados conteúdos o que desencadeia um processo educacional e as chances de sucesso serão provavelmente maiores. A proibição leva à burla, estudantes com bom conhecimento de informática podem burlar os mecanismos de proibição. Ademais, o importante é estimular os estudantes a pesquisar temas relacionados às aulas e isso deve ser instigado, a curiosidade aguçada. A internet é aliada e não deve ser uma inimiga.

Além disso, alguns docentes que responderam “Não” argumentaram que a restrição de acesso tende a proibir situações que sequer se transformaram em um problema. Fazendo com que o impedimento de acesso torna-se, ele mesmo, o problema a ser evitado, como menciona docente O: “*Vejo que muitas vezes a segurança proíbe algo que nem mesmo chegou a ser um problema, e a restrição passa a ser um problema quando se quer fazer algo legítimo mas com a política de segurança fica impedido*.”

Um ponto a comentar é a resposta de dois dos docentes que optaram pelo "Não" como resposta. A partir da justificativa por eles apresentada, não é possível saber se os docentes concordam ou discordam das restrições de acesso. O que eles são categóricos em afirmar é que são contrários à afirmação do enunciado da questão, que diz: “*Proteger os estudantes em um ambiente virtual é um papel da instituição de ensino*.”

Ou seja, para esses docentes, não cabe à instituição de ensino proteger os estudantes no ambiente virtual, como afirma o docente P: “*Proteger os estudantes em um ambiente virtual NÃO é um papel da instituição de ensino*”.

Principais justificações dos docentes por discordarem das restrições de acesso à internet na instituição	**Percentagem (%)**
Restrições de acesso ferem o direito à liberdade à informação.	47,8
Só deve haver restrições de acesso aos sites que trazem tema como racismo, homofobia, e similares.	13,0
Devem ser estabelecidos critérios de desbloqueio para sítios bloqueados.	13.0
Não é papel da instituição de ensino proteger os estudantes em ambiente virtual.	8,7
O controle de acesso deve ser estabelecido de acordo com o perfil dos usuários.	8,7
Justificou genericamente.	8,7

Quadro 3 – Principais justificações dos docentes que discordam das restrições de acesso à internet

Interessante observar que, com exceção da visão de que não é papel da escola proteger os estudantes no ambiente virtual, as preocupações apresentadas pelos docentes que discordam das restrições de acesso, enquadram-se nos mesmos temas daqueles que concordam.

A Tabela 4 mostra a relação entre a quantidade de justificativas similares apresentadas em respostas opostas.

	SIM	NÃO	TOTAL
Critérios de bloqueio/desbloqueio	08	03	**11**
Liberdade à informação	04	11	**15**
Acesso de acordo com o perfil	05	02	**07**
Risco de problemas jurídicos, éticos, legais	27	03	**30**
Justificou genericamente	09	02	**11**

Tabela 4 – Relação entre a quantidade de justificativas similares mesmo em respostas opostas

Quando agrupadas as cento e trinta e duas justificativas de acordo com os temas, tem-se o seguinte cenário:

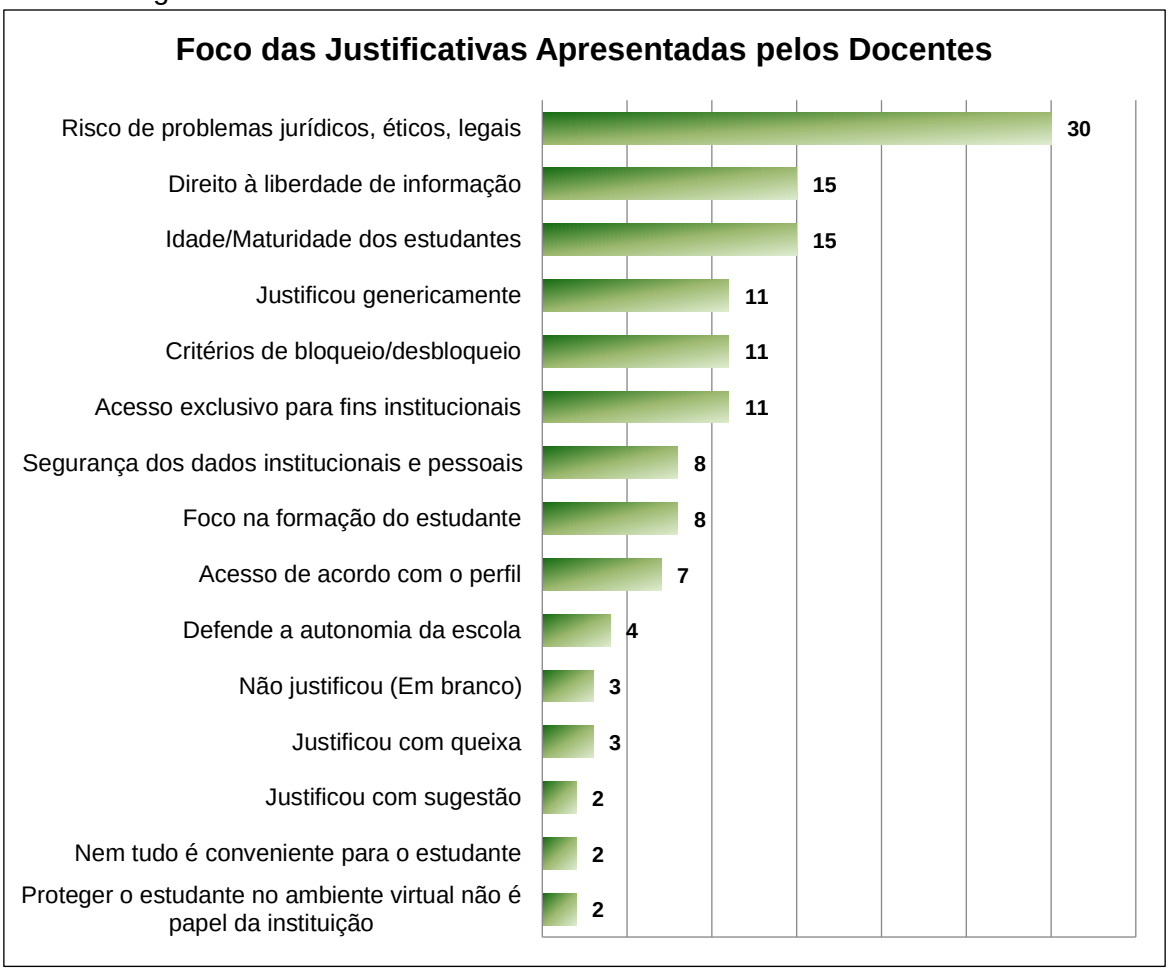


Gráfico 3 – Foco das Justificativas Apresentadas pelos Docentes

Algumas considerações:

Embora o índice de justificativas em branco tenha sido baixo, aquelas genéricas e/ou que apenas reafirmavam o enunciado da questão 1 corresponderam a 8,3% do total de

respostas dos docentes. Para a maioria dos docentes, proteger os estudantes no ambiente virtual é papel da instituição. As poucas queixas (2,3%) apresentadas pelos docentes não estavam voltadas para as restrições de acesso, mas sim, para a dificuldade de os docentes conseguirem assegurar o correto uso da internet em sala de aula.

As sugestões (1,5%) recebidas traziam a necessidade de participação dos docentes no processo de definição dos critérios de acesso. A autonomia da escola para impor critério de acesso, por ela considerado necessário, é legitimada por apenas 3% dos docentes.

Dentre os respondentes, 5,3% dos docentes acreditam que o critério de acesso à internet deve ser estabelecido de acordo com o perfil do usuário. Entendem que deve haver uma classificação por nível de escolaridade do estudante e que servidores e estudantes devem ter níveis de acesso diferenciados, mas ambos com restrições.

A segurança dos dados tanto institucionais quanto dos estudantes foi considerada por 6,1% dos docentes, por acreditarem que o acesso a um sítio inadequado pode trazer risco de vírus e de outros softwares maliciosos serem instalados nos computadores e consequentemente repassados pela rede, colocando em risco as informações institucionais.

O direito de acesso à informação foi defendido por 11,4% dos docentes. De acordo com o gráfico apresentado, essa motivação dividiu com a preocupação quanto à idade e maturidade do estudante, a segunda posição no *ranking* das justificativas.

Um percentual de 8,3% dos docentes defende que o acesso à internet deve ser exclusivo para fins educacionais e, para garantir essa finalidade, as restrições devem existir.

Um bloqueio efetivo e um processo simplificado de liberação de sites proibidos, quando estes se fizerem necessários para o processo ensino-aprendizagem, foi a justificativa apresentada por 8,3% dos docentes.

É preocupação de 11,4% dos docentes, o papel da instituição de ensino de criar nos estudantes o senso crítico e de torná-los cidadãos conscientes.

A maior preocupação do docente está no risco de a instituição, os docentes ou os estudantes enfrentarem, no futuro, problemas jurídicos, éticos e/ou legais. Essa justificativa foi apresentada por 22,7% dos respondentes.

Resumidamente, seguem as principais visões dos docentes tanto para os favoráveis quanto para os contrários às restrições de acesso à internet.

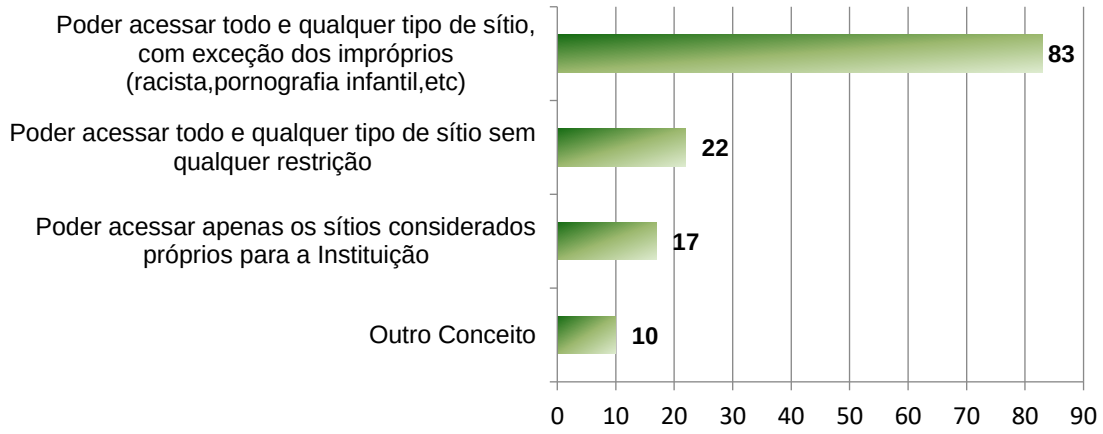
Principais justificativas dos 109 docentes que concordam com a existência de controles de acesso à internet na instituição	**Percentagem (%)**
Risco de problemas futuros sejam eles de esfera legal, ética ou jurídica.	**24,8**
Idade e a maturidade dos estudantes.	**13,8**
O acesso à internet deve ser voltado apenas para fins educacionais.	**9,6**

Principais justificativas dos 23 docentes que discordam das restrições de acesso à internet na instituição	Percentagem (%)
Restrições de acesso ferem o direito à liberdade à informação.	**47,8**
Só deve haver restrições de acesso aos sites que trazem tema como racismo, homofobia, e similares.	**13,0**
Devem ser estabelecidos critérios de desbloqueio para sítios bloqueados.	**13,0**

Quadro 4 – Quadro resumo das principais justificativas dos docentes contrários e favoráveis às restrições de acesso à internet

Q2. Foi perguntado a cada docente acerca de seu entendimento sobre ter livre acesso à informação na internet no âmbito de uma Instituição Federal de Ensino.

Respostas



Resultados

- Dez docentes (7,6%) discordam dos três conceitos de livre acesso à informação na internet no âmbito de uma instituição de ensino federal, apresentados na Questão 2.
- Ter livre acesso à informação não significa poder acessá-la sem restrição é resposta de 12,9% dos docentes.
- Aproximadamente 17% dos docentes, isto é, 22, acreditam que não deve existir nenhuma restrição de acesso à internet.
- A maioria dos docentes, 83 que corresponde a 62,9%, considera que sítios com teor racista e pornográfico, por exemplo, devem ser bloqueados.

Tabela 5 – Gráfico e resultados sobre a visão do docente sobre o livre acesso à informação na internet no âmbito de uma Instituição Federal de Ensino.

Análise dos Resultados

Item a) Navegar na internet podendo acessar todo e qualquer tipo de sítio, com exceção daqueles de temas impróprios, a exemplo dos de cunho racista, de pornografia infantil, dentre outros do tipo, foi a resposta escolhida pela maioria dos docentes (62,9%).

As justificativas apresentadas foram diversas para essa resposta. Passaram desde a defesa da liberdade à informação até a preocupação com questões legais, como pode ser observado no Gráfico 4.

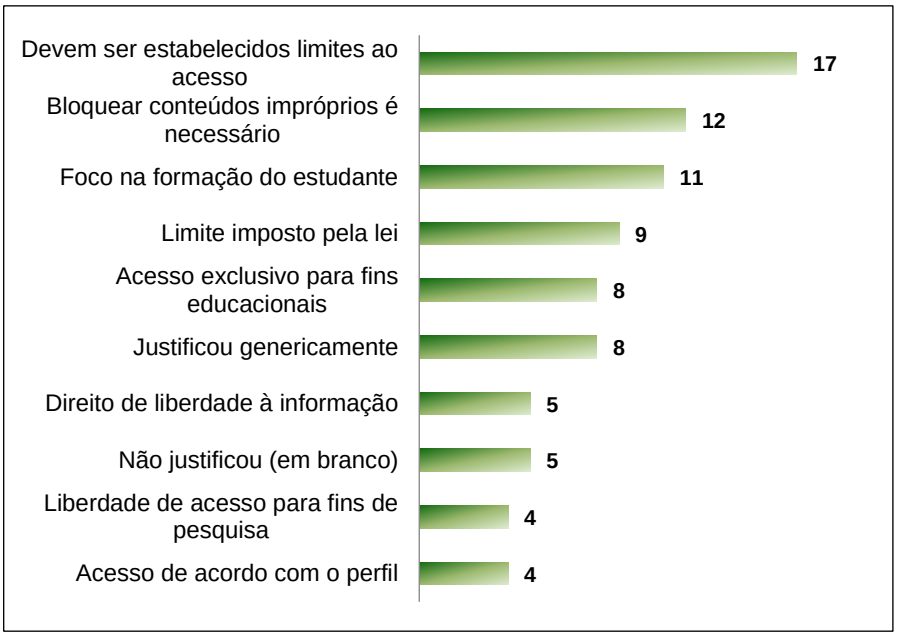


Gráfico 4 – Justificativas apresentadas pelos docentes quanto ao livre acesso à informação na internet no âmbito de uma Instituição Federal de Ensino.

Das justificativas apresentadas para o conceito de livre acesso como sendo "navegar na internet podendo acessar todo e qualquer tipo de sítio, com exceção daqueles de temas impróprios, a exemplo dos de cunho racista, de pornografia infantil, dentre outros do tipo", 20,5% das respostas estavam relacionadas à definição de limite de acesso. Para esse grupo de docente, o conceito de livre acesso à internet implica em não se ter restrições. Todavia, na prática, consideram importante impor limites a esse acesso, porque este não pode ser realizado de forma inadequada.

Justificam ainda que livre acesso não é sinônimo de propagação de violência e *fakenews*, por exemplo. Portanto, os docentes acreditam que deve ter um monitoramento, uma limitação imposta, ainda mais pelo público da instituição. Por outro lado, defendem que devem também existir mecanismos que facilitem o desbloqueio de determinados sites, quando forem utilizados para fins de ensino e de pesquisa. O exemplo a seguir traz a visão do docente Q: *"Penso que devemos ter cuidado com o tipo de informação que está circulando, e definir critérios de acesso a certos sites é uma forma de atenção principalmente por termos estudantes adolescentes."*

Outro grupo de docentes, que corresponde a 14,4% deles, entende que o livre acesso à internet não abarca a liberação de conteúdos impróprios. Nenhum desses docentes trouxe uma nova definição para o termo "impróprio", portanto, limitaram-se ao descrito no item: racismo, pornografia infantil, etc. Como se pode observar na resposta do docente R: *"A instituição é responsável pelo que ela propicia aos estudantes, por essa razão, da mesma*

forma que não deve possuir livros de conteúdos impróprios em sua biblioteca, não deve ter acesso aos mesmos pela internet."

Interessante ressaltar que para alguns docentes que adotam o conceito de que livre acesso é navegar na internet podendo acessar todo e qualquer tipo de sítio, com exceção daqueles de temas impróprios, a exemplo dos de cunho racista, de pornografia infantil, dentre outros do tipo, entendem que tais conteúdos não devem ser acessados por ninguém, conforme diz o docente S: *"Importante restringir esse tipo de site. Nenhuma pessoa deveria acessar tais conteúdos".*

Educar para que os estudantes façam uso consciente da internet é papel da Instituição de Ensino, segundo 13,2% dos docentes que entendem que livre acesso é navegar na internet podendo acessar todo e qualquer tipo de sítio, com exceção daqueles de temas impróprios, a exemplo dos de cunho racista, de pornografia infantil, dentre outros do tipo. Para esse grupo, deve haver o cuidado e a proteção, mas estes não podem atrapalhar o ambiente de pesquisa. O docente tem o papel de ser mediador desse acesso, como menciona T:

> Novamente proteger mas não diminuir o ambiente de pesquisa. Num trabalho sobre racismo por exemplo temos aqui páginas ruins, porém verdadeiras, por isso sou a favor. Mesmo que vejam pessoas mortas, a história da escravidão teve muito disso e nos livros não temos tantas fotos chocantes, como nos filmes que concorrem ao Oscar, como por exemplo "12 anos de escravidão". As vezes eles tem que ver o passado, a verdade contida nele para evitar uma atitude similar no futuro.

A preocupação com as questões legais e com o risco de crimes no ambiente virtual estava presente em 10,8% das justificativas desse grupo de docentes. Segundo eles, os temas tipificados como crime na legislação brasileira devem ser vetados pela instituição uma vez que esse tipo de conteúdo contraria qualquer princípio a ser transmitido em uma instituição de ensino, conforme diz o docente U: *"Os temas impróprios usados são tipificados como crime no código penal brasileiro, diante disso, acredito que uma instituição federal de ensino possa/deva ter vedações mínimas no acesso."*

Outros docentes defendem que o livre acesso seja para conteúdos que agreguem valor à formação do estudante o que, para eles, não é o caso dos sites tidos como impróprios. Portanto, para 9,6% dos docentes, o acesso livre à internet deve ser limitado aos fins estritamente institucionais: "*A informação acessada dentro do ambiente do instituto federal deve ser livre de conteúdos impróprios, já que estes conteúdos não fazem parte do desenvolvimento educacional do estudante."* docente F

A preocupação com a liberdade à informação também foi tema de justificativa de 6% dos docentes. Para eles, é difícil mensurar o "próprio" e o "impróprio" sem correr o risco de cercear o acesso às informações importantes para a formação do estudante e até mesmo de afastar o estudante da escola como justifica o docente A: *"A internet é uma ferramenta fabulosa, limitar demais seu uso vai afastar os estudantes da instituição."*

Houve ainda grupos de docentes que defenderam que o acesso deve ser irrestrito para alguns perfis institucionais (4,8% dos docentes) e os que defenderam que para fins de pesquisa o acesso não deve ser limitado (também 4,8% dos docentes), menciona o docente V: "*Numa escola que incentiva a pesquisa e a extensão, restrições bloqueiam a inteligência e a capacidade de promover mudanças em redes de interesse*".

Item b) Navegar na internet podendo acessar todo e qualquer tipo de sítio, ou seja, sem qualquer restrição, foi a segunda resposta mais escolhida pelos docentes (16,7%).

As justificativas apresentadas por esses docentes não foram muito diferentes umas das outras. Partiram do princípio que o termo livre acesso é sinônimo de acesso sem restrições, mesmo que alguns ainda discordem dessa prática. Para outros, desde que mediado, esse é o melhor contexto para o ambiente de ensino como alude o docente W "*Não acredito que qualquer tipo de a restrição caracterize "liberdade" no sentido pleno. Sendo assim entendo que o acesso sem qualquer restrição com responsabilidade do agente responsável pelos acessos seja a melhor maneira de conceituar livre acesso"*.

Item c) Navegar na internet podendo acessar apenas os sítios considerados próprios para a Instituição, foi a segunda resposta mais escolhida pelos docentes (12,9%).

Neste ponto, as justificativas dos docentes giraram em torno da autonomia da escola, da preocupação com a idade e a maturidade dos estudantes, e do entendimento que os estudantes só precisam acessar conteúdos voltados para fins educacionais e de pesquisa, diz X:

> No âmbito da instituição deveria-se ter sites disponíveis para pesquisa, apenas. Infelizmente, a restrição torna-se necessária, pois estamos lidando com um público com idade inferior à 18 anos, em sua maioria. Se algum crime virtual for cometido através do sinal da Instituição, a própria também responderá.

Item d) Outro conceito (7,6%).

Com exceção de um docente, os demais justificaram sua escolha argumentando que o acesso deve ser ou direcionado a temas próprios para a formação do estudante ou condicionado ao perfil do usuário.

A resposta diferente foi apresentada pelo docente B que trouxe um novo conceito sob o prisma da ética e da cidadania: *"Ter ética para acessar informações de interesse para a pesquisa e a formação cidadã."*

Discussão:

A restrição de acesso é um tema bastante complexo e nada consensual entre os docentes. Enquanto para alguns os limites de acesso não devem ser impostos e sim

construídos, para outras é obrigação da instituição de ensino bloquear conteúdos que, de alguma forma, coloquem em risco a comunidade escolar.

Mesmo para os docentes que defendem o livre acesso, parte deles acredita que algum nível de restrição deve ser imposto. A opção pela restrição de acesso está fortemente ancorada no receio dos docentes quanto à responsabilização da instituição de ensino e, consequentemente deles próprios, em casos de uso indevido da internet.

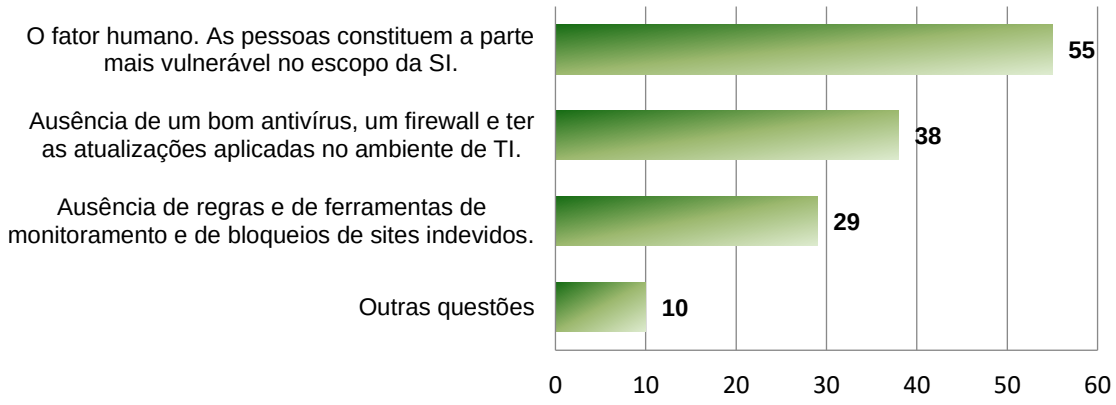
O direito de acesso à informação, enquanto direito fundamental tutelado pelo Estado Democrático de Direito e que garante a cidadania, não foi a maior defesa dos docentes, uma vez que só foi citado em uma das justificativas.

A maior discordância dos docentes quanto às restrições de acesso à internet, não está no cerceamento da informação por si só. Está na dificuldade que estes enfrentam quando necessitam da liberação do acesso aos sites tradicionalmente “bloqueados”.

O nível de maturidade e a idade é um ponto de preocupação seja por conta da responsabilidade ou quanto ao cuidado que têm enquanto responsáveis pela formação dos estudantes, deixando-os aptos ao uso consciente e responsável da internet.

Questão 3 (Q3) - No universo de segurança da informação, o que lhe é mais preocupante?

Respostas



Resultados

- Para a maior parte dos inquiridos (41,7%), o fator humano representa a maior vulnerabilidade em segurança da informação.
- A ausência de equipamentos e software que visam a segurança da informação é a preocupação de 28,8% dos inquiridos.
- Para 22% dos docentes a maior fonte de risco em segurança da informação é a ausência de regras de acesso e de ferramentas de monitoramento do ambiente.
- Outros 7,6% dos docentes defendem que outras questões são mais preocupantes dos que as apresentadas nesta questão.

Tabela 6 – Gráfico e resultados da Q3 sobre a maior preocupação dos docentes no universo de segurança da informação.

Análise dos Resultados

A maioria dos docentes inquiridos (41,7%) atribui ao fator humano o ponto de maior vulnerabilidade quando o assunto é Segurança da Informação.

Na visão dos que assim justificaram sua escolha, o ser humano é a parte mais vulnerável por vários quesitos.

Segundo esse grupo de inquiridos, o ser humano é imprevisível e suas atitudes perfazem a preocupação com segurança. Consideraram também que sempre existirão pessoas mal-intencionadas que farão mau uso do ambiente virtual. Por outro lado, a inabilidade humana de lidar com as ferramentas e com a internet, leva a vulnerabilidades, mesmo que não de forma intencional. Portanto, defendem, também, que são necessárias orientação e formação sobre o assunto, como menciona Y:

> O ser humano, buscando comodidades e facilidades na utilização das TIs sacrifica muitas vezes a segurança para este fim. Aqui no instituto não é diferente, como, por exemplo, professores/servidores informando senha de administrador para os estudantes acessarem um programa com privilégios para executá-lo em sua aula.

Também o inquirido F, e depois o Z referem, respectivamente: "*A ação humana má intencionada quando do acesso e alteração de dados institucionais é o fator mais preocupante quanto à segurança da informação*". "*Se as pessoas não estiverem preparadas e ter conhecimento sobre segurança da informação, de nada adiantará regras e ferramentas*."

A ausência de um bom antivírus, de um firewall e de ter todas as suas atualizações aplicadas no ambiente tecnológico é a preocupação de 28,8% dos docentes. Para estes inquiridos é importante garantir o bom funcionamento da infraestrutura e não comprometer dados relevantes da instituição e as soluções de segurança da informação são fundamentais para disponibilizar um mínimo de credibilidade para a comunidade académica.

Além disso, segundo eles, o fator humano deve ser considerado. E se falhas humanas existem, é interessante que a Instituição além de tratar a temática de segurança, também diminua as possibilidades de risco. "A preservação da informação e das ferramentas da instituição são muito importantes. Então a proteção da produção intelectual da instituição é peça chave para a manutenção do trabalho". É o que afirma o docente C. O inquirido AA diz: "ainda que o órgão tenha uma excelente POSIC ou humanos bem treinados, o mínimo necessário ainda é um antivírus atualizado e um FW".

Para 22% dos docentes, **a ausência de regras e de ferramentas** de monitoramento e de bloqueios de sites indevidos constitui o maior risco à segurança da informação. Esse grupo acredita que políticas de uso adequadas e monitoramento são necessários, visto a capilaridade de uma instituição como esta.

Eles não descartam o fator humano, que também consideram preocupante, mas compreendem que as pessoas podem ser educadas e orientadas com ações contínuas de

conscientização e que o regramento é um pré-requisito para essa ação. Se a instituição não tiver essa preocupação, para eles, será negligente.

Contudo, esse grupo acredita que a construção das regras deve acontecer de forma colaborativa, com a participação de todos os envolvidos dentro da instituição. Abaixo seguem as respostas, na íntegra, dos docentes AB, AC e AD, respectivamente.

> "Infelizmente muitas pessoas só "funcionam" com regras".
> "Por mais que se invista em firewalls e não educação e conscientização, a instituição não pode abrir mão de seu papel normalizador e de intervenção quando anomalias forem detectadas. Isso é negligência"
> "Deve-se, antes de tudo, definir-se critérios, a prioridade deve ser dada ao aspecto formativo. Acredito que deveria ter maior participação dos docentes, visto que a atividade fim, que é a formação do sujeito, deve ser priorizada".

Dentre os 7,6% dos docentes que optaram por "Outras questões" como opção de resposta, assim o fizeram por entenderem que todas as questões anteriores são importantes e complementares. Seguem duas respostas que refletem essa visão: *"todos os itens são importantes em diferentes graus";* docente AE e *"É um tripe das três ações. Nao adianta ter um se nao tem o outro".* docente O

Algumas considerações:

É clara para os docentes a importância de requisitos de segurança da informação. Nenhuma justificativa dada trouxe o aspecto de que essas iniciativas são desnecessárias ou que não constituem ação de valor.

A preocupação com o fator humano foi notória. Mesmo os que não optaram por essa resposta, mencionaram a preocupação com a fragilidade que as pessoas trazem ao processo de segurança da informação.

Outra questão presente nas justificativas é a importância de conhecerem o assunto. O desconhecimento seja do assunto seja das regras é uma grande vulnerabilidade para instituição.

Interessante ressaltar que nenhum docente se manifestou contrário ao uso de normativos sobre Segurança da Informação. Ao contrário. Alguns se mostraram ansiosos por tê-la (conhecê-la e/ou aprendê-la) e outros desejosos de serem partícipes nessa construção.

Bloco II – Vivência/Experiência do docente em situações que envolveram o tema Segurança da Informação no exercício da profissão.

Questão 4 (Q4) - Em algum momento de sua experiência de docente você já foi questionado pelos pais ou pela comunidade se o acesso à internet é restrito ou se é tudo liberado durante as aulas de laboratório?

Quantas vezes o docente foi questionado sobre Segurança da Informação no exercício da profissão										
Quantos docentes foram questionados	111	4	3	2	5	1	1	1	1	3
Número de vezes que o docente foi questionado	0	1	2	3	5	6	7	8	9	10

Tabela 7 - Resultados da Q.4 - Quantas vezes o docente foi questionado sobre a existência de restrição de acesso nas aulas em laboratório de informática

Resultados

- Dos 132 respondentes, apenas 21 (16%) deles foram questionados pela comunidade se o acesso à internet é restrito ou liberado nas aulas em laboratório.
- Apenas 3 (2,3%) deles foram questionados por 10 ou mais vezes sobre o assunto.
- Enquanto que 84% nunca foram questionados a respeito.

Análise dos Resultados

Com base nos dados apresentados, é possível inferir que, de maneira geral, a comunidade académica não cobra dos docentes e nem da instituição de ensino uma postura em relação às condições de acesso à internet, dado que 84% dos respondentes nunca foram questionados a respeito.

Algumas Considerações:

Apesar da questão não exigir uma justificativa para a escolha do docente, 12,8% deles optaram por comentar a resposta. E a partir desses comentários, pode-se ter uma noção da causa da passividade da comunidade quando se trata de políticas de acesso à internet:

- Muitos docentes ministram aula para estudantes adultos;
- Alguns não utilizam laboratórios de internet para ministrar uma aula, seja porque entendem que não precisam deste ambiente seja porque a instituição não disponibiliza nenhum ou uma quantidade insuficiente de espaço para atender a todos os docentes;
- "*A população assistida pelo órgão, em geral, é muito vulnerável social e economicamente, na maioria das vezes não está ciente da existência desse tipo de perigo*". docente D. Se o risco não é conhecido, não há porque existir preocupação;
- A ausência de discussão sobre o assunto na escola;
- Os pais e/ou responsáveis pelos estudantes menores de idade pouco participam da vida escolar desses estudantes ou por confiar nos profissionais de educação ou por imputar essa responsabilidade à escola e ao docente. De uma forma ou

de outra, o fato é que essa postura dos pais aumenta a responsabilidade da instituição de ensino.

Questão 5 (Q5) - Em sua visão e com base em sua experiência como docente, a implementação de regras de controle de acesso à internet ajuda ou confunde a dinamização das aulas?

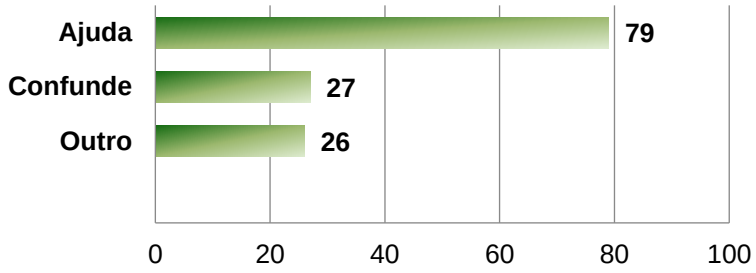
Respostas

Resultados
- Aproximadamente 60% dos docentes afirmam que as regras de controle de acesso à internet ajudam no desenvolvimento das aulas e 20% entendem que as regras trazem confusão. - Cerca de 20% não defendem nenhuma das hipóteses e trazem consigo outra visão.

Tabela 8 – Gráfico e resultados da Q.5 sobre as regras de controle de acesso à internet ajudam ou confundem a dinamização das aulas

Análise dos Resultados

Um percentual significativo dos docentes inquiridos (60%) afirma que as regras de controle de acesso à internet não atrapalham a dinamização das aulas.

Para esse grupo, os controles ajudam a dinâmica das aulas, uma vez que os professores não precisam se preocupar em como os estudantes estão usando a rede de computadores, o qual permite que eles fiquem dedicados ao aprendizado do estudante. Para o docente B: *"É uma preocupação a menos para o docente, assim ele se preocupa com o aprendizado do estudante e não com a navegação indevida em certos sites*."

Esses docentes também afirmam que, com as restrições de acesso, a dispersão dos estudantes diminui ficando eles mais focados nos assuntos abordados em sala de aula. *"Os estudantes não se dispersam com sites de jogos, ou demais sites que não possuem relevância para aquele momento."* docente AF

Além disso, os docentes entendem que os limites fazem parte da formação do estudante e que estes estarão expostos às regras em todo e qualquer ambiente e isso não necessariamente é algo negativo. *"Faz com que o estudante saiba que o mundo possui regras e que regras bem implementadas ajudam a instituição seguir em frente",* essa foi a justificativa do docente AG.

A defesa de participação coletiva na construção das regras e a divulgação desse documento também foi uma das justificativas apresentada pelos docentes. *"Desde que as regras sejam publicitadas, e construídas conjuntamente com os usuários."* docente AH

A argumentação de 20% daqueles que acreditam que as regras confundem a dinamização das aulas está baseada, principalmente, no fato de em algum momento ter enfrentado dificuldade para acessar sites que seriam úteis em sala. A exemplo do que disse o docente AI: *"As regras de controle impedem muitas vezes o andamento da aula. Por exemplo, em uma aula sobre currículo, a ferramenta que seria utilizada foi bloqueada por causa da primeira sílaba da palavra."*

O entendimento de que a educação tem que ser um espaço livre e que a "proibição impede a reflexão" também aparece na justificativa dos docentes. O estudante precisa adquirir autonomia e responsabilidade ao usar a internet. Mas, isso só acontece quando eles, por si mesmos, compreenderem o risco do mau uso desse ambiente, o qual está a sua disposição dentro e fora do ambiente escolar.

> O acesso a internet não é blindado fora da escola, deste modo, o mais importante seria a mediação educativa para que esta prepare futuros cidadãos conscientes e aptos a lidar com situações de violência e abuso que ocorrem tanto no ambiente virtual quanto cotidiano. docente AJ

Da parcela de 19,7% que optou por "outro" como resposta apresentou justificativas em três linhas: a dos que consideram indiferente a existência do controle de acesso à internet; a dos que entendem que tanto ajuda quanto atrapalha; e a dos que entendem que as regras efetivamente atrapalham a dinamização das aulas.

Os que defendem que o controle de acesso é indiferente acreditam que se houver planejamento das aulas, o docente não enfrentará nenhum problema. *"Não interfere. Tudo é possível com um bom planejamento de aula.",* segundo o docente AK.

Para alguns, as regras de controle de acesso podem tanto ajudar quanto confundir a dinamização das aulas, a depender do contexto.

> A instituição de ensino deve ter bem clara a sua função social, ou seja, a que, a quem serve, numa perspectiva de formação. Dessa forma, a definição de valores, marcos teóricos, filosóficos, epistemológicos, dentre outros, é fundamental para a convergência de ações na prática docente. Nesse sentido, a normatização se faz necessária, porém deve ser largamente discutida entre os docentes, o que não ocorre, ficando as decisões, em geral, para os técnicos na área de informática, e estes, a partir de seus próprios valores, decidem sobre o uso da internet, o que muitas vezes atrapalham. docente Q

Apenas dois docentes afirmaram que o controle de acesso atrapalha a dinamização das aulas e não apresentaram uma defesa clara sobre a opinião deles. Um apenas usou a palavra "atrapalha" para justificar sua resposta e o outro disse que "pode atrapalhar sim. Precisamos encontrar um meio termo". docentes AL e AM

Algumas considerações:

Os docentes, em sua maioria, não são contrários às regras por si só. Aliás, assim como o docente AN apoiam-se na ideia de que "*o mundo vive em função de controles*". O que eles não são favoráveis é à forma como as restrições de acesso são definidas.

Por vezes, o regramento não traz consigo a visão pedagógica, tão necessária ao ambiente de ensino. Portanto, faz-se necessário um estudo e um trabalho conjunto entre as equipes técnica e pedagógica para a elaboração dessas normas.

A partir do inquérito por questionário utilizado não se tem elementos para analisar a resposta dos docentes que disseram não ter uma opinião formada sobre o assunto. Essa justificativa pode estar fundamentada em uma série de fatores, como, por exemplo, no desconhecimento do assunto por parte do docente; no fato deste nunca ter sido provocado a pensar nessa questão; na irrelevância do tema, dentre outros. Portanto, para um entendimento claro sobre esse tipo de resposta, far-se-á necessário um estudo futuro.

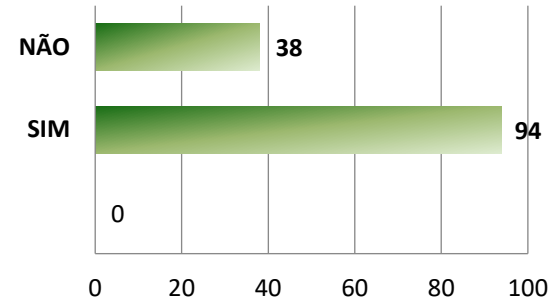
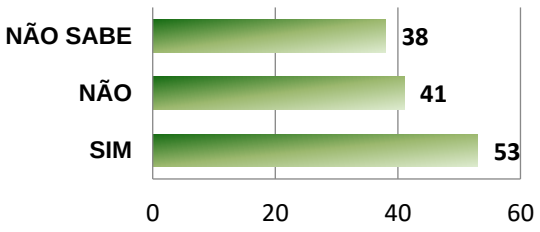
Questão 6A (Q6A) - Enquanto docente que faz uso das tecnologias educacionais, há de sua parte a preocupação quanto aos riscos e aos crimes virtuais que podem ocorrer durante suas aulas?	**Questão 6B (Q6B) -** Você acredita que pode ser responsabilizado numa situação como essa?
Respostas	**Respostas**
	
Resultados	
- Não existe preocupação quanto aos riscos e aos crimes virtuais durante suas aulas para 28,8% dos docentes que entendem que não podem ser responsabilizados, caso estes ocorram. - Dos 71,2% dos docentes que têm essa preocupação, 31,1% deles desconhecem se podem ser responsabilizados numa situação como essa e 40% acreditam que sim.	

Tabela 9 – Gráficos e Resultados da Q.6, itens A e B, sobre se os docentes se preocupam com o risco de crimes virtuais acontecerem em suas aulas e, em caso afirmativo, se consideram que podem ser responsabilizados por isso.

Análise dos Resultados

Mesmo não se preocupando com os riscos de crimes virtuais, os docentes acreditam que possam ser responsabilizados, caso ocorram durante suas aulas?

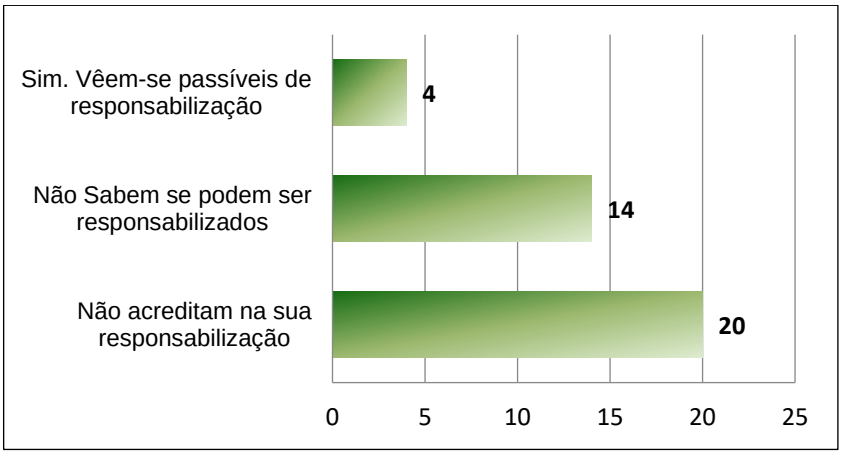


Gráfico 5 – Análise das respostas dos docentes que não se preocupam com o risco de crimes virtuais acontecerem em suas aulas.

Dos 38 que responderam que não se preocupam com o risco de crimes virtuais em suas aulas, 52,6% deles não acreditam que possam ser responsabilizados caso ocorram. São várias as justificativas apresentadas. Esses docentes acreditam que:

- Têm um comportamento relativamente seguro em relação à segurança;
- O professor ensinando um conteúdo não pode ser responsabilizado por uma ação de um estudante que não tem interesse de prestar atenção na aula;
- Não há como vincular um estudante cometendo um crime em sala de aula à responsabilidade do professor;
- As responsabilidades dos docentes sobre as ações dos estudantes também têm limites. O docente não é totalmente responsável pelo discente;
- Falhas de segurança informática não poderão ser imputadas ao professor;
- Cada um é responsável pelo equipamento que usa, portanto, a responsabilidade do crime é de quem infringe a lei;
- A instituição possui uma política de segurança e os usuários são responsáveis pelos seus atos;
- Se a aula é dirigida, os desvios são minimizados.

Alguns docentes disseram não ter conhecimento suficiente sobre o assunto; que não utilizam a internet em sala de aula; e outros afirmaram que não se preocupam mesmo com o tema.

Por trazer uma reflexão bastante pertinente, apresento abaixo a resposta de um docente, exatamente como foi redigida pelo autor:

> Não tenho como monitorar todos os estudantes e preciso confiar na autonomia deles. Se um estudante escrever em seus cadernos mensagens de cunho racista ou nazista durante as minhas aulas, serei responsável pelo conteúdo? Se um estudante trouxer uma arma e atirar em alguém durante a aula, eu serei

> responsável? Não acredito que o mundo virtual seja tão diferente do mundo real. Qualquer crime pode ser cometido em um ambiente escolar e não tenho como desempenhar o papel de agente de segurança ao mesmo tempo em que sou docente. docente O

Essa resposta traz à reflexão o papel do docente em sala de aula e até onde vai a responsabilidade dele frente às atitudes dos estudantes. Para ele a liberdade de acesso, de expressão do estudante não pode ser atrelada à responsabilização do docente.

Já 36,8% não sabem se pode haver responsabilização para o docente. E quando a justificativa é o desconhecimento do tema, não há muito que se falar. Todavia, ressalto duas delas: "*Nem faço ideia de que tipo de risco ou crime virtual existem e nem porque eu poderia ser responsabilizada. Seria bom que isso fosse melhor divulgado para nós docentes*" docente AO

Pode-se entender a partir dessa resposta que os docentes utilizam as tecnologias da informação em suas aulas, mas não dispõem de conhecimento suficiente que lhes dê segurança neste ambiente como diz AP: "*Falta de conhecimento. Gostaria de receber conhecimento nessa área*."

Interessante observar que, existindo desconhecimento do assunto, os docentes estão abertos e até se mostraram desejosos a receberem seja uma capacitação seja uma orientação sobre o tema.

Tem-se ainda a visão de 10,5% dos inquiridos que mesmo não se preocupando com os riscos, acreditam que podem ser responsabilizados caso um crime virtual aconteça durante suas aulas. Essas justificativas trouxeram:

- A incerteza do docente quanto à sua responsabilização: "*Não me preocupo com riscos e crimes durante as aulas em si mas acredito que na eventualidade de algo do tipo acontecer, talvez eu possa ser responsabilizada. Mas não tenho certeza nem saberia dizer em qual medida*" docente J;
- A ausência de reflexão sobre o tema no ambiente escolar: "*nunca parei para refletir sobre essas questões antes*", afirmou o docente AQ;

A conscientização do docente face à sua responsabilidade com a informação em sala de aula: "*Trabalhar com informação exige muita responsabilidade e é importante que haja essa conscientização por parte do corpo docente*" como afirma AR; e o peso da responsabilidade imputada ao docente seja por questões gerenciais, administrativas seja por desconhecimento (ou ausência) de um normativo que explicite até onde vai a responsabilização dos diversos servidores da instituição de ensino, como refere D: "*Porque com certeza a culpa não seria da direção*".

E os docentes que já trazem consigo a preocupação quanto aos riscos de crimes virtuais acontecerem durante suas aulas, será que entendem que a responsabilização pelo crime compete a eles?

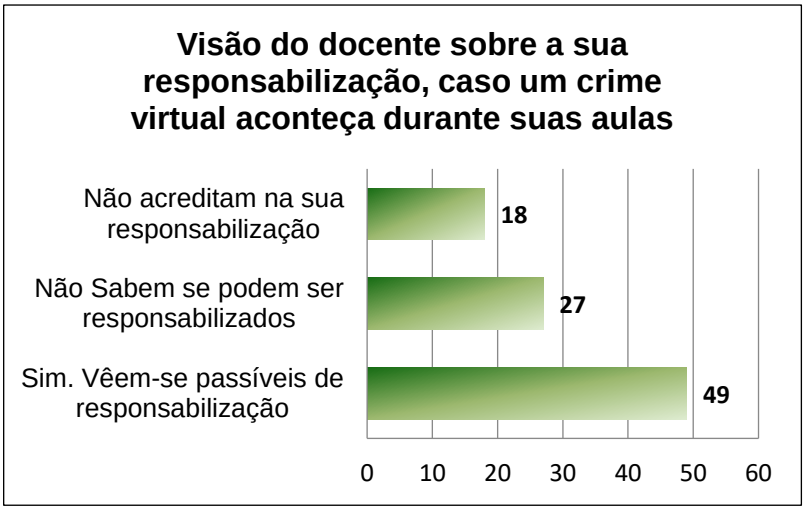


Gráfico 6 – Visão do docente sobre a sua responsabilização, caso um crime virtual aconteça durante suas aulas

Ainda que adicionados o número de docentes que não acreditam na possibilidade de serem responsabilizados (19%) ao número daqueles que desconhecem o assunto (29%), é maior a quantidade daqueles que acreditam em sua responsabilização no caso de crimes virtuais ocorrerem em suas aulas (52%).

As alegações dos 19% que dizem não serem responsáveis pelos crimes cometidos pelos estudantes são diversas. Neste documento são apresentadas algumas que resumem o escopo das alegações, como é o caso da do inquirido AS: "*Pois como professor, meu papel é ensinar e não vigiar os estudantes*."

Os docentes não se vêm como vigilantes e sim, como educadores, uma vez que, na visão deles, não é possível controlar todos os fatores que impeçam os discentes de cometerem algum crime, dentre os diversos crimes virtuais.

Há uma preocupação em orientar e coordenar as atividades de forma a minimizar as possibilidades de que haja ações ilícitas, mas não é possível impedir que isso aconteça. Salvo em casos específicos, onde houver algum incentivo consciente, não veem o porquê de serem responsabilizados por uma atuação criminosa que não cometeram.

Além disso, observam que, para serem responsabilizados, estes devem, primeiro, serem informados sobre o que podem e o que não podem fazer. Julgam ser inadequado serem responsabilizados por algo que sequer conhecem, afirma V:

> A preocupação com a segurança da informação deve ser constante, a não ser que eu tenha sido previamente informado dos cuidados mínimos que deverei ter e/ou ser capacitado para isso, acredito que eu não possa ser responsabilizado por nenhuma imperícia por desconhecimento de uma área que não é a minha.

Já os 52% dos docentes que acreditam que é de sua responsabilidade os crimes cometidos pelos estudantes durante suas aulas, as justificativas apresentadas tinham o viés da proteção do estudante no ambiente institucional. *"Tudo que ocorre dentro do ambiente de*

ensino é de responsabilidade dos gestores e o docente é o gestor da sala de aula" menciona o docente AT.

Esse grupo ainda defende que, entre o cerceamento da informação e o risco de ser responsabilizado por uma conduta ilegal do estudante, os docentes preferem se expor ao risco sob o argumento da tutela da liberdade à informação. *"o acesso irrestrito não pode nos eximir de nossas responsabilidades. Com o acesso irrestrito aumentam nossos riscos e responsabilidades, mas os riscos são necessário, pois o controle limita demasiadamente a atividade docente."* diz o docente L.

O grupo que representa 29% dos docentes que não sabem se podem ser responsabilidades por uma conduta ilegal dos estudantes durante suas aulas alega que não tem conhecimento para discorrer sobre o assunto ou ainda, nunca ter refletido sobre o assunto. "*Não tenho conhecimento, nunca pensei nisso*" docente AU

Apesar de não terem conhecimento sobre o assunto, esse grupo não concorda que o docente seja responsabilizado por uma ação que ele próprio não tenha praticado ou incentivado. "*Os docentes não deveriam ser responsabilizados pelo mal uso de terceiros*", afirma AV.

Discussão:

O risco de crimes virtuais serem praticados durante suas aulas é um fator de preocupação para maior parte dos respondentes, que também acreditam que podem ser responsabilizados caso eles ocorram.

Apesar de o número dos que não se preocupam com crimes virtuais em sala de aula ser idêntico ao daqueles que não sabem se podem ser responsabilizados caso ocorram, não há uma relação direta entre eles.

Tanto para os docentes que se preocupam com a ocorrência de crimes virtuais em sala de aula quanto para aqueles que não têm essa preocupação, há uma parcela desses profissionais que desconhece o assunto e/ou as legislações que tratam o tema.

Ao mesmo tempo em que o docente tem consciência do seu papel enquanto educador e responsável pelo ambiente de sala de aula, ele se sente incapaz de controlar tudo que ocorre nesse espaço de ensino-aprendizagem, principalmente, quando se refere ao ambiente virtual.

Se a responsabilização por todo e qualquer crime ocorrido dentro de sala de aula for imputada ao docente, corre-se o risco destes deixarem de usar as tecnologias da informação, por receio de serem culpados por algo que não detém o poder de controlar em sua totalidade.

Resume bem as considerações apresentadas acima, a resposta transcrita a seguir:

> Sim, mas dentro de um bom senso mínimo, que inclusive acredito existir entre a maioria dos responsáveis, gestores e também no âmbito da justiça. Tentarei explicar meu raciocínio por meio de um exemplo prático. Digamos que durante uma

> aula sob minha responsabilidade em laboratório de informática com uma turma de 40 estudantes um deles, naturalmente desobedecendo minhas orientações enquanto docente, acesse sites impróprios e eventualmente cometa crimes virtuais. Posso ser responsabilizado por esse crime? Tecnicamente sim. Mas, a menos que eu tenha sido comprovadamente muito irresponsável ou displicente (como, por exemplo, proposto uma atividade inapropriada que levou o estudante a agir de tal maneira, ou ainda, ter deixado a turma sem nenhuma supervisão durante a atividade), penso que dificilmente um responsável, gestor ou mesmo a justiça, me responsabilizaria por tal crime. E se algum responsável, gestor ou juiz me responsabilizasse pela atitude desse estudante, estaria fugindo do bom senso e demonstrando total desconhecimento das limitações da realidade da sala-de-aula, caso em que, naturalmente, eu recorreria. O que quero dizer é que o professor não pode ser 100% responsabilizado por tudo que acontece no âmbito de sua aula. Cobrar isso seria uma visão ingênua e injusta sobre nosso trabalho e levaria os professores a, por exemplo, nunca utilizarem o laboratório de informática ou ambientes virtuais de aprendizagem, POR MEDO, uma vez que é impossível ter 100% de controle sobre o que ocorre nesses ambientes. Seria o extremo da ditadura do politicamente correto reinando em nossa sociedade. Mas, naturalmente, o planejamento das atividaes e a postura do professor no uso dessas tecnologias e ambientes deve ser cuidadoso, criterioso, no sentido de oferecer orientação sobre o uso desses instrumentos pelos estudantes, supervisão sobre o que se passa durante as atividades e evitar possíveis problemas. docente AW

Cabe ressaltar que, por mais que a instituição de ensino seja responsável pelo estudante enquanto este estiver sob sua tutela, não foi encontrada no arcabouço legislativo brasileiro uma lei que imputa ao docente, seja total ou parcialmente, a responsabilidade sob os crimes cometidos por seus estudantes durante as aulas, salvo se comprovada a sua efetiva participação.

Todavia, ficou clara a fragilidade do conhecimento dos docentes sobre esse assunto, o que evidencia a necessidade da instituição de trazer esse tema à discussão, não só entre os servidores docentes, mas em todo seu público, servidores técnicos e estudantes.

Bloco III - Como o instituto lida com Segurança da Informação, sob a perspectiva do docente.

Questão 7A (Q7A) - A instituição já lhe ofereceu capacitação sobre o tema Segurança da Informação?

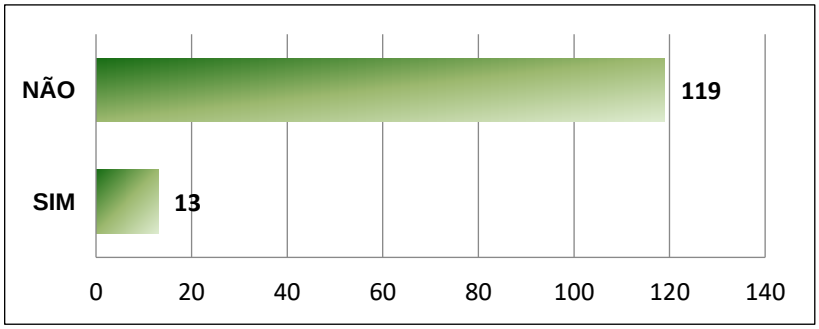


Gráfico 7 – Resposta dos docentes sobre se a instituição já lhe ofereceu capacitação sobre o tema Segurança da Informação

Questão 7B (Q7B) - Por quantas capacitações você já passou sobre Segurança da Informação?

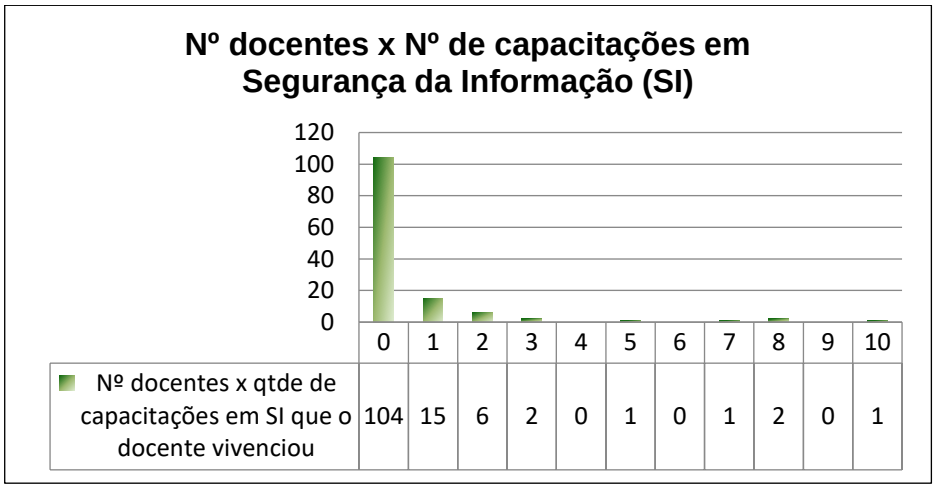


Gráfico 8 – Nº de docentes x Nº de capacitações em Segurança da Informação (SI)

Resultados

- Do total, 90,2% nunca receberam da instituição capacitação sobre o tema Segurança da Informação.
- A instituição capacitou 9,8% dos docentes.

Análise dos Resultados

Dos 119 docentes nunca capacitados pela instituição, apenas 15 deles já tiveram alguma capacitação sobre o assunto, o que equivale a 12,6%.

Dessa forma, 78,8% não tem nenhuma formação em Segurança da Informação.

Dentre os que foram capacitados pela instituição, apenas cinco deles receberam mais de uma formação sobre o tema (quatro receberam duas capacitações e um recebeu cinco capacitações).

Dentre aqueles que não receberam da instituição capacitação sobre segurança da informação, sete deles participaram de uma única capacitação no assunto; quatro deles vivenciaram entre duas e três formações a respeito; três disseram ter passado por sete e/ou oito capacitações; e apenas um afirmou ter se capacitado por dez ou mais vezes neste tema.

De todos que tiveram formação sobre segurança da informação, apenas cinco deles passaram por cinco ou mais capacitações.

O percentual de docentes capacitados em segurança da informação corrobora com a análise das questões anteriores quanto à necessidade de trazer em voga a discussão sobre o tema em todos os fóruns da instituição.

Questão 8 (Q8) - Considera que ter uma Política de Segurança da Informação é importante para o Instituto?

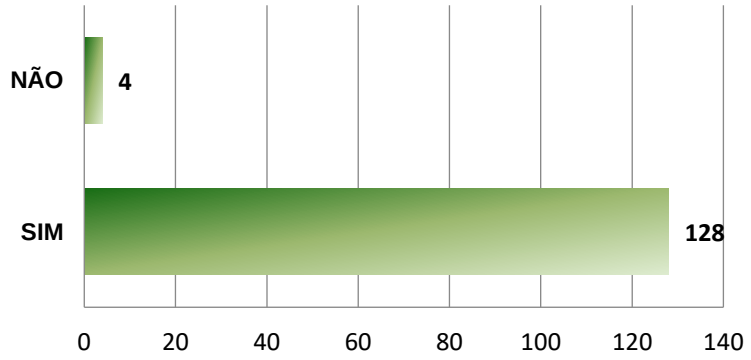
Respostas	Resultados
	Para 97% dos docentes é importante ter uma política de Segurança da Informação na instituição e apenas 3% disseram que não.

Tabela 10 – Gráfico e Resultados da Q.8 que questiona se o docente considera que ter uma Política de Segurança da Informação é importante para o instituto

Análise dos Resultados

Na visão do docente, ter uma Política de Segurança da Informação (PSI) é importante para o Instituto. Essa constatação dá-se pelo fato de que, quando questionados sobre se há importância de uma PSI para o instituto, 97% responderam que sim.

Essa importância passa por diversas vertentes conforme justificativas apresentadas pelos docentes.

Uma delas é que qualquer instituição precisa de uma Política de Segurança da Informação (PSI). "*Qualquer instituição precisa ter segurança da informação para garantir os níveis de sigilo das informações.*" docente AX

Também é dito que a importância da PSI vem da necessidade de se garantir a segurança das informações institucionais. Os docentes consideram que o instituto trabalha com informações críticas que precisam ser protegidas, como dados pessoais de servidores, de estudantes e de pesquisa. *"Informação de um órgão é fundamental para a sua existência, imagem e correto funcionamento. Portanto, a segurança desses dados, tanto internos quanto externos, é primordial."* docente AY

Alguns também trouxeram o viés da conformidade com as leis impostas à Administração Pública Federal. *"É importante porque demonstra que estamos em conformidade com outras leis que tratam sobre o tema e orienta e resguarda a circulação de informações de propriedade do instituto."* docente I

Os docentes também justificaram que a Política de Segurança da Informação (PSI) não pode ser confundida com regras de bloqueio de palavras.

> Bom, não creio que possamos imaginar uma instituição do tamanho do instituto sem um PSI, mas PSI não pode se confundir, nem mesmo interseccionar, com bloqueio por palavras definidas como semanticamente sexuais que impeçam, por exemplo, o acesso a sites cubanos, que terminam com .cu. Esquece-se também

> que a sexualidade é um campo de pesquisa extremamente relevante para a formação cidadã propagada pelo órgão. A propósito, a palavra sexualidade também gera (ou ao menos gerava) bloqueio de sites no instituto. docente L

É interessante ressaltar que, mais uma vez, os docentes defendem a participação desses profissionais na construção da PSI e que o tema Segurança da Informação precisa ser mais debatido na instituição. *"É importante desde que a comunidade académica discuta os princípios dessa política"* docente AZ*; "Acho que precisamos de capacitação, compreender se essa política nos favorece ou se nos deixa mais vulnerável ao ambiente profissional".* docente BA

Os poucos que não consideram importante a instituição ter uma Política de Segurança da Informação argumentaram que esse normativo aumenta a burocracia; que os docentes sofrem pressão para utilizar ambiente tecnológico; e que esta não é uma questão prioritária para a escola. *"mais burocracia" segundo o* docente J*; e BB diz: "Acredito que esse problema apenas existe pois há uma pressão para que os docentes usem essas tecnologias. Entretanto, existem diversas outras questões prioritárias na escola.".*

Algumas considerações:

Embora a Política de Segurança da Informação seja classificada como importante para maior parte dos docentes do Instituto Federal, percebe-se ainda certa resistência de alguns docentes pelo desconhecimento do assunto e/ou pela forma em que o tema é tratado pela instituição.

Capacitação no assunto e participação no processo de construção das políticas institucionais são pontos recorrentes nas justificativas dos docentes.

Questão 9A (Q9A) - Relativamente à Política de Segurança da Informação (PSI) do instituto, indique o seu grau de conhecimento:

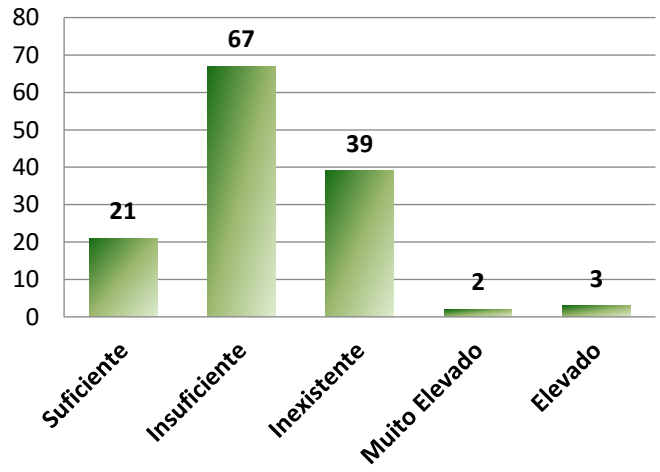
Percentual de Respostas	Resultados
	- A maioria dos docentes, 50,7%, considera ter conhecimento insuficiente sobre a PSI. - Cerca de 30% desconhecem totalmente a Política de Segurança da Informação - PSI. - Outros 15,9% disseram ter conhecimento suficiente sobre o documento. -Dos respondentes, 2,27% consideram ter conhecimento elevado sobre a norma. - Apenas 1,51% dos docentes têm conhecimento muito elevado sobre a PSI.

Tabela 11 – Gráfico e resultados da Q.9A que questiona o grau de conhecimento do docente acerca da Política de Segurança da Informação (PSI) do instituto

Questão 9B (Q9B) - Indique a (s) razão (ões) para sua resposta.

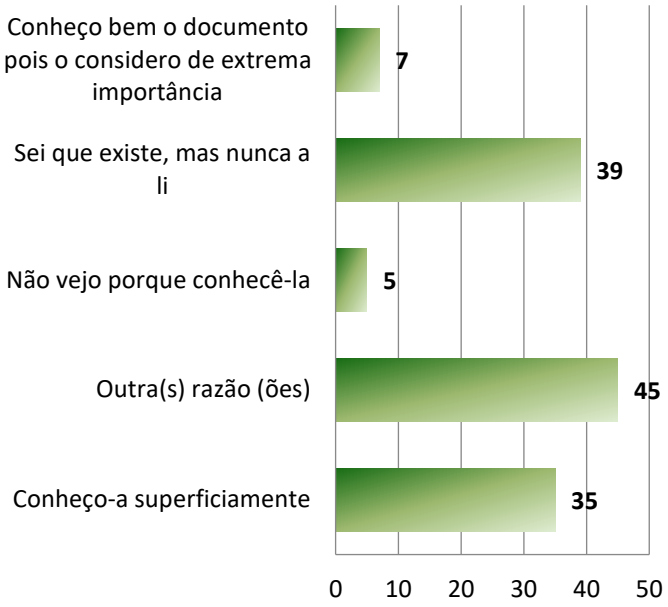
Respostas e Resultados	
- O item “conhecer bem a PSI” foi escolhido por 5% dos docentes. - Cerca de 30% dos docentes sabe que existe uma PSI na instituição, mas nunca a leram. - Os que conhecem superficialmente a política, representam 27% dos docentes. - Alguns docentes (4%) não se interessam em conhecer a POSIC. - Outras razões foram apresentadas por 34% dos docentes.	

Tabela 12 – Gráfico e resultados da Q.9B que apresenta as razões apontados pelo docente para o grau de conhecimento por ele apontado sobre a PSI

Análise dos Resultados

A primeira análise realizada foi relacionar o tipo de justificativa apresentada pelo docente (Q9B) para cada grau de conhecimento apresentado (Q9A).

Ao realizar esse cruzamento de dados, obtiveram-se as seguintes correlações:

- Dos dois docentes que afirmaram ter conhecimento “Muito elevado” sobre a Política de Segurança da Informação (PSI), um indicou conhecê-la e que já ministrou aula de segurança da informação e o outro alegou “outra razão”, uma vez que participou da construção da norma.
- Todos os docentes que afirmaram ter grau de conhecimento “elevado” sobre a PSI, também indicaram que o documento é de extrema importância. Interessante observar que todos eles são da área de Tecnologia da Informação. Ou seja, os 4% dos profissionais que dizem ter um bom conhecimento da PSI ou são profissionais da área e/ou participaram da confecção do documento.

Os 15,9% dos que disseram ter conhecimento “Suficiente” da Política de Segurança da Informação do Instituto apresentaram as seguintes razões:

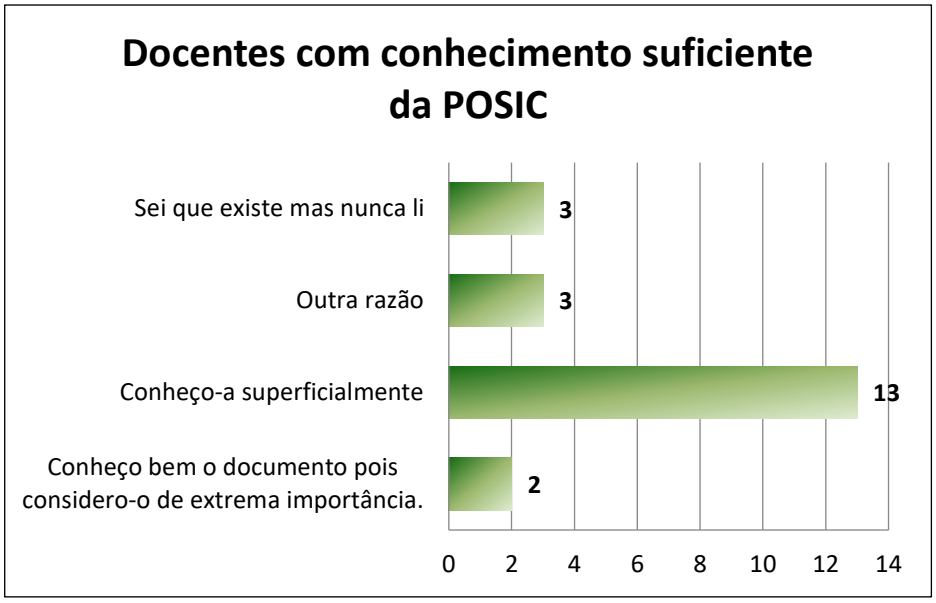


Gráfico 9 – Docentes com conhecimento suficiente da POSIC

Os professores que afirmaram saber da existência da norma, mas que nunca a leram, justificaram que não se debruçaram sobre o assunto e que não tiveram necessidade de conhecê-la.

Aqueles que alegaram "Outra razão", um disse que leu o documento, mas não se aprofundou no assunto; outro disse que conhece o tema e acredita que este deve ser tratado pela instituição; e o último, não apresentou coerência em sua justificativa ao dizer que nunca leu a norma. "*imagino que exista, mas nunca li*" disse o docente F.

Dentre as justificativas do grupo que afirma conhecer superficialmente a PSI, elas indicaram que o docente consultou o documento quando teve necessidade; que alguns participaram de apresentação da Diretoria de TIC do instituto sobre o tema; e, ainda, que até então não tinham se atentado para a relevância do assunto, mas que a pesquisa lhes mostrou a importância de se aprofundar no tema.

A maioria (50,7%) afirmou ter conhecimento insuficiente sobre a Política de Segurança da Informação. As razões apresentadas pelos professores para o grau de conhecimento que eles detêm sobre a PSI também foram bastante variadas, conforme pode se observar no Gráfico 10.

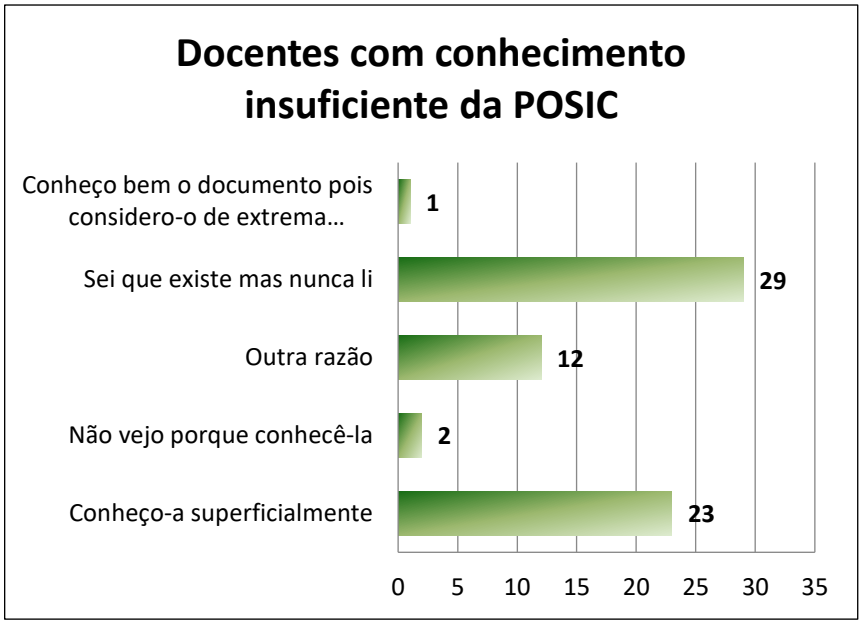


Gráfico 10 – Docentes com conhecimento insuficiente da POSIC

A maior parte desses docentes afirmou nunca ter lido a PSI. Alguns alegaram que falta divulgação do documento; outros que nunca receberam orientação prévia nesse sentido; e, ainda, que a instituição não faz uma abordagem sobre o tema, o que desestimula os servidores na busca pela norma. "*Não é discutido em horários e ambientes coletivos, indicando baixa importância do tema pelos gestores e desestimulando os usuários a conhecer melhor essa política*." docente J

As justificativas daqueles que disseram conhecer superficialmente a PSI foram desde o argumento de que conhecem o necessário para desempenhar sua função de docente, até a falta de incentivo e de informação sobre o assunto, passando ainda por aqueles que não têm interesse no assunto e que não há divulgação da norma. *"Por não ser da área de TI, nunca me preocupei em buscar informações sobre o assunto." Foi a justificativa do* docente BC*; BD argumenta: "Se tiver uma documentação que rege os procedimentos com relação a informação é pouco difundida." Para* BE: *"Nunca tive interesse".*

Os docentes que alegaram "Outra razão" justificaram que desconhecem a existência de uma Política de Segurança da Informação no Instituto. *"Não sabia que existia algum documento norteador sobre o assunto"* docente B*; "Simplesmente, ela não existe !!!"* docente BF

Da mesma forma, aqueles docentes que não veem porque conhecer a PSI, apoiaram-se no desconhecimento da norma e no fato de não a considerarem relevante. *"Não acho relevante.";* docente BG *"Desconheço o documento."* docente C

Constatou-se incoerência na resposta de um dos docentes uma vez que ele tenha selecionado a opção "Conhece bem o documento", não poderia, ao mesmo tempo, declarar em sua justificativa que tem "conhecimento insuficiente sobre a PSI".

Os docentes que afirmaram não ter nenhum conhecimento sobre a Política de Segurança da Informação (29,5%) optaram por marcar três das opções apresentadas: Não vejo porque conhecê-la, Sei que existe mas nunca a li e Outra razão.

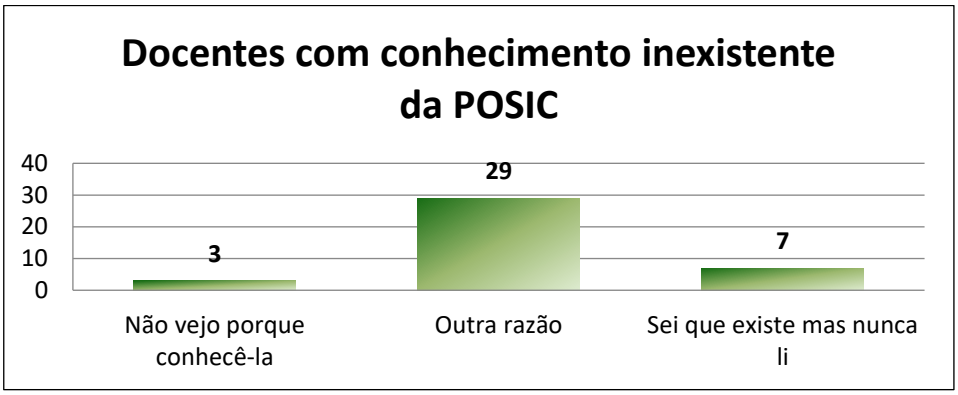


Gráfico 11 – Docentes com conhecimento inexistente da POSIC

Embora as razões tenham sido diferentes, as justificativas foram, praticamente, as mesmas para esse grupo de docentes: falta de divulgação da norma e de incentivo para o seu uso; desconhecimento da existência do documento; e falta de interesse do profissional.

Seguem alguns exemplos das respostas desse grupo de docentes: *"Não conheço a divulgação desta política"* docente O*; "Não sabia da existência dessa política"* docente BH*; "falta de despertar o interesse"* docente BI

Algumas considerações:

Se somados o número de docentes com conhecimento "inexistente" ao de "insuficiente", constata-se que 80% não conhecem a Política de Segurança da Informação do Instituto Federal estudado.

A maior queixa dos docentes quanto à PSI é a falta de uma divulgação efetiva da norma em todo o Instituto.

Muitos não se viram sensibilizados quanto à importância da Política, o que remete à falta de discussão sobre o tema na instituição.

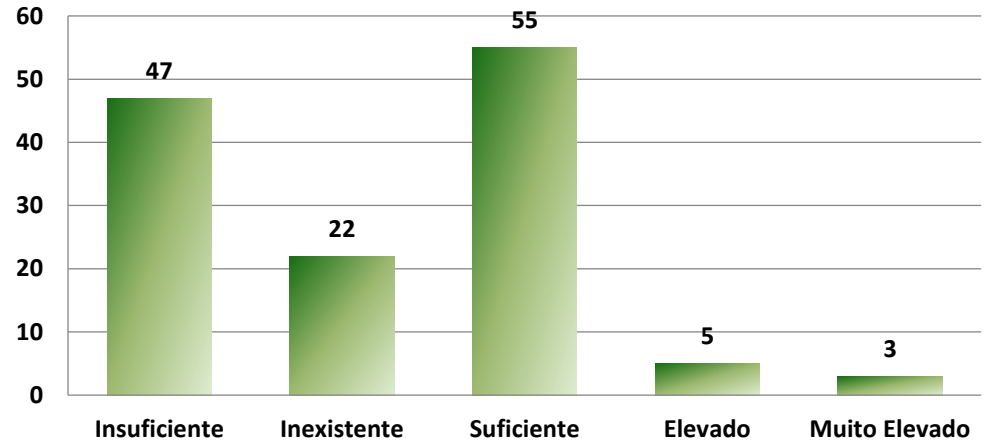
Em sua maioria, os docentes que alegaram ter conhecimento suficiente da PSI, recorreram ao documento por uma necessidade específica.

Só conhece bem a PSI os docentes que ministram aulas em disciplinas de Tecnologias da Informação ou que participaram da criação do documento.

O difícil acesso à Política de Segurança da Informação, também foi um ponto abordado pelos docentes.

Questão 10 (Q10) - Em sua opinião, qual o grau de efetividade da PSI (Política de Segurança da Informação) deste Instituto Federal?

Respostas



Resultados

- A maioria dos docentes (41,7%) entende que a Política de Segurança da Informação – PSI tem grau de efetividade suficiente.
- Cerca de 35% dos docentes consideram insuficiente a efetividade da PSI.
- A PSI não é efetiva na visão de 16,7% dos docentes.
- Para 3,8% dos docentes é elevada a efetividade da PSI.
- Apenas 2,2% acreditam que PSI tem um grau muito elevado de efetividade.

Tabela 13 – Gráfico e Resultados da Q.10 sobre grau de efetividade da PSI (Política de Segurança da Informação) do instituto para os docentes

Análise dos Resultados

Somando-se os que optaram por insuficiente e inexistente, caracterizando que a PSI do Instituto não é efetiva, tem-se um percentual de 52%, enquanto que 48%, correspondente à soma dos quantitativos de suficiente, elevado e muito elevado acreditam que a PSI é efetiva.

Os docentes que optaram pelos itens “Elevado” e “Muito Elevado” como resposta à eficiência da Política de Segurança da Informação, argumentaram que o documento é importante por trazer confiabilidade e segurança aos dados institucionais. *“A segurança dos dados é de extrema relevância ao órgão.”* docente BJ

Outros ainda disseram que acreditam que o grau de efetividade da PSI do instituto é elevado por acreditar na sua função, mas que desconhecem o documento. “*Mesmo não conhecendo acredito que é elevada, devido ao público educacional*.” docente BK

Para o grupo de docentes que considera “Suficiente” o grau de efetividade da PSI, a maior defesa é de que, embora não conheçam o documento, desconhecem problemas

ocorridos na instituição nessa esfera. "*Nunca ouvi sobre ocorrência de fatos que demonstrassem ineficiência."* docente BL

Alguns docentes defendem o documento, mas não a forma como ele está sendo aplicado na instituição. *"Nossa política de segurança da Informação é bem feita, porém a Instituição não utiliza como deveria, talvez por não saber dos riscos, simplesmente por falta de conhecimento na área."* docente BM

E a maior parte dos docentes deste grupo afirma desconhecer o documento e por isso não tem condições de melhor avaliá-la. *"Creio que precisa ser divulgado com maior publicidade para que seja mais efetivo, muitos servidores mal conhecem que existe uma política de segurança."* docente BN

Aqueles que declararam "Insuficiente" o grau de efetividade da Política de Segurança da Informação defenderam sua opinião alegando que se já houve histórico de ataques cibernéticos à instituição, se não há aplicabilidade da norma, se ela não é divulgada e se o documento é desconhecido, não tem como a PSI ser efetiva. "*Talvez fosse mais apropriado eu deixar esta pergunta em branco, visto que mal conheço tal política. Mas pensei que o fato de um coordenador mal conhecer a PSI da instituição deve ser motivo suficiente para considerá-la de efetividade insuficiente*". docente L

Há ainda aqueles que são contrários ao uso de uma Política de Segurança da Informação numa instituição de ensino, por entender que a norma é um empecilho para o ensino e para a pesquisa.

> Respondo a partir de minha experiência e do que considero necessário em uma instituição de ensino e pesquisa. Se a PSI é um estorvo ao ensino e à pesquisa, ela não pode ser considerada eficiente, não em uma instituição de ensino e pesquisa. docente BO

De forma unânime, os docentes que avaliaram como "Inexistente" o grau de efetividade da Política de Segurança da Informação do instituto, assim o fizeram por desconhecer o documento. *"eu não conheço a política nem ao menos as ações decorrentes dela.";* disse o docente BP e BQ defende:*"inexistente pq não a conheço".*

Algumas considerações:

A Política de Segurança da Informação deste Instituto não é divulgada adequadamente, o que decorre da ausência de institucionalização da PSI no âmbito da instituição;

Os docentes não têm um conhecimento claro sobre o que é uma Política de Segurança da Informação;

Para muitos docentes a PSI se limita às regras de controle de acesso, as quais não são foco da Política e sim, de ferramentas/dispositivos de controle de acesso como *Proxy* e *Firewall*, por exemplo;

O desconhecimento da PSI faz com que os docentes tenham certa estranheza e dificuldade em aceitar a norma;

Neste sentido, faz-se necessário estabelecer um processo de divulgação, conscientização e capacitação sobre a Política de Segurança da Informação na instituição;

A PSI deste Instituto Federal data de 2011, portanto, precisa ser atualizada para refletir as necessidades e desafios atuais da instituição, conforme, justificativa de um dos docentes:

> Muito acesso liberado, pouco monitoramento, principalmente no que se refere a Impressão de documento. Não temos classificação da documentação, nem tão pouco uma política de descartes de lixo. Política de acesso tanto na Reitoria quanto nos campi. Uso da Internet, não vejo nenhuma política de uso, nem de restrições o que afeta consideravelmente o tráfego de dados. docente BR

IV – CONCLUSÕES E PROJETO DE INTERVENÇÃO

A educação, enquanto processo que proporciona acesso aos meios de informação e produção, torna-se um elemento fundamental para o exercício da cidadania, pois, "*além de facilitar o acesso a uma formação baseada na aquisição de conhecimentos, deve permitir o desenvolvimento das habilidades necessárias na sociedade da informação.*" (Flecha & Tortajada, 2000, p.24).

Dessa forma, é um desafio para a instituição de ensino capacitar digitalmente seus estudantes, ensinando-os sobre propriedade intelectual, privacidade e segurança em ambiente virtual, além de torná-los indivíduos adaptáveis, criativos, cidadãos digitais éticos e cientes de que são passíveis de responsabilização caso extrapolem seus limites.

Ou seja, se de um lado existem legislações que trazem o regulamento acerca da segurança da informação na Administração Pública Federal, do outro existem também normas que defendem o livre acesso à informação para um produtivo processo de ensino-aprendizagem, a exemplo da Lei de Diretrizes e Bases (Lei 9394/96) que, em um dos incisos do Art. 3º, diz que o ensino será ministrado com base nos princípios de liberdade de aprender, ensinar, pesquisar e divulgar a cultura, o pensamento, a arte e o saber.

Não é tarefa simples resolver os conflitos oriundos desta oposição, mas também não é possível furtar-se a eles, sob risco de transformar a internet numa plataforma para a promoção da intolerância, do racismo, do preconceito e intimidação de grupos e pessoas. A internet, apesar de seu alcance e dinamicidade, não pode ser considerada "terra de ninguém" onde tudo pode ser dito e estimulado impunemente.

Toda comunidade escolar precisa estar ciente de que seus discursos e opiniões podem gerar responsabilização e que a responsabilidade das instituições de ensino extrapola o que ocorre nos seus domínios, uma vez que não se restringe à integridade física de seus estudantes, mas, também e principalmente, por sua integridade moral, já que os danos incidentes sobre esta influenciam substancialmente no processo de aprendizagem.

Dessa forma, é preciso admitir que, em tempos de internet, o grande desafio das instituições de ensino está em como direcionar o uso das Tecnologias de Informação e Comunicação positivamente, ou seja, como orientar seus educandos a explorar todos os benefícios que este avanço propicia e, ao mesmo tempo, conscientizá-los das graves consequências que o uso inadvertido dessa ferramenta pode lhes causar.

Por ser um Instituto Federal, a instituição estudada se submete às normas, regulamentações e definições sobre Segurança da Informação e Comunicação aplicáveis a toda Administração Pública Federal Brasileira. Por outro lado, preza pela democratização do acesso à informação nos ambientes acadêmicos, que é contrária a qualquer tipo de

cerceamento de acesso à informação, prática esta recorrente quando se trata de políticas de segurança da informação.

Diante dessa dualidade, o estudo em questão trouxe o caso de um Instituto Federal Brasileiro e buscou analisar em que medida a aplicação das políticas de segurança da informação impacta o trabalho do docente no momento em que este busca a dinamização das aulas por meio do acesso à internet.

Um dos objetivos deste estudo era verificar se a Política de Segurança da Informação (PSI) criada pelo Instituto estava de acordo com que determinam os órgãos regulamentadores nacionais quanto à segurança da informação na Administração Pública Federal. Verificou-se que, embora esteja com data de vigência expirada, a PSI está em conformidade com as recomendações e legislações, estabelecidas pelos órgãos regulamentadores nacionais. Além disso, a política está em processo de revisão para um novo biênio (2019/2020) de vigência.

Identificar se os docentes conhecem a política de segurança da informação da instituição, constituiu o segundo objetivo deste trabalho e, a partir, deste estudo, pôde-se verificar que 50,7% dos docentes tinham conhecimento insuficiente sobre a Política de Segurança da Informação e apenas 4% dos inquiridos disseram ter um conhecimento adequado do documento.

As justificativas para o desconhecimento da PSI trouxeram questões como falta divulgação do documento; ausência de orientação prévia nesse sentido; e, ainda, que a instituição não faz uma abordagem sobre o tema, o que desanima os servidores na busca pela norma.

O terceiro objetivo deste estudo estava voltado em captar a visão dos docentes acerca da Segurança da Informação e, principalmente, analisar – em meio ao cenário conflitante de limites legais versus direito à informação – se a Política de Segurança da Informação adotada pela instituição impactava o trabalho do docente no momento em que este busca, ou buscava, a dinamização das aulas por meio do acesso à internet.

Com esse intuito, foi enviado aos docentes do Instituto um questionário com dez perguntas envolvendo segurança da informação, para que a partir de suas respostas fosse possível mapear, de maneira geral, a visão desses profissionais sobre o tema proposto.

Ao serem questionados diretamente sobre se as regras de controle de acesso à internet ajudam ou confundem a dinamização de suas aulas, 60% dos docentes afirmaram que os controles não atrapalham. Mais que isso, defenderam que estes controles ajudam a dinâmica das aulas, uma vez que tiram do docente a preocupação de como os estudantes estão usando a rede de computadores, o que lhes dá maior tranquilidade para se focarem no processo ensino-aprendizagem em contexto de sala de aula.

Quando os docentes se referiram à preocupação de como os estudantes estão usando a rede de computadores, supôs-se que esta se relacionasse ao uso inadequado da

internet e, consequentemente, ao risco de crimes virtuais se concretizarem durante as aulas. Para validar essa hipótese buscou-se a resposta dos docentes em outra questão do formulário que trazia exatamente esse questionamento.

Os resultados demonstraram que 71% dos docentes têm a preocupação de que crimes virtuais ocorram durante suas aulas. Destes, 40% também acreditam que podem ser responsabilizados por esses crimes e 31% desconhecem se cabe a eles essa responsabilização.

Outra constatação importante é que 82,6% dos docentes afirmam que é papel da instituição de ensino controlar o acesso à internet. E quando questionados do porquê de sua resposta, verificou-se que, dentre os diversos pontos de vista identificados nas justificativas, a maioria dos docentes desse grupo (25%) defende a existência do controle de acesso por ter preocupação com o risco de a instituição, os estudantes ou eles próprios enfrentar, no futuro, problemas jurídicos, éticos ou legais.

Já na visão do grupo de docentes que discorda que seja papel da escola estabelecer critérios de controle de acesso, a preocupação que sobressaiu às demais apresentadas (47,8%) estava no risco de as restrições ferirem a liberdade à informação.

Ressalta-se que os percentuais apresentados nos dois parágrafos anteriores foram obtidos a partir da análise dos resultados dentro daquele grupo de resposta. Ou seja, os percentuais se referem, primeiro, aos 109 docentes que responderam “Sim” e no seguinte, aos 23 docentes que responderam “Não”.

De todo modo, é interessante perceber que os principais argumentos dos dois grupos corroboram com a constatação de que o conflito entre a “liberdade” e o “controle” é uma realidade entre os docentes deste Instituto Federal.

Entretanto, quando se analisa de maneira geral, ou seja, considerando o número total de respondentes (132) sem considerar a que grupo eles pertencem, esse conflito não chega a ser significativo, uma vez que apenas 8,3% dos docentes se mostraram preocupados com o risco a liberdade à informação.

Infere-se a partir desses dados que, apesar de no meio académico muito se defender que instituição de ensino não deve estabelecer limites ao acesso à informação na internet e que cabe à escola preparar cidadãos críticos e conscientes, essa defesa perde força quando o docente se depara com o risco de o estudante, a instituição, ou mesmo ele próprio, sofrer alguma penalização pelo uso inadvertido da internet.

Além disso, mesmo para muitos dos docentes contrários às definições de regras que restrinjam o acesso à internet, a discordância não estava exatamente na possibilidade de cerceamento da informação e sim, na dificuldade que eles enfrentam para conseguir a liberação quando necessitam navegar em algum site bloqueado.

Portanto, a ausência de um procedimento eficaz de desbloqueio dos sites necessários para que o docente tenha condições de preparar ou ministrar suas aulas ou, ainda, realizar suas pesquisas é que constitui um fator que impede a dinamização das aulas.

Outros fatores tangenciam essa discussão e se faz necessário considerá-los. Um deles é identificar, em meio a tudo que já foi pontuado, o que o docente entende como livre acesso à informação.

Novamente não há um consenso. Aproximadamente 17% dos docentes foram enfáticos ao afirmar que “livre é livre”, portanto, argumentaram que não cabe nenhum tipo de restrição e se os limites forem necessários, estes deverão ser construídos e não impostos.

Por outro lado, aproximadamente 63% defenderam que ter livre acesso à informação significa poder acessar todo e qualquer tipo de sítio, com exceção daqueles considerados impróprios, como os que trazem conteúdo racista, de pornografia infantil, homofóbicos, dentre outros.

E 7,6% dos docentes optaram pelo item “Outro Conceito”, mas ao justificarem sua escolha, acabaram por defender a ideia de que é importante ter certo nível de limite de acesso. O que eleva para aproximadamente 71% o número de docentes favoráveis às restrições de acesso.

O receio dos docentes quanto à possibilidade de responsabilização da instituição ou deles próprios oriunda de um acesso indevido à internet está baseado em dois fatores: no nível de maturidade/idade dos estudantes e na incapacidade do docente em controlar tudo que ocorre durante suas aulas, especialmente, quando se refere ao ambiente virtual.

Cabe ressaltar que, por mais que a instituição de ensino seja responsável pelo estudante enquanto este estiver sob sua tutela, não foi encontrado no arcabouço legislativo brasileiro uma lei que imputa ao docente, seja total ou parcialmente, a responsabilidade sob os crimes cometidos por seus estudantes durante as aulas, salvo se comprovada sua efetiva participação. Esses resultados permitiram afirmar que segurança da informação é uma preocupação da maioria dos sujeitos da amostra.

Portanto, foi importante entender o que neste universo merece mais atenção na visão destes docentes. Do total de respondentes, 41,7% endossaram o pensamento de Frish (2002) ao afirmarem que o fator humano é o ponto de maior vulnerabilidade quando o assunto é segurança da informação, ou seja, a segurança começa e termina nas pessoas. Essa tese está baseada na imprevisibilidade, na inconsequência, no desconhecimento e na inabilidade com o ambiente e, até mesmo, na maldade, características estas inerentes ao ser humano.

Para 28,8% dos docentes é importante garantir o bom funcionamento da infraestrutura e não comprometer dados relevantes da instituição e, nessa linha, defendem que as soluções de segurança da informação são fundamentais para disponibilizar um mínimo de credibilidade para a comunidade académica. Dessa forma, a ausência de um bom

antivírus, de um firewall e de ter todas as atualizações necessárias aplicadas no ambiente tecnológico constitui uma vulnerabilidade para a instituição.

Outros 22% entendem que o maior risco à segurança da informação está na ausência de regramento, uma vez que também considerando que o fator humano constitui uma vulnerabilidade, esta pode ser minimizada com ações contínuas de orientação e conscientização das pessoas, educando-as sobre o tema. E as normas constituem a base para a construção desse conhecimento.

Quando questionados se consideram que ter uma Política de Segurança da Informação (PSI) é importante para o Instituto, 97% dos docentes responderam que sim. Entretanto, 80% desses docentes ou desconhecem totalmente se a instituição possui uma PSI ou detém um conhecimento que eles próprios consideraram insuficiente acerca do documento.

Todavia, alguns docentes mostraram-se ansiosos por conhecê-la e/ou aprendê-la, além de desejosos de serem partícipes na construção dessa Política, caso ela não exista.

Dado o elevado índice de desconhecimento da norma, a Política de Segurança da Informação foi considerada ineficiente por aproximadamente 52% dos docentes.

A justificativa para essa ineficiência estava amparada, principalmente na ausência de institucionalização da PSI, uma vez que não se tem estabelecido um processo de divulgação, conscientização e capacitação sobre a norma, nem fóruns de discussão sobre o tema na instituição.

Além disso, 90,2% dos docentes nunca receberam do Instituto, uma capacitação na área de segurança da Informação. Destes, somente 12,6% fizeram cursos na área, independente do patrocínio do Instituto. Portanto, 78,8% dos docentes da instituição não tem nenhuma formação em Segurança da Informação.

Neste estudo também se buscou avaliar se há, na visão do docente, preocupação da comunidade com as questões de segurança da informação. Portanto, foi questionado ao professor se alguma vez ele foi abordado ou pelos pais e responsáveis ou pelos próprios estudantes sobre as condições de acesso à internet nos laboratórios de informática.

A partir das respostas, concluiu-se que mesmo se mostrando fundamental o cuidado com segurança da informação nos dias de hoje, a comunidade académica, de maneira geral, não cobra dos docentes e nem da instituição de ensino uma postura em relação às condições de acesso à internet, dado que 84% dos docentes nunca foram questionados pelos pais e/ou responsáveis e tampouco pelos estudantes sobre a existência de restrição de acesso à internet nas aulas em laboratório de informática.

Um dos pontos levantados pelos docentes que pode dar indícios que justifiquem essa postura da comunidade está no fato de que a população assistida por este Instituto Federal Brasileiro, em geral, é muito vulnerável social e economicamente. Além disso, na maioria das

vezes, esse público não está ciente da existência desse tipo de perigo. Se o risco não é conhecido, consequentemente não haverá preocupação.

Outro fator considerado pelos docentes para essa passividade da comunidade escolar está no fato de que os pais e/ou responsáveis pelos estudantes menores de idade pouco participam da vida escolar desses estudantes ou por confiar nos profissionais de educação ou por imputar essa responsabilidade à escola e ao docente.

Nesse ponto, chega-se à conclusão que, de uma forma ou de outra, a passividade da comunidade e a postura dos pais e/ou dos responsáveis frente às questões relacionadas à segurança da informação, aumentam a responsabilidade da instituição de ensino na abordagem e no tratamento deste assunto.

Contudo, por mais que segurança da informação seja uma preocupação dos docentes, ainda é incipiente a relação desses profissionais, e talvez de toda comunidade académica, com o tema, principalmente se confrontados o grau de responsabilidade atribuído ao Instituto e, consequentemente, aos docentes, com o alto índice de desconhecimento desses profissionais tanto sobre as políticas institucionais de Segurança da Informação, quanto sobre o próprio assunto, de maneira geral.

.

4.1 Projeto de Trabalho / Projeto de Intervenção

Embora a Política de Segurança da Informação seja classificada como importante e crítica para a maior parte dos docentes do Instituto Federal Brasileiro estudado, percebe-se ainda certa resistência de alguns deles em relação ao tema, seja pelo desconhecimento do assunto seja pela percepção que têm de como a instituição aborda essa questão.

Este Projeto de intervenção decorre dos pontos críticos identificados neste estudo e que são necessários à instituição no que diz respeito à segurança da informação: atualização da Política de Segurança da Informação com a participação da comunidade académica; plano de divulgação da PSI; e plano de capacitação dos servidores em segurança da informação e na política de segurança institucional. Portanto, este projeto propõe o escopo de uma metodologia para a criação de um Sistema de Gestão de Segurança da Informação – SGSI para a instituição.

Para Fontes e Araujo (2008), o Sistema de Gestão de Segurança da Informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como podem ser reduzidos os riscos para a segurança da informação.

Martins e Santos (2005) corroboram com essa visão quando afirmam que resultam da implantação de um Sistema de Gestão da Segurança da Informação (SGSI) a

padronização e documentação dos procedimentos; ferramentas e técnicas utilizadas; a criação de indicadores e de registros; a definição de um processo educacional de conscientização dentro da organização.

O escopo da metodologia proposta neste trabalho está amparado nas fundamentações apresentadas e na norma BS 7799-2 que recomenda os controles necessários a um Sistema de Gestão de Segurança da Informação – SGSI e visa desenvolver, implementar e estabelecer uma melhoria contínua para segurança da informação e que foi estruturado em fases a serem seguidas.

Fase 1: Definições

A) Criação do Comitê de Segurança

Para o sucesso do Sistema de Gestão de Segurança da Informação, este deve ser construído em colaboração entre representantes de todos os setores da organização (campi e reitoria).

Essa equipe é denominada Comitê de Segurança da Informação. Devem fazer parte desse comitê pessoas que atuam nas áreas de TIC e de Educação/Ensino, e também aquelas que detenham poder de decisão dentro da organização. Esta equipe deve ser atuante e estar comprometida com a política de Segurança da Informação a ser implantada.

Uma das funções principais deste comitê é definir o nível de risco aceitável pela organização e, a partir disso, definir a política de Segurança da Informação da instituição, conforme os objetivos e metas traçados para o Sistema de Gerenciamento da Segurança da Informação, em conformidade com o planejamento estratégico da organização. A inexistência do comitê afastará a instituição dos níveis de segurança da informação adequados e necessários às estratégias estabelecidas.

O Comitê de Segurança da Informação deve, primeiramente, trabalhar na concepção do Sistema de Gestão de Segurança da Informação. Essa etapa consiste na análise de viabilidade do projeto, na definição do planejamento inicial de suas fases, bem como em algumas estimativas iniciais de custo, alocação de pessoal, de tempo, de escopo, de objetivos e de metas.

Também é papel deste comitê supervisionar o processo de implantação; tomar todas as decisões que vão desde a viabilidade até avaliação do projeto; realizar formação básica e conscientização dos servidores.

Fase 2: Medições

A) Aplicação do Questionário

Uma vez que este instituto já possui uma Política de Segurança da Informação, a realização do diagnóstico será importante para verificar se os controles já implementados são

eficientes ou não e, em caso afirmativo, aproveitá-los. Esta etapa pode ser realizada por meio de entrevistas, técnicas de *Brainstorming*, dentre outras.

Além disso, a utilização de questionários, entrevistas e de outros instrumentos para captar as percepções dos usuários têm o intuito de minimizar a rejeição que, geralmente, a implementação das políticas de segurança da informação causa aos usuários.

Da mesma forma, essas informações ajudarão a compreender tanto as relações sociais no âmbito da instituição quanto o comportamento dos servidores frente ao tema segurança da informação. Os resultados obtidos servirão de insumo para a revisão ou para elaboração de uma nova política de segurança, bem como para definir como será realizado o programa de adesão e de conscientização a essa política.

B) Inventário dos Ativos

A ideia desta etapa é identificar quais os ativos (tecnologias, processos, informação) importantes para o fluxo de funcionamento da instituição e que possam ser pontuados níveis de ameaças, de vulnerabilidades e a probabilidade de riscos sobre um determinado ativo.

Equipamentos, sistemas, nome da instituição, estrutura de comunicação (Internet, correio eletrônico), pessoas, serviços, infraestrutura de rede interna e externa e classificação da informação são exemplos de ativos que podem ser observados neste trabalho. O mapa do perímetro da rede de computadores onde será aplicado o SGSI e o inventário dos ativos e suas respectivas classificações são resultados desse processo.

Como a entrada e saída de ativos é um processo dinâmico, o inventário de ativos precisa ser revisado e detalhado de tempos em tempos, de acordo com a declaração do escopo, no qual precisa constar a base para as decisões futuras.

A delimitação do escopo é extremamente necessária, pois quanto maior o escopo maior a complexidade do SGSI a ser implementado.

C) Classificação da Informação

O Instituto Federal estudado ainda não dispõe de uma política de classificação da informação, porém é um trabalho que já está em construção. Sendo assim, durante o processo de avaliação dos ativos da instituição, físicos ou digitais, é interessante que as informações sejam classificadas quanto ao critério de tratamento que, segundo Ferreira e Araújo (2006), pode ser definida como informação pública (comum a todos), informação interna (somente dentro da organização ou setor) e informação confidencial (somente por pessoas autorizadas).

Como resultado desta fase, a instituição terá condições de identificar o nível de segurança atual, para posteriormente trabalhar neste processo de melhoria.

Fase 3: Análises

A) Gestão dos Riscos

Fundamentalmente, essa fase deve abarcar a análise dos riscos que serão priorizados. Portanto, é necessário descobrir, visualizar e priorizar as causas do problema a ser tratado. (Aguiar, 2006)

Uma das formas de tratar os riscos é através do princípio de Pareto, o qual determina que cerca de 20% das causas geram 80% das consequências. Desta forma, nem todos os riscos devem ser tratados, apenas aqueles que representam uma importância mais significativa para a instituição. (Campos, 2007)

É importante estabelecer o nível de risco envolvido para cada ameaça detectada. A ISO 13335-3 trata detalhadamente as opções e as estratégias de condução da análise de riscos, que podem ser definidas em função ou do tempo ou do orçamento existente ou dos objetivos. Após esta fase, recomenda-se o uso da BS 7799-2 para decidir a estratégia de gestão de riscos.

De posse do diagnóstico dos riscos, o Comitê de Segurança da Informação deverá, junto à alta administração do órgão, estabelecer quais os níveis de risco são aceitáveis e aqueles não-aceitáveis e, para estes, definir o procedimento a ser seguido em cada situação.

Exemplo de decisões: reduzir o nível de risco, por meio da aplicação de controles de segurança; aceitar o risco, ou seja, considerar que ele existe, mas não aplicar qualquer controle; transferir o risco repassando a responsabilidade de segurança a um terceiro; negar o risco que é a opção menos recomendada.

Pode-se fazer a análise de riscos tanto por uma abordagem quantitativa, baseada em estatísticas e na análise dos registros de incidentes de segurança, quanto qualitativa, esta baseada no conhecimento e na experiência dos especialistas da área. Ambas oferecem informações importantes para a estruturação das atividades de identificação de riscos.

B) Revisão e/ou Elaboração da Política de Segurança da Informação

Com base nos riscos mais significativos e urgentes apontados no relatório de gestão de riscos, o Comitê de Segurança da Informação deverá especificar quais pontos deverão ser formalizados na Política de Segurança da Informação e, após validar o documento o encaminhará ao Comitê de Governança Digital para aprovação e determinação de execução e divulgação da política.

De acordo com as RFC´s 2196 e 2828, a Política de Segurança da Informação é um documento que deve ser construído conforme especificidade de cada instituição e nela devem constar recomendações, regras, responsabilidades e as práticas de segurança desejadas e adequadas à realidade da instituição.

Segundo a ISO/ IEC17799, a PSI deverá ser aprovada pela diretoria; divulgada e publicada de forma ampla para todos os colaboradores; ser revisada regularmente; estar em conformidade com a legislação; deve definir as responsabilidades gerais e específicas; deve dispor acerca das consequências das violações.

Portanto, é de fundamental importância a existência de uma política de segurança da informação e esta deve ser referência para todos os servidores da instituição.

Fase 4: Implementação

Para que a cultura da instituição seja modificada em relação à segurança da informação, “é fundamental que os funcionários estejam preparados para a mudança, por meio de avisos, palestras de conscientização, elaboração de guias rápidos de consulta e treinamento direcionado”. (Freitas & Araujo, 2008, P. 47).

A política deve ser escrita de forma clara para não gerar dúvidas nos servidores. Todos aqueles que atuam na instituição devem ser informados e capacitados para que tenham condições de se adequarem às mudanças propostas na Política de Segurança da Informação. Aqui inclui servidores efetivos, substitutos, estagiários, terceirizados e prestadores de serviços de forma geral, abarcando toda a cadeia funcional da instituição.

De acordo com a NBR ISSO IEC 27002 (2005), os servidores precisam conhecer e estarem clientes das ameaças e das vulnerabilidades de segurança da informação que podem impactar o Instituto. Se os servidores não conhecerem a Política de Segurança da Informação do órgão, eles não se preocuparão em cumprir essas recomendações durante a execução normal do trabalho e a PSI estará cada vez mais distante de fazer parte da cultura organizacional.

Há várias frentes que podem ser adotadas nesta instituição para que a implantação da Política de Segurança da Informação tenha sucesso e traga resultados para a instituição. No momento de seu lançamento, o instituto poderá promover rodadas de conversas, palestras, workshops, painéis que trabalhem juntos aos servidores a importância com o cuidado com a segurança da informação.

Concomitante a isso, pode-se estabelecer um plano de comunicação da PSI, comunicando-a no e-mail institucional, nas páginas da intranet e extranet do instituto e, também nos diversos fóruns onde for possível fazer essa divulgação.

Para reforçar e estar sempre relembrando a importância da Política de Segurança da Informação aos servidores, pode ser instituída, no calendário académico da instituição, a semana de Segurança da Informação, evento este no qual os servidores e toda comunidade académica do órgão poderão ouvir especialistas da área e debater a importância do tema.

Outro viés de atuação que deve ser construído para ser ofertado a todos os servidores no órgão é o plano de capacitação em Segurança da Informação. Essa capacitação pode se dar tanto presencial quanto virtualmente. Uma vez estabelecido esse plano, todo servidor ao entrar para a instituição deverá percorrer essa trilha de capacitação. Dessa forma, já começará a trabalhar no Instituto conhecendo as políticas de segurança da informação do órgão.

Todavia, se não houver o comprometimento da alta gestão da instituição para apoiar todas essas iniciativas, a política de segurança da informação não será efetiva e, mais que isso, iniciar qualquer ação neste sentido será algo temerário e com alto índice de insucesso.

Fase 5: Controle

Uma vez implantado o Sistema de Gestão de Segurança da Informação, faz-se necessário o acompanhamento constante da Política e demais controles, com o objetivo de verificar os impactos e a adesão dos servidores quanto à política de segurança da informação.

Nesta etapa podem ser aplicados os mesmos questionários da etapa inicial, verificando se houve aprendizagem e entendimento quanto às questões perguntadas na fase inicial sendo possível comparar as respostas de ambas as fases e, a partir da análise desses resultados, propor ações corretivas e de melhoria do processo, que deve ser um processo contínuo e evolutivo.

Sempre ao final dessa etapa, a instituição deverá identificar se houve melhorias e, em caso positivo, registrar as evoluções conquistadas e, se não foram detectadas melhorias ou aumento de nível de aprendizado dos servidores quanto à Segurança da Informação, reinicia-se o ciclo, de modo a identificar as falhas encontradas no processo e propor os ajustes cabíveis.

Cabe ressaltar que o gerenciamento de riscos, a implantação de contramedidas e de diretivas de segurança devem permear todas as fases do processo de implantação da metodologia proposta ao Instituto. Para tanto, devem ser definidos indicadores que possibilitem a mensuração do funcionamento e do desempenho do ambiente monitorado.

Com essas medidas poderão ser identificadas as áreas da instituição que foram bem-sucedidas e as que precisão de apoio e de ajustes.

Quando o instituto alcançar um nível maior de maturidade em Segurança da Informação, medidas adicionais de segurança poderão fazer parte do Sistema de Gestão de Segurança da Informação. O Plano de Continuidade dos Negócios é um exemplo dessas medidas, que busca a disponibilidade dos serviços de missão-crítica considerados para a instituição.

Fase 6: Seleção dos Controles e Declaração de Aplicabilidade

Para a realidade do Instituto Federal estudado, não se faz necessária a implementação de todos os cento e vinte e sete controles recomendados pela norma BS7799-2. Dessa forma, é preciso que o Comitê de Segurança da Informação escolha quais controles devem ser implementados para assegurar que os riscos encontrados sejam mitigados ou reduzidos a um nível aceitável.

O comitê deve ainda atentar-se quanto às normas aplicadas à Administração Pública Federal, em especial pelo Gabinete de Segurança da Informação da Presidência da República e pelo Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) de maneira que os controles contidos nessas e nas demais normas estejam integrados de forma natural ao SGSI.

Cabe esclarecer que a definição de regras não garantirá a segurança da informação no Instituto. Sem procedimentos e controles, a segurança será uma realidade distante para a instituição.

Portanto, o Comitê de Segurança da Informação apoiado pelo Comitê de Governança Digital precisará se debruçar na definição de políticas para acesso (interno e externo) às bases corporativas; nas normas complementares de política de uso da intranet e Internet; na definição de modelo de identificação de pirataria; de gerenciamento de rede; de distribuição de versões de software e de padrões Internet; detecção de *modems* ligados à rede; definição do padrão de atualização de antivírus; padronização do portal institucional; implantação, roteamento, criptografia, certificação digital, configuração de *firewall*, dentre outras ferramentas e tecnologias necessárias.

Um dos cuidados que o Comitê de Segurança da Informação deverá ter ao especificar os critérios de escolha dos controles a serem adotados é o de não afastar desse processo decisório a relação custo x benefício; a capacidade de gerenciamento do controle e de substituição deste, caso não se apresente efetivo no decorrer do processo e que fuja aos propósitos do órgão, ou ainda que prejudique, inviabilize ou atrapalhe a atividade fim da instituição.

Fase 7: Auditoria do Sistema

No escopo da metodologia sugerida, o ciclo do Sistema de Gestão de Segurança da Informação finda com o processo de auditoria interna ao SGSI, cuja finalidade é verificar se os procedimentos foram adequados e eficazes, se as diversas áreas do órgão estão conseguindo cumprir os normativos estabelecidos, dentre outros.

Para tanto, recomenda-se a independência dos auditores, o planejamento e notificação prévios, o aprimoramento contínuo do SGSI e a busca de constatações e

observações que agreguem valores às atividades referentes à segurança da informação, aos objetivos e metas da organização e às suas políticas. (Martins & Santos, 2005)

O Comitê de Segurança da Informação deverá registrar todas as não conformidades (reais e potenciais) detectadas no SGSI com base no procedimento específico por ele definido.

Deve-se ainda adotar um plano de tratamento das não-conformidades que apresente ações definidas de acordo com a criticidade de cada uma delas. Investigação das causas das não-conformidades, a definição e a implantação de ações corretivas, o registro destas alterações são exemplos de procedimentos a serem adotados, mas que devem ser analisados se são cabíveis ao órgão.

A instituição também deverá estar preparada para tratar as não-conformidades potenciais que serão detectadas por meio do registro de incidentes relacionados ao SGSI. Para tanto, ações preventivas devem ser definidas e implantadas para evitar que estas ocorrências se repitam.

Toda fase só deverá ser encerrada após implantação de ações corretivas e validação de sua eficácia.

Considerações acerca do Projeto de Intervenção

A implantação de um Sistema de Gestão de Segurança da Informação não é um processo trivial e requer um processo contínuo de aprimoramento do modelo. Portanto, é condição para o sucesso desta implantação o apoio da alta gestão deste Instituto Federal Brasileiro que terá papel de motivar a participação de todos os servidores na criação da cultura de segurança da informação dentro da instituição.

Para facilitar a implantação e a comunicação desse sistema, recomenda-se a geração de um manual de segurança do projeto SGSI, contendo todos os documentos gerados em cada etapa do processo.

Dessa forma, serão frutos do Sistema de Gestão de Segurança da Informação:

- Política de Segurança;
- Análise de risco;
- Inventário;
- Temos e Políticas de Uso dos Sistemas e dos Serviços Oferecidos;
- Indicadores de acompanhamento;
- Incidentes Registrados e Classificados;
- Instrumentos Normativos;
- Plano de Comunicação sobre o Sistema de Segurança da Informação;

- Plano de Capacitação em Segurança da Informação, dentre outros.

Um dos pontos fortes da implantação de um Sistema de Gestão Segurança da Informação no órgão está no fato de que, por ser construído em colaboração com os servidores que atuam nas diversas áreas e esferas da instituição (administrativas e educacionais), permitirá que os servidores (se não todos, mas a grande parte deles) tenham conhecimento da existência do plano e que tenham ciência de quão protegidas e seguras estarão as suas informações.

Já os profissionais técnicos terão um modelo de atuação comum, o que evitará que cada campus, ou mesmo que cada equipe crie um padrão específico e desconexo das demais equipes. Com isso, o profissional responsável pela implementação do projeto de segurança terá visão única do sistema de segurança da informação e dos diversos padrões, controles e métodos que o compõem.

V – LIMITAÇÕES DO ESTUDO

O estudo em questão não teve a pretensão de esgotar as questões relacionadas à Segurança da Informação na instituição em estudo e por isso podem ser propostas de estudos futuros como continuação deste.

O público alvo deste estudo foram os docentes que atuam ativamente em um Instituto Federal Brasileiro. Neste estudo, não foram contempladas variáveis como a idade, sexo, formação académica, área de atuação e campus de trabalho do docente, entre outras. Dessa forma, não se pode, por exemplo, avaliar o grupo de docentes da área de exatas é mais favorável às normas da Política de Segurança da Informação os da área de ciências sociais e humanas, assim como também não se pode estudar se os docentes com mais idade e/ou com mais tempo de serviço aceitam melhor as restrições de acesso estabelecidas na PSI, que os mais novos. Portanto, todas essas questões podem ser um ponto de partida para ampliação deste estudo.

Outro ponto que não se teve elementos para analisar neste estudo foi a causa para alguns docentes não terem uma opinião definida sobre o tema Segurança da Informação, mas que são tidos como formadores de opinião pelos estudantes. Essa justificativa pode estar fundamentada em uma série de fatores, como no desconhecimento do assunto, por nunca terem sido provocados a pensar nessa questão; talvez por entenderem que o tema é irrelevante para eles, dentre outras possibilidades. Descobrir a causa desse afastamento do docente com o tema Segurança da Informação também pode ser uma proposta de estudo futuro.

Também não constituíram objeto do projeto de intervenção deste estudo, a definição de ferramentas e nem a criação de instrumentos de diagnóstico, de inventário e de gestão de riscos. Isso porque tais construções exigiriam uma equipe de trabalho, que somente será composta no momento de implantação deste projeto.

A classificação dos dados instituição é necessária para a construção do Sistema de Gestão de Segurança da Informação, todavia, a criação deste documento não foi escopo deste projeto.

Referências Bibliográficas

Abreu, D. (2001). *Melhores Práticas para Classificar as Informações*. Módulo e-Security Magazine. São Paulo, agosto. http://www.modulo.com.br. [consulta em 17/03/2018].

Aguiar, S. (2006). *Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma.* Nova Lima: INDG Tecnologia e Serviços Ltda.

Albuquerque, R.; Ribeiro, B. (2002). *Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408*. Editora Campus. Rio de Janeiro.

Associação Brasileira de Normas Técnicas. ISO/IEC 17799 (2000). *Tecnologia da Informação - Código de prática para a Gestão da Segurança da Informação*. International Organization for Standardization, Switzerland.

Associação Brasileira de Normas Técnicas. ISO/IEC 27001 (2013). *Tecnologia da Informação. Técnicas de segurança. Sistemas de gestão de segurança da informação*. Requisitos.

Associação Brasileira de Normas Técnicas. ISO/IEC 27002 (2013). *Tecnologia da informação. Técnicas de segurança. Sistemas de gestão de segurança da informação.* Requisitos.

Bardin, L. (2016). *Análise de conteúdo* (1º ed.). São Paulo: Edições 70.

Barroso, L. R. (2011). *Colisão entre liberdade de expressão e direitos da personalidade. Critérios de Ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa.* <http://www.migalhas.com.br/arquivo_artigo/art_03-10-01.htm>. [consulta em 22/02/2019].

Beal, A.(2005). *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações* - São Paulo: Atlas.

Birou, A. (1982). *Dicionário de Ciências Sociais*. Lisboa: Publicações Dom Quixote.

Boran, S. (1996). IT Security Cookbook. http://www.boran.com/security/ [Consulta em 15/01/19]

Bowles, M. D.(1999). The information wars: two cultures and the conflict in information retrievel, 1945-1999. Conference on the History and Heritage of Science Information Systems. p. 156-166.

British Standard (1999). *Information security management – Part 2 (1999). Specification for information security management systems, BS 7799-2:1999*. London: BSI, 1999.

Campos, A. (2007). *Sistema de Segurança da informação: Controlando os Riscos*. 2.ed. Florianópolis: Visual Books.

Caruso, C. A. A.; Steffen, F. D. (1999). *Segurança em Informática e de Informações* - São Paulo: Editora SENAC. São Paulo.

Castells, M. (2009).*Comunicación y Poder*. Madrid: Alianza Editorial.

Chiavenato, I. (1999). Gestão *de Pessoas: O novo papel dos recursos humanos nas organizações*. 6ª triagem. Rio Janeiro.

Davenport, T.H.; Prusak, L. (2000). *Working Knowledge: How Organizations Manage What They Know.* Harvard Business Press.

Deresky, H. (2004). *Administração Global: estratégica e interpessoal*. Porto Alegre: Bookman.

Dias, C. (2000). Segurança *e Auditoria da Tecnologia da Informação.* Rio de Janeiro: Axcel Books.

Flecha, R.; Tortajada, I. (2000). *Desafios e saídas educativas na entrada do século*. In: Imbernon, F. *A Educação no século XXI*: os desafios do futuro imediato. Porto Alegre: Artmed. p. 21-36.

Freitas,F;Araujo, M.(2008). *Políticas de Segurança da Informação: Guia prático para elaboração e implementação*. 2ed. Rio de Janeiro: Ciência Moderna LTDA.

Frisch, E. (2002). Essential System Administration, 3rd Edition. O´Reilly Media.

Godoy, C. L. B.(2008). *A Liberdade da Imprensa e os Direitos da Personalidade*. 2. ed. São Paulo: Atlas.

Gonçalves, E. L. (2015). *Políticas de Segurança da Informação*. Rio de Janeiro: RNP/ESR.

Greenberg, J.(1963). *Universals of Human Language, 73-113*. Cambridge, Mass: MIT Press.

Hayes, R M. (1999); *History review: the development of Information Science in the United States*. In: Bowden, M.E. et al. (ed.) Proceedings of the 1998 Conference on the History and Heritage of Science Information Systems. p. 223-236.

Hefferan, R. (2000). *BS 7799 – Information Security Management*. http://www.istc.org.uk [Consulta em 04/07/18]

Internacional Organization For Standardisation. DRAFT BS7799-2:2002 (2001): *Information security management – specification for information security management systems*. British Standard Institute, Londom.

Internacional Organization For Standardisation. ISO/IEC 15408-n. (1999*). Information Technology - Security Techniques – Evaluation Criteria for IT Security.* International Organization fo Standardization, Switzerland.

International Organization For Standardisation. ISO/IEC TR 13335-n (1998). *Guidelines for the Management of IT Security (GMITS). I*nternational Organization for Standardization, Switzerland.

Jordão, T.C. (2009). A *formação do professor para a educação em um mundo digital*. In: Tecnologias digitais na educação. Boletim 19 Salto para o futuro, Nov/Dez, Brasília: MEC.

Júnior, A. R. (2009).*Liberdade de Expressão e Liberdade de Informação*. Curitiba: Juruá, 2009.

Júnior, W. F. C.(2005). *Inteligência empresarial estratégica*. Tubarão:Ed. Unisul.

Krause, M ; Tipton, H. F. (1999). *Handbook of Information Security Management. Auerbach Publications*.

Libâneo, J. C. (2007). *Educação Escolar: políticas, estrutura e organização*. Coleção Docência em Formação. 5. ed. São Paulo: Cortez.

Lopes, J. J. (2004). *A introdução da informática no ambiente escolar*. http://www.clubedoprofessor.com.br/artigos/artigojunio.htm. [Consulta em 12/11/18].

Lüdke, M.; André, M.E.D.A. (1986). *Pesquisa em educação: abordagens qualitativas*. São Paulo: EPU.

Martins, A. B.; Santos. C.A.S. (2005). *Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação*. Revista de Gestão e Tecnologia e Sistema de Informação. Vol. 2, No. 2.

Moreira, S. V. (2005). *Análise documental como método e como técnica*. São Paulo:Atlas.

Oliveira, A. A. P. (2007). *Análise documental do processo de capacitação dos multiplicadores do projeto "Nossas crianças: Janelas de oportunidades"* 2007. Universidade de São Paulo, SP.

Oliveira, E. http://www.infoescola.com/sociedade/estudo-de-caso/[consulta em 21/05/17].

Ralph, M. S.; George W. R.(1998). *Princípios de sistemas de informação*. Rio de Janeiro: LTC.

Rezende, D.; Abreu, A. F. de. (2000). *Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas*. São Paulo: Atlas.

Santos, A. R. (2000). *Metodologia Científica: a construção do conhecimento*. 3. ed. Rio de Janeiro: DP&A.

Schneier, B. (2001). *Segurança.com: segredos e mentiras sobre a proteção na vida digita*l - Rio de Janeiro: Campus.

Shera, J. H., Cleveland, D. B. (1977). *História e fundamentos da Ciência da Informação*.Revisão Anual da Ciência e Tecnologia da Informação (ARIST) Washington. n.12, p.249-275.

TCU. (2007). Tribunal de Contas da União. *Manual de Boas Práticas em Segurança da Informação.* Brasília:TCU.

TCU. (2012). Tribunal de Contas da União. *Boas práticas em Segurança da Informação.* Brasília:TCU, Secretaria de Fiscalização de Tecnologia da Informação.

Toigo, J. W. (2003). *Disaster recovery planning: preparing for the unthinkable*. 3rd ed. New jersey: Prentice Hall, PTR.

Triviños, A. N. S. (1987). *Introdução à pesquisa em ciências sociais: A pesquisa* qualitativa em educação. São Paulo, SP: Atlas.

Wadlow, T. (2000). Segurança de Redes. Editora Campus. Rio de Janeiro.

Wang, A. J. A. (2006). *IT Education in the Flattening World. Paper presented at the SIGITE'0*6: ACM Special Interest Group for Information Technology Education, Minneapolis, MN, October, 19-21.

Wurman, R.S. (1991). *Ansiedade de Informação.* São Paulo: Cultura Editores Associados.

Yin, R. K. (2001). Estudo de caso: *Planejamento e métodos*. Porto Alegre, RS: Bookman.

Legislação consultada

Constituição da República Federativa do Brasil de 1988. (2016). Senado Federal, Coordenação de Edições Técnicas. Brasília: Senado Federal.

Decreto n° 678, de 6 de novembro de 1992 (1992). Promulga a Convenção Americana sobre Direitos Humanos. Diário Oficial da União. Brasília. DF.

Decreto-Lei nº 43, de 03 de fevereiro de 1989 (1989). Dispõe sobre o regime jurídico da autonomia das escolas. Diário Oficial da União. Brasília. DF.

Decreto-Lei nº 115-A, de 04 de maio de 1998 (1998). Dispõe sobre o regime de autonomia, administração e gestão dos estabelecimentos de ensino. Diário Oficial da União. Brasília. DF.

Decreto Nº 3.505, de 13 de junho de 2000 (2000) da Presidência da República, institui a Política de Segurança da Informação. Diário Oficial da União. Brasília. DF.

Lei n. 9.394, de 20 de dezembro de 1996 (1996). Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União. Brasília. DF.

Lei n. 11.892, de 29 de dezembro de 2008 (2008). Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, Brasil. Recuperado em 30 de outubro, 2017, de http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm

Lei n. 12.965, de 23 de abril de 2014 (2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Recuperado em 13 de março de 2019.

Lei n. 13.709, de 14 de agosto de 2018 (2018). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Recuperado em 13 de março de 2019.

Plano Nacional de Educação 2014-2024. (2014), http://www.observatoriodopne.org.br/uploads/reference/file/439/documento-referencia.pdf. Recuperado em 19 de junho de 2017.

Tribunal de Contas da União, Acórdão 1.233/2012. Plenário. Rel. Ministro Aroldo Cedraz. Sessão de 23/05/2012. http://porta.tcu.gov.br/pesquisaJurisprudencia/#/pesquisa/acordaocompleto. Recuperado em 21 de maio de 2017.

Tribunal de Contas da União, Acórdão 3.051/2014. Plenário. Rel. Ministro Substituto Weder de Oliveira. Sessão de 05/11/2014.

Anexos

I – Instrumento de Coleta de Dados: Questionário

II – Eixo Tecnológico por Campi

Anexo I – Instrumento de Coleta de Dados

Mestrado em Ciência da Educação/Administração Escolar

Prezado (a) Docente,

este questionário servirá de insumo para minha dissertação de Mestrado em Ciência da Educação/Administração Educacional, que é oriundo de uma parceria entre o Instituto Federal e o Instituto Politécnico de Santarém - Portugal.

É um questionário com 10 (dez) questões e tem por objetivo verificar como os docentes vivenciam o tema Segurança da Informação neste Instituto Federal.

A confidencialidade, tanto da resposta quanto da assinatura, será preservada conforme as normas e preceitos da ética na pesquisa.

De forma antecipada, agradeço-lhe pelo apoio e por ter compartilhado comigo sua visão sobre o tema!

Edimária Lamounier
Tecnóloga em Redes de Computadores

Questionário

1. Proteger os estudantes em um ambiente virtual é um papel da instituição de ensino. Você concorda que a escola defina critérios para liberar ou negar acesso a ferramentas disponíveis na internet, efetivar a blindagem de certos sites, dentre outras ações?
   ( ) Sim.
   ( ) Não.
   Justifique: _____
2. Em seu entendimento, o que é ter livre acesso à informação na internet no âmbito de uma Instituição Federal de Ensino?
   a) Navegar na internet podendo acessar todo e qualquer tipo de sítio, ou seja, sem qualquer restrição.
   b) Navegar na internet podendo acessar todo e qualquer tipo de sítio, com exceção daqueles de temas impróprios, a exemplo dos de cunho racista, de pornografia infantil, dentre outros do tipo.
   c) Navegar na internet podendo acessar apenas os sítios considerados próprios para a Instituição.
   d) Outro Conceito.

Comente sua resposta: _____

3. No universo de segurança da informação, o que lhe é mais preocupante?
   Invasões por hackers e vulnerabilidades em sistemas.
   a) Ausência de um bom antivírus, um firewall e ter todas as suas atualizações aplicadas no ambiente tecnológico.
   b) O fator humano, uma vez que as pessoas constituem a parte mais vulnerável no escopo da segurança da informação.
   c) Ausência de regras e de ferramentas de monitoramento e de bloqueios de sites indevidos.
   d) Outras questões.

   Explique sua resposta:

   _____

4. Em algum momento de sua experiência de docente você já foi questionado pelos pais ou pela comunidade se o acesso à internet é restrito ou se é tudo liberado durante as aulas de laboratório?

   0 1 2 3 4 5 6 7 8 9 10

   (Nenhuma) (igual ou acima de 10)

   Caso queira comentar a respeito, fique à vontade.

   _____

5. Em sua visão e com base em sua experiência como docente, a implementação de regras de controle de acesso à internet ajuda ou confunde a dinamização das aulas?
   ( ) Ajuda.
   ( ) Confunde.
   ( ) Outro.
   Como? _____

6. Enquanto docente que faz uso das tecnologias educacionais, há de sua parte a preocupação quanto aos riscos e aos crimes virtuais que podem ocorrer durante suas aulas?
   ( ) Sim.
   ( ) Não.

   Você acredita que pode ser responsabilizado numa situação como essa?
   ( ) Sim.

( ) Não.

( ) Não sei.

Quais as razões para sua resposta?

_____

7. A instituição já lhe ofereceu capacitação sobre o tema Segurança da Informação?

   ( ) Sim.

   ( ) Não.

   Por quantas capacitações você já passou sobre Segurança da Informação?

   0 1 2 3 4 5 6 7 8 9 10

8. Considera que ter uma Política de Segurança da Informação é importante para o órgão?

   ( ) Sim.

   ( ) Não.

   Justifique sua resposta: _____

9. Relativamente à Política de Segurança da Informação (PSI) do órgão indique o seu grau de conhecimento:

   ( ) Muito elevado.

   ( ) Elevado.

   ( ) Suficiente.

   ( ) Insuficiente.

   ( ) Inexistente.

   Indique a (s) razão (ões) para sua resposta.

   ( ) Não vejo porque conhecê-la.

   ( ) Sei que existe, mas nunca a li.

   ( ) Conheço-a superficialmente.

   ( ) Conheço bem esse documento, pois considero-o de extrema importância.

   ( ) Outra (s) razão (ões).

   Fale sobre sua escolha:

   _____

10. Em sua opinião, qual o grau de efetividade da PSI (Política de Segurança da Informação)?

    ( ) Muito elevado.

    ( ) Elevado.

    ( ) Suficiente.

    ( ) Insuficiente.

    ( ) Inexistente.

    Comente sua escolha:

    _____

Anexo II – Eixo Tecnológico por Campus

EIXO TECNOLÓGICO POR CAMPUS

	Campus Central	Campus Rural	Campus Urbano 1	Campus Urbano 2	Campus Urbano 3	Campus Urbano 4	Campus Urbano 5	Campus Urbano 6	Campus Urbano 7	Campus Urbano 8
Cursos Técnicos Integrados ao Ensino Médio	Técnico em Eventos	Técnico em Agropecuária	Técnico em Eletrônica	Técnico em Manutenção Automotiva	Técnico em Alimentos	Técnico em Produção em Áudio e Vídeo	Técnico em Cozinha	Técnico em Controle Ambiental	Técnico em Administração	Técnico em Eletromecânica
	Técnico em Informática				Técnico em Química		Técnico em Hospedagem	Técnico em Design de Móveis	Técnico em Secretariado	
Cursos Técnicos Subsequentes	Técnico em Comércio	Técnico em Agroindústria	Técnico em Eletrônica	Técnico em Manutenção Automotiva	Técnico em Logística	Técnico em Produção de Áudio e Vídeo	Técnico em Cozinha	Técnico em Controle Ambiental	Técnico em Secretaria Escolar	Técnico em Eletromecânica
	Técnico em Eventos	Técnico em Agropecuária	Técnico em Equipamentos Biomédicos				Técnico em Panificação	Técnico em Edificações	Técnico em Secretariado	Técnico em Manutenção e Suporte em Informática
	Técnico em Informática: Desenvolvimento de Sistemas		Técnico em Segurança do Trabalho (modalidade a distância)					Técnico em Móveis		Técnico em Vestuário
	Técnico em Serviços Públicos									

	Campus Central	Campus Rural	Campus Urbano 1	Campus Urbano 2	Campus Urbano 3	Campus Urbano 4	Campus Urbano 5	Campus Urbano 6	Campus Urbano 7	Campus Urbano 8
Cursos Técnicos da modalidade Educação de Jovens e Adultos (PROEJA)				Técnico em Reciclagem	Técnico em Administração	Técnico em Produção de Áudio e Vídeo	Técnico em Restaurante e Bar	Técnico em Edificações	Técnico em Secretariado	Técnico em Artesanato
Cursos Superiores - Graduação - Bacharelado					Administração					Ciências da Computação
Cursos Superiores - Graduação - Licenciatura	Dança	Biologia	Letras - Língua Espanhola	Matemática	Química		Letras - Inglês Geografia	Educação Profissional	Língua Portuguesa e Pedagogia	Computação Física
Cursos Superiores - Graduação - Tecnologia	Eventos e Gestão Pública e Processos Gerenciais e Sistemas para Internet	Agroecologia			Alimentos e Logística		Gastronomia		Secretariado	Automação Industrial e Desing de Modas
Curso Superiores - Especialização	Especialização em Gestão Pública: Governança e Políticas Públicas		Esp. em Segurança Pública				Esp. em Ensino de Humanidades e Linguagem			

	Campus Central	Campus Rural	Campus Urbano 1	Campus Urbano 2	Campus Urbano 3	Campus Urbano 4	Campus Urbano 5	Campus Urbano 6	Campus Urbano 7	Campus Urbano 8
Curso Superiores - Mestrado	Mestrado Profissional em Educação Profissional e Tecnológica em Rede Nacional									
Cursos de Formação Inicial e Continuada (FIC)	Auxiliar de Marketing	Auxiliar de Produção Animal (PROEJA)	Cadista para a construção civil	Auxiliar Administrativo	Boas práticas e noções de controle de qualidade de alimentos	Alfabetização e Letramento para a terceira idade	Agente de Recepção e Reservas em Meios de Hospedagem		Assistente Administrativo	Libras Básico
	Espanhol	Horticultor (PROEJA)	Canto coral para a terceira idade	Educador Infantil	Ensino de Ciências para os anos iniciais do ensino fundamental	Informática Básica	Informática		Monitor Infantil	Libras Intermediário
		Libras Básico Saúde	Doula	Espanhol Básico	Libras Básico	Inglês Básico I	Libras Básico - Turmas I e II		Operador de Computador	

	Campus Central	Campus Rural	Campus Urbano 1	Campus Urbano 2	Campus Urbano 3	Campus Urbano 4	Campus Urbano 5	Campus Urbano 6	Campus Urbano 7	Campus Urbano 8
Cursos de Formação Inicial e Continuada (FIC)		Teclado Básico	Espanhol Básico	Inglês Básico	Libras Intermediário	Inglês Básico II	Libras Intermediário		Programador de Dispositivos Móveis	
			Espanhol Intermediário	Libras	Língua Estrangeira Aplicada ao Trabalho - Espanhol	Libras Básico I			Viveiricultora	
			Informática básica para a terceira idade	Preparatório para o Enem	Processamento de frutas e hortaliças	Libras Básico II				
				Preparatório para o Enceja		Musicalização ao Violão-Iniciação 1				
				Tecnologias de Informação e Comunicação para a maturidade		Preparatório para o Enem				
						Recreador				