SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DAS DIRETRIZES DE SEGURANÇA IMPLEMENTADAS PELOS RECURSOS HUMANOS EM ESCOLAS MUNICIPAIS DAS CIDADES DE TIMON-MA, TERESINA E NAZÁRIA NO PIAUÍ.

Antonio Brito dos Santos[1]
Stephenson de Sousa Galvão[2]

RESUMO

Com o eminente avanço tecnológico batendo a porta dos profissionais da área da educação quase que diariamente, é necessário que haja um processo de recrutamento e treinamento cada vez mais eficiente a fim de garantir uma maior eficácia na prática da segurança da informação dentro das escolas. Visando conhecer esse processo de recrutamento e treinamento desenvolvido nas escolas de educação básica (educação infantil até o quinto ano do ensino fundamental) de Timon-MA, Teresina e Nazária no estado do Piauí, este trabalho pretende verificar se controles básicos recomendados pela ISO 27001 e 27002, para garantir a segurança da informação nas organizações, são aplicados de maneira eficiente. Para isso uma pesquisa de cunho descritivo e com uma abordagem quantitativa dos dados foi realizada, onde ouve a aplicação de um questionário com perguntas diretas e objetivas junto aos servidores das escolas (diretores, professores e secretários), elaboradas a partir da seção sétima da ISO 27002, que faz recomendações ao setor de recursos humanos, para implementar diretrizes que garantam a eficácia da pratica da segurança da informação tanto para novos como para antigos colaboradores. Os resultados apontaram que, a prática de segurança da informação nessas escolas ainda é muito deficiente, pois mais de 50% dos pesquisados revelaram que não existe um treinamento voltado para a área de segurança da informação, e mais de 70% informaram que não existe se quer campanhas educativas para incentivar a prática da segurança da informação dentro da escola.

Palavras-chave: Sigilo de dados. Normativas da ABNT – ISO 27001 e 27002. Segurança da informação.

ABSTRACT

With the eminent technological advance knocking the door of education professionals almost daily, it is necessary to have an increasingly efficient recruitment and training process in order to ensure greater effectiveness in the practice of information security within schools. Aiming to know this process of

[1] Graduando de Licenciatura em Informática. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. antonyobryto@hotmail.com.

[2] Professor do curso de Licenciatura em Informática do Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. sgalvao@ifpi.edu.br.

recruitment and training developed in basic education schools (child education up to the fifth year of elementary school) in Timon-MA, Teresina and Nazária in the state of Piauí, this work intends to verify if basic controls recommended by ISO 27001 and 27002, to ensure information security in organizations, are applied efficiently. For this, a descriptive research with a quantitative approach to the data was carried out, where a questionnaire with direct and objective questions was applied to the servers of the schools (principals, teachers and secretaries), prepared from the seventh section of the ISO 27002, which makes recommendations to the human resources sector, to implement guidelines that guarantee the effectiveness of the information security practice for both new and old employees. The results showed that the practice of information security in these schools is still very deficient, as more than 50% of those surveyed revealed that there is no training focused on the area of information security, and more than 70% reported that there is no wants educational campaigns to encourage the practice of information security within the school.

Keywords: Data secrecy. ABNT regulations – ISO 27001 and 27002. Information security.

1 INTRODUÇÃO

De acordo com a norma da ABN[3] 27001, a segurança da informação entende-se como a "preservação da confidencialidade, integridade e disponibilidade da informação" (ISO/IEC 27001, 2006, p.10). Requisitos importantes para qualquer organização, pois é com a informação que os processos organizacionais funcionam, a geração de conhecimento acontece e o compartilhamento desse conhecimento é realizado. Dessa forma, "falhas na segurança da informação podem representar tanto prejuízos financeiros como danos à imagem das organizações" (POSTHUMUS; VON SOLMS, 2004).

> Os potenciais prejuízos causados por um incidente de segurança da informação somam perdas financeiras, desgaste da imagem, perda na qualidade dos serviços prestados, insatisfação dos colaboradores e clientes, perda de recursos entre outros. (Sêmola, 2003).

Com as instituições de ensino não é diferente, as informações sobre sua tutela, como identificação de alunos, funcionários, diários escolares, notas, entre outros, são fundamentais para um ensino de qualidade. Além disso, os documentos coletados e produzidos por uma escola ao longo do tempo contêm um grande potencial informativo, capaz de fornecer informações sensíveis,

[3] ABNT: Associação Brasileira de Normas Técnicas.

como informações financeiras ou informações altamente confidenciais, e falhas na guarda dessas informações podem acarretar prejuízos administrativos e financeiros incalculáveis para todos. Capacitar pessoas para garantir a proteção dessas informações é algo essencial esperado por todos que fornecem seus dados às escolas. As instituições de ensino da educação básica (séries iniciais) são as que mais coletam informações pessoais no ato da matricula, para isso precisam ter pessoas ainda mais capacitadas a fim de garantir uma maior proteção a essas informações.

Devido a essa importância, algumas empresas têm investido em seus sistemas digitais de informação. De acordo com um estudo divulgado pelo Gartner Group[4], (Gartner, 2018) mostrou que "os gastos mundiais com segurança da informação em 2018 podiam chegar a US$ 96,3 bilhões, e em 2019 75% dos gastos em segurança da informação seria voltado para serviços de terceirização de segurança, como produtos de software e hardware". Entretanto, segundo outra pesquisa feita pelo Grupo Stefanini, Consultoria e Assessoria em Informática S/A relata que:

> "Os investimentos em segurança da informação, que visam à proteção dos ativos das organizações, não podem ser voltados em sua maior parcela apenas para falhas nos sistemas, mas também para a capacitação das pessoas que têm acesso a eles". (STEFANINI, 2020).

Uma ferramenta muito importante no auxílio à segurança da informação é o Sistema de Gestão de Segurança da Informação (SGSI), que para a ABNT 27001 (ISO/IEC 2006, p.5), é: "a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação". A ABNT 27002 (ISO/IEC 2013, p.17) também estabelece de maneira mais direta em sua seção sétima, que trata da segurança em recursos humanos, que se deve "Assegurar que funcionários e partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais eles foram selecionados".

[4] Gartner Group: instituto de pesquisa e consultoria na área tecnologia da informação reconhecido e respeitado mundialmente.

Ainda segundo a própria norma, para estabelecer um SGSI é necessário à elaboração de um propósito que venha disponibilizar requisitos para implementar, operar, monitorar, efetuar uma análise crítica, mantendo e melhorando de forma contínua esse Sistema de Gestão de Segurança da Informação, ficando sempre atualizado com as atuais características da organização. Esse SGSI é um conjunto de controles implementados pela organização para proteger suas informações e ativos aos quais ela é detentora.

Diante do exposto, será que as instituições de ensino possuem um Sistema de Gestão de Segurança da Informação para proteger as informações a ela confiadas, e se o setor responsável pela contratação, treinamento de novos e antigos funcionários adotam controles de segurança recomendados pela ISO 27002 em sua seção sétima? Visando responder essa pergunta, este trabalho pretende analisar se procedimentos de segurança da informação, recomendados pela seção sétima da ISO 27002, são implementados por algumas escolas da educação básica da rede municipal de Timon-MA, Teresina e Nazária no Piauí. Para isso, fez um levantamento bibliográfico das principais orientações de segurança da informação direcionadas aos recursos humanos e verificou se estas orientações são adotadas pela escola, também analisou se procedimentos de segurança da informação, relacionadas a este mesmo setor, está de acordo com as principais orientações sugeridas pela literatura que venha a garantir uma maior segurança na hora do tratamento de dados[5] feito pela escola.

A grande quantidade de informações coletadas pelas escolas municipais de educação básica (séries iniciais) no ato da matrícula de um aluno, trás consigo uma preocupação, se procedimentos básicos na área de segurança da informação são aplicados na hora da contratação e treinamento de colaboradores novos e veteranos, com a finalidade de garantir a segurança dessas informações. Outro fator que chama atenção é que pouco se fala em segurança da informação nestas instituições de ensino. Uma pesquisa de cunho descritiva que vise o levantamento de dados e que venha esclarecer

[5] Tratamento de dados é qualquer atividade realizada com dados pessoais, informações que sozinhas, ou em conjunto com outras, permite identificar uma pessoa. Atualmente, o processo de tratamento de dados é regulamentado e protegido pela LGPD, Lei Geral de Proteção de Dados Pessoais.

esse questionamento torna-se necessária, pois o atual momento de evolução tecnológica requer uma preocupação cada vez maior com segurança das informações.

Para a realização deste trabalho ouve uma divisão em etapas para uma melhor compreensão de tudo que foi feito no decorrer de sua elaboração, que trás a seguir seu referencial teórico com seus embasamentos legais e contribuições de trabalhos já realizados e relacionados ao assunto, posteriormente trás a metodologia utilizada na elaboração do questionário para a coleta de dados.

2 ABORDAGEM DO REFERENCIAL TEÓRICO

Com a finalidade de expor os principais embasamentos literários que guiaram a elaboração do trabalho e para uma melhor compreensão do assunto que se caracteriza a seguir, fez-se uma divisão com os principais tópicos abordados que se caracterizam a seguir.

2.1 SEGURANÇA DA INFORMAÇÃO

A informação é algo muito valioso e desejado não só para uma pessoa, mas também para uma organização, devendo está protegida obrigatoriamente de acesso não autorizado. Sêmola (2003, p. 9) conceitua Segurança da Informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Para Ferreira, a Segurança da Informação:

> Protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades. (2003, p.162)

Ainda sobre segurança da informação, Tanenbaum (2003) destaca que, “em rede de computadores a segurança é a preocupação em garantir que pessoas mal-intencionadas não consigam ler ou modificar secretamente qualquer informação enviada a outro destinatário”.

2.2 NORMATIVAS DA ABNT – ISO 27001 E 27002

Este trabalho tem como base de estudo os princípios básicos do Sistema de Gestão de Segurança da Informação - SGSI (ISO 27001 e 27002),

e em especial sua seção sétima da ISO 27002 que trata da segurança em recursos humanos, e que define e gerencia os controles que uma organização precisa implementar junto aos seus colaboradores, antes, durante e depois da contratação, para garantir que estejam protegendo de forma sensata suas informações, pois a LGPD que é a sigla para Lei Geral de Proteção de Dados do Brasil trouxe em sua redação regras para dar às pessoas maior controle sobre suas próprias informações e estabelece também regras para empresas e organizações sobre coleta, uso, armazenamento e compartilhamento de dados pessoais, impondo multas e sanções no caso de descumprimento, com a finalidade de garantir uma maior eficácia nos requisitos básicos de segurança de informações.

> Convém que as informações sobre todos os candidatos que estão sendo considerados para certas posições dentro da organização, sejam levantadas e tratadas de acordo com a legislação apropriada existente na jurisdição pertinente. (ISO/IEC 27002, 2013, p.18).

As escolas devem se preocupar com a segurança da informação, pois as informações coletadas e armazenadas por elas são utilizadas por seus colaborados. Vale ressaltar que a segurança da informação aplicada aos recursos humanos é um processo que precisa ser constantemente atualizado de acordo com as políticas atuais da instituição. A partir do exposto, Gouvêa (2010), diz que:

> Partindo do princípio de que não existe zero por cento de risco, por mais que todas as portas estejam protegidas e que os processos sejam bem estruturados, há normas e código de ética, dando origem ao “elo” mais fraco da segurança – as pessoas. Não há maior vulnerabilidade que o funcionário insatisfeito, ou seja, todo o imenso investimento para proteger as informações cruciais pode ser prejudicial se a companhia descuidar do que ela tem de mais importante – os profissionais que ali trabalham. (GOUVÊA 2010, p. 01).

2.3 NORMATIVA DA ABNT ISO 27002 APLICADA AO SETOR DE RECURSOS HUMANOS

O setor de recursos humanos deve garantir uma maior eficácia na hora da seleção de candidatos que irão ser empossados aos cargos, a ISO 27002

estabelece um dos controles básicos e essencial a ser adotado para essa finalidade seja:

> “Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.” (ISO/IEC 27002, 2013, p.17).

Cabe também aos recursos humanos a adoção de políticas específicas no campo da segurança da informação, como o treinamento não só de novos colaboradores, mas também daqueles que já fazem parte do quadro de funcionário, fazendo com que melhorias significativas no nível de segurança da informação sejam adotadas. Um treinamento adequado, em consonância com a adoção de um comportamento que visa garantir uma maior segurança no tratamento de dados pode aumentar o nível de segurança que uma escola usa para garantir a guarda de suas informações.

> A segurança da informação não se resume apenas a dados, papéis ou meios de armazenamento, é necessário a existência de normas dentro de uma organização que determine quem, como, quando e onde possa ter acesso a sistemas, arquivos ou documentos (SÊMOLA, 2003; STALLINGS, 1999; MARCIANO, 2006).

A escola também deve deixar bem claro que se preocupa e leva a sério a proteção das informações sobre sua tutela, conscientizando seus colaboradores dos perigos existentes e dos riscos que a falta de cuidados adequado dentro da escola pode causar. É recomendado também que se elabore um código de conduta dentro da instituição de ensino, de acordo com seus princípios, com processo disciplinar a serem aplicadas caso algum colaborador venha a cometer uma violação de segurança da informação. Segundo a (ISO/IEC 27002, 2013, p.21) “Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.”

As informações armazenadas pelas escolas de educação básica necessita de pessoas cada vez mais comprometidas e treinadas para desenvolver um bom trabalho na sua guarda e sigilo. A política de segurança adotada por cada instituição bem como funcionários bem capacitados e cientes

de suas responsabilidades e funções faz com que haja um controle mais adequado a fim de garantir a confidencialidade no tratamento dos dados.

> “Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.” (ISO/IEC 27002, 2013, p.20).

A adoção dos procedimentos mencionados anteriormente faz com que todos os colaboradores submetidos a eles fiquem sempre atualizados com as atuais políticas de segurança adotada pela escola, aumentando assim a segurança dos dados que estão sobre a responsabilidade dela.

3 METODOLOGIA

A natureza da pesquisa caracteriza-se como descritiva, pois tem como objetivo fazer um levantamento do comportamento humano, abordando seus principais níveis de conhecimento e treinamento no campo da segurança da informação, e descrevendo suas fragilidades. Segundo Gil (1991, p. 45) pesquisas descritivas “objetiva descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Envolve o uso de técnicas padroniza das de coleta de dados: questionário e observação sistemática”.

A abordagem utilizada na pesquisa foi a quantitativa, que fez um levantamento com a finalidade de buscar uma realidade estatísticas do problema, pois segundo (GATTI, 2004), “pesquisas com abordagem quantitativa em educação proporciona maiores condições de analisar quantitativamente questões investigadas”. Também é através da abordagem quantitativa que é possível mensurar e quantificar as respostas dos pesquisados e obter dados que vão confirmar ou contestar as hipóteses iniciais.

3.1 DESCRIÇÃO DO ESPAÇO E PÚBLICO ALVO DA PESQUISA

O público alvo foram diretores, professores e secretários da educação básica (séries iniciais) das escolas municipais de Timon-MA, Teresina e Nazária no estado do Piauí. Eles foram convidados a responder um questionário com perguntas objetivas e diretas, este questionário foi capaz de identificá-los profissionalmente e verificar se os procedimentos adotados pelo

setor responsável por recrutar e treinar novos e antigos funcionários foram adequadamente realizados de acordo com as recomendações do SGSI.

As características das escolas escolhidas para a realização da pesquisa foram escolas da rede municipal de ensino da educação básica (séries iniciais), do ensino infantil até o último ano do fundamental, onde três eram da cidade de Timon-MA, três de Teresina-PI e uma da zona rural de Nazária-PI. As escolas são caracterizadas também por oferecer um ensino a alunos que ainda são muitos dependentes de seus responsáveis, e por isso são coletados muitos dados considerados sensíveis dos alunos, e em maior quantidade de seus representantes. O processo de escolha das escolas também levou em consideração que, elas exigem que cada aluno precisa ter o cadastro de mais de um responsável por ele.

3.2 ETAPAS DA PESQUISA

As principais etapas para a realização da pesquisa podem ser vistas no Quadro 01, no qual são listadas de acordo com a sua ordem de execução. Nas seções seguintes, cada uma dessas etapas é detalhada.

Quadro 01: Etapas da Metodologia da Pesquisa

Etapa 1	Pesquisa bibliográfica
Etapa 2	Coleta de dados

Fonte: Própria do Autor

3.1.1 Pesquisas bibliográficas

De início, realizou-se uma pesquisa sobre os principais trabalhos que tratam de segurança da informação, controles de segurança da informação e recomendações em segurança da informação para recursos humanos. Essa pesquisa teve como base os livros e normas de renome no assunto e o repositório de artigos da Capes (PERIÓDICOS CAPES, 2021).

Os principais autores que influenciaram esse trabalho foram as normas da ABNT (ISO 27001 e 27002); os livros de Tanenbaum (2003) e Stallings (1999); e a Lei Geral de Proteção do Dados - LGPD. Os livros serviram para conceitos e entendimentos gerais sobre o assunto. As normas serviram para compreender princípios e recomendações básicas de segurança da

informação, principalmente procedimentos utilizados em recursos humanos que podem contribuir para futuras falhas ou violações de segurança. A LGPD serviu para entender conceitos fundamentais de expressões específicas que pudessem auxiliar e aclarar dúvida sobre o processamento de dados.

3.1.2 Coleta de dados

A coleta de dados foi realidade mediante a aplicação de um questionário estruturado elaborado na plataforma *Google Forms*, onde este foi encaminhado via rede social *WhatsApp* para os 19 profissionais envolvidos na pesquisa (diretores, professores e secretários) de 7 escolas públicas municipais, sendo 3 da cidade de Timon-MA, 3 de Teresina-PI e uma da zona rural de Nazária-PI. Esse questionário foi igual para os três tipos de participantes e ficou disponível para aceitar resposta entre os dias 17 e 21 de janeiro de 2022. Também foi realizado um contato prévio com todos os participantes, para expor o objetivo da pesquisa e sua finalidade, pois Marconi e Lakatos destacam que:

> Junto com o questionário deve-se enviar uma nota ou carta explicando a natureza da pesquisa, sua importância e a necessidade de obter respostas, tentando despertar o interesse do recebedor para que ele preencha e devolva o questionário dentro de um prazo razoável (Marconi e Lakatos 1999, p. 100).

Ainda durante a semana de coleta de dados, também foi realizado quase que diariamente um contato com todos que ainda não haviam respondido o questionário, com a finalidade de aclarar eventuais dúvidas que viessem a surgir sobre sua resolução.

A escolha da plataforma para a elaboração do questionário levou em consideração sua gratuidade, a possibilidade de manter o anonimato do pesquisado e a facilidade de envio para o publico que iria participar da pesquisa, pois segundos Ribeiro (2008) um dos pontos fortes para a realização de uma pesquisa é seus custos e a garantia do anonimato.

Para que o estudo fosse realizado e viesse a produzir os resultados esperados, foi abordada a seção sétima da ISO 27002 para a elaboração do questionário com questões fechadas, explorando os principais requisitos de segurança da informação recomendados por esta seção.

Este questionário teve como finalidade identificar falhas cometidas pelo setor responsável pela seleção e treinamento de novos e antigos funcionários

das escolas de educação básica, falhas essas que podem comprometer a seguranças da informação. As perguntas foram bem objetivas e diretas, onde o participante iria apenas assinalar a resposta mais adequada de acordo com os procedimentos ao qual ele foi submetido. Gil (1999) destaca o seguinte:

> a) as perguntas devem ser formuladas de maneira clara, concreta e precisa;
> b) deve-se levar em consideração o sistema de preferência do interrogado, bem como o seu nível de informação;
> c) a pergunta deve possibilitar uma única interpretação;
> d) a pergunta não deve sugerir respostas;
> e) as perguntas devem referir-se a uma única ideia de cada vez.

A escolha do questionário como técnica de coleta de dados foi adotada, pois foi através dela que os resultados foram colhidos e anotados para que posteriormente fossem transformados em estatísticas quantitativas da pesquisa, pois segundo GIL (2002):

> "A preocupação do pesquisador é a de descrever com precisão essas características, utilizando instrumentos padronizados de coleta de dados, tais como questionários e formulários, que conduzem a resultados de natureza quantitativa".

Os resultados obtidos através da coleta de dados podem ser observados em termos percentuais expostos a seguir, resultados esses que foram capazes de mostrar a importância da segurança da informação para as escolas pesquisadas e se seus funcionários são submetidos a algum treinamento que venha a garantir a segurança das informações.

4 RESULTADOS

Os resultados, a exemplo das etapas anteriores, foram divididos em categorias para uma melhor abordagem e exposição delas. Essas subseções se caracterizam a seguir.

A subseção **caracterização do público envolvido na pesquisa** fez uma abordagem do perfil profissional dos pesquisados e suas respectivas funções dentro da instituição de ensino.

A subseção **requisitos exigidos para ocupar o cargo** abordou o que é preciso comprovar por cada profissional antes que ele possa assumir o cargo ao qual ele foi selecionado.

A subseção **termos e condições de contratação** buscou verificar se cada instituição pesquisada celebrava com cada profissional contratado um termo de responsabilidade.

A subseção **conscientização, educação e treinamento em segurança da informação** buscou verificar se os pesquisados receberam treinamento antes e depois de sua contratação e se eram incentivados a praticar a segurança da informação.

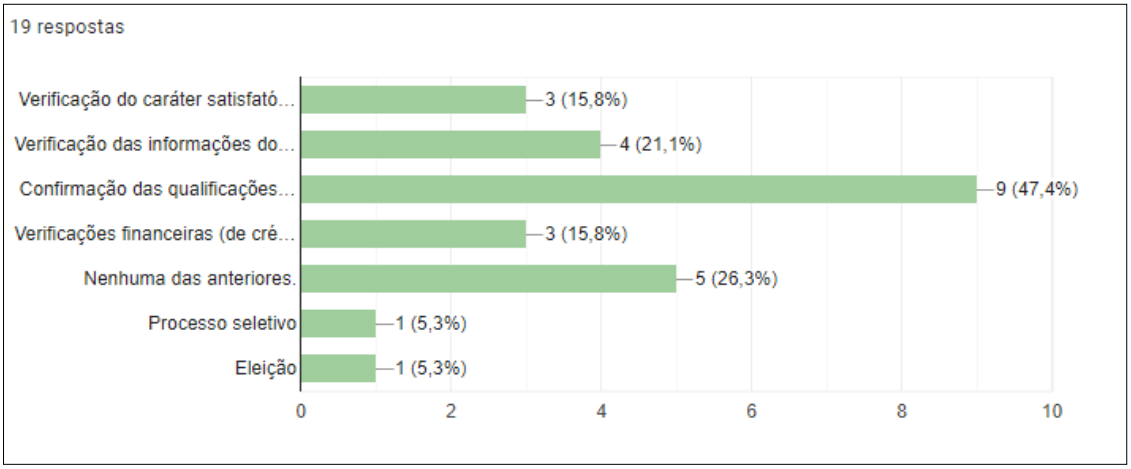
4.1 CARACTERIZAÇÃO ACADÊMICA DO PÚBLICO ENVOLVIDO NA PESQUISA

A pesquisa contou com a participação de 19 profissionais, sendo 7 diretores(as) das escolas pesquisadas, a graduação deles variava entre o curso de licenciatura até o mestrando(a) (36,8% dos pesquisados), 10 foram professores(as) onde a graduação deles variava entre o curso licenciatura até a licenciatura com especialização (52,6% dos pesquisados) e 2 secretários(as) onde a graduação deles variava entre o ensino médio até o curso de bacharel.

4.2 REQUISITOS EXIGIDOS PARA OCUPAR O CARGO

Dos itens implementados e recomendados pela ISO 27002 na sua seção sétima que trata da segurança em recursos humanos, que pede que verificações do histórico sejam realizadas para todos os candidatos ao emprego, 47.4% dos pesquisados responderam que precisaram comprovar apenas sua qualificação acadêmica e profissional para assumir o cargo e 26.3% não precisou comprovar nenhum dos itens recomendados pela ISO 27002. Ficando 21.1% comprovar apenas verificação das informações do curriculum vitae, 15.8% comprovarem o caráter satisfatório, por exemplo, um profissional e um pessoal, 15.8% comprovar verificações financeiras (de crédito) ou verificações de registros criminais e 10.6% não conseguiram assimilar e dar uma resposta satisfatória conforme mostra a Figura 01.

Figura 01: Requisitos necessários para investidura no cargo



Fonte: Google Forms

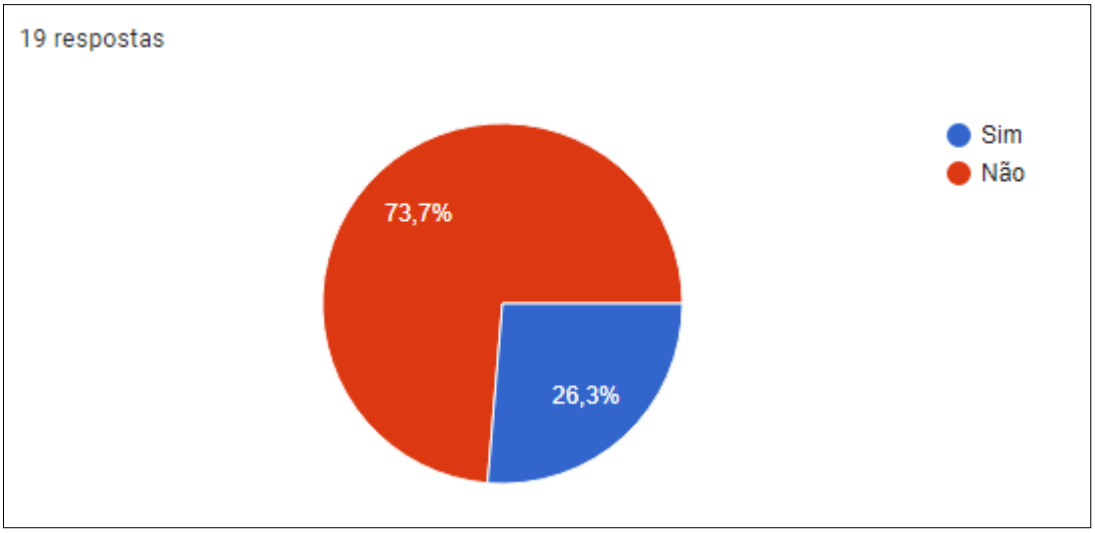
O resultado desta etapa mostrou que a implementação de itens verificação, para garantir a segurança da informação em uma escola, está muito deficiente, uma vez que, algumas escolas não adotam nenhum dos itens recomendados pela ISO 27002 antes da contratação de funcionários.

> a) disponibilidade de referências de caráter satisfatórias, por exemplo uma profissional e uma pessoal;
> b) uma verificação (da exatidão e completeza) das informações do curriculum vitae do candidato;
> c) confirmação das qualificações acadêmicas e profissionais;
> d) verificação independente da identidade (passaporte ou documento similar);
> e) verificações mais detalhadas, tais como verificações financeiras (de crédito) ou verificações de registros criminais. (ISO/IEC 27002, 2013, p.17).

4.3 TERMOS E CONDIÇÕES DE CONTRATAÇÃO

A confidencialidade das informações sobre a tutela das escolas é muito importante, a própria ISO 27002, recomenda a criação de um termo de confidencialidade para que seja celebrado no ato da posse, porém o que pode ser observado, é que 73.7% dos funcionários pesquisados não assinaram esse termo e apenas 26.3% celebraram sua assinatura conforme mostra Figura 02 do gráfico a seguir.

Figura 02: Assinatura de um termo de confidencialidade



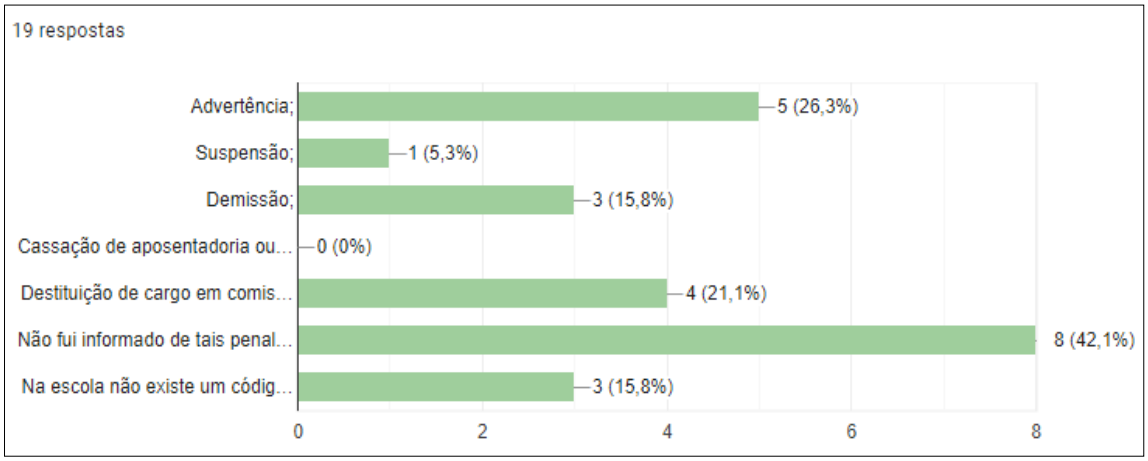
Fonte: Google Forms

> Convém que as obrigações contratuais para funcionários e partes externas, reflitam as políticas para segurança da informação da organização, esclarecendo e declarando:
> a) que todos os funcionários, fornecedores e partes externas que tenham acesso a informações sensíveis assinem um termo de confidencialidade ou de não divulgação, antes de lhes ser dado o acesso aos recursos de processamento da informação (ISO/IEC 27002, 2013, p.18).

Segundo Felix Schultz (2019), o Termo de Confidencialidade tem o objetivo de proteger dados estratégicos da parte contratante, nesse viés, a parte contratada assume o compromisso de não divulgar as informações às quais terá acesso, possuindo a previsão de multa em caso de descumprimento do contrato. Ainda sobre a confidencialidade das informações, a pesquisa mostrou que 42.1% dos pesquisados não são informados que existem penalidades a ser aplicadas caso as regras para garantir a segurança da informação sejam violadas, e 15.8% relataram que não existe um condigo de conduta para estabelecer penalidades a fim de dar maior garantia no comprimento dos controles de segurança. Quanto à existência das principais penalidades administrativas questionadas na pesquisa, 26.3% foram informados sobre a existência de advertência, 15.8% informados da existência de demissão, 21.1% que poderiam ser destituídos do cargo que ocupavam e 5.3% da existência de suspensão. A cassação de aposentadoria e de disponibilidade não foi mencionada suas existências como forma de penalidade

administrativa. Isso mostrou que tais penalidades são poucas adotadas pelas escolas como forma de punições administrativas, conforme mostra Figura 03 do gráfico a seguir.

Figura 03: Penalidades administrativas aplicáveis

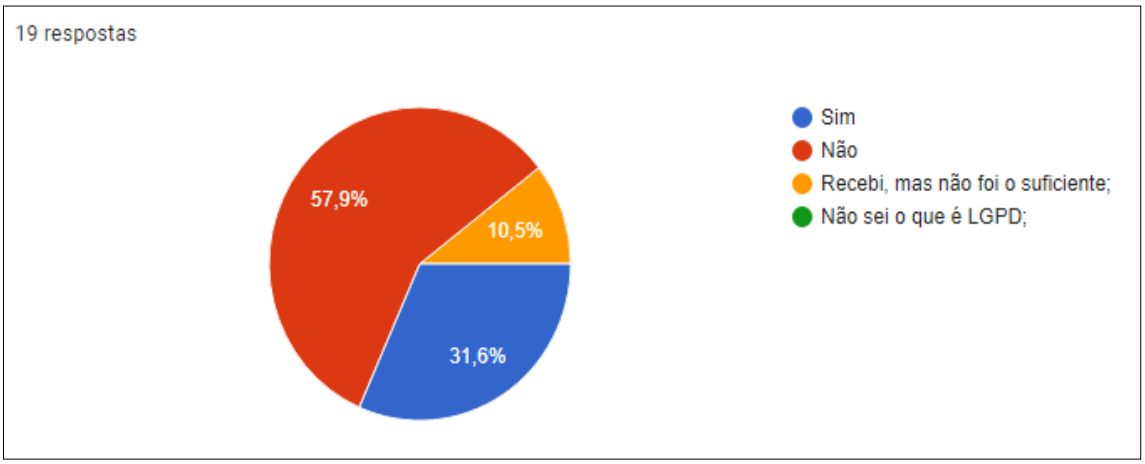


Fonte: Google Forms

4.4 CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO.

A prática da segurança da informação depende de fatores básicos como treinamento e orientações para garantir sua execução, a pesquisa revelou que 57.9% dos pesquisados não receberam treinamento e tão pouco orientações, conforme exige a legislação atual (LGPD), de como proceder de maneira adequada na hora de ter acesso às informações pertencentes à escola. Também foi constatado que 31.6% receberam treinamento e orientações adequadas, 10.5% do total dos pesquisados responderam que receberam treinamento, mas não foi o suficiente, e ninguém informou que desconhece a legislação atual que regula o sigilo das informações (LGPD), conforme mostra Figura 04 do gráfico a seguir.

Figura 04: Recebimento de orientações e treinamento para garantir a segurança da informação.



Fonte: Google Forms

A norma ISO 27002 estabelece que seja implementado um controle que vise o treinamento e conscientização dos colaboradores.

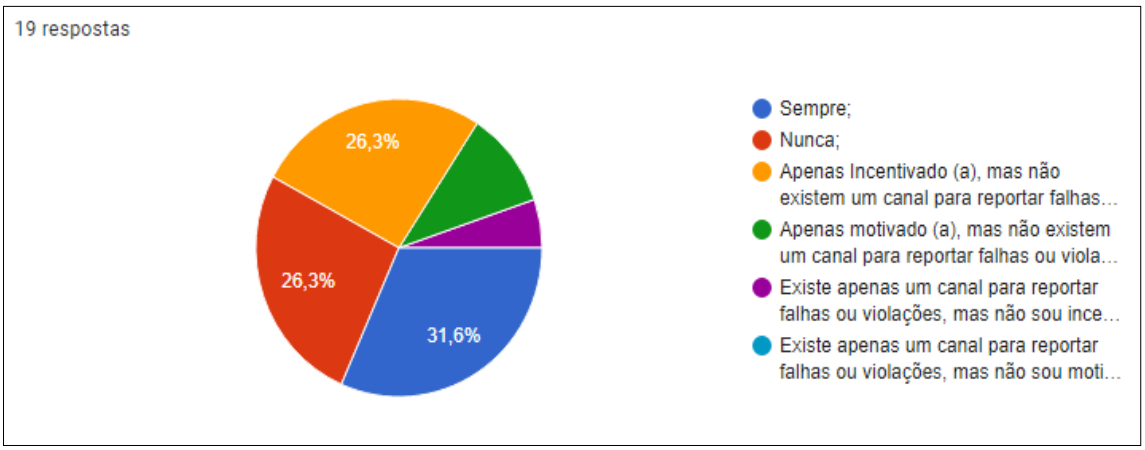
> Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções (ISO/IEC 27002, 2013, p.20).

É importante que, cada escola elabore um programa de conscientização e treinamento de seus colaboradores, garantindo que todos entendam o motivo pelo qual cada controle de segurança foi implementado dentro da escola para que não tentem quebrar nenhuma regra de segurança por mania adquirida ao logo de sua carreira profissional. “A ignorância não pode ser usada como desculpa pelo empregado, pois é exatamente esta vulnerabilidade que os engenheiros sociais vão tentar explorar” (MITNICK & SIMON, 2003; p.198).

No quesito incentivar e motivar os colaboradores a praticarem a segurança da informação e também relatar falhas que venha a ser descoberta dentro da instituição de ensino, 31.6% dos pesquisados responderam que sempre são incentivados a praticarem essas recomendações de segurança da informação, porém 26.3% dos pesquisados responderam que nunca foram incentivados ou motivados a praticarem, e 26.3% disseram que eram apenas incentivados a praticarem, porém não existia um canal para relatar falhas ou violações encontradas. Quanto à existência de um canal para reportar falhas

ou violações, 5.3% relataram sua existência, no entanto, não são incentivados a usa-lo e 10.5% informaram que são incentivados a relatar falhas ou violações de segurança da informação, mas não existe um canal para reportar essas falhas, e quanto à falta de motivação para reportar falhas de seguranças através de um canal específico, ninguém informou sua existência, conforme mostra Figura 05 do gráfico a seguir.

Figura 05: Incentivado e motivado a praticar segurança da informação



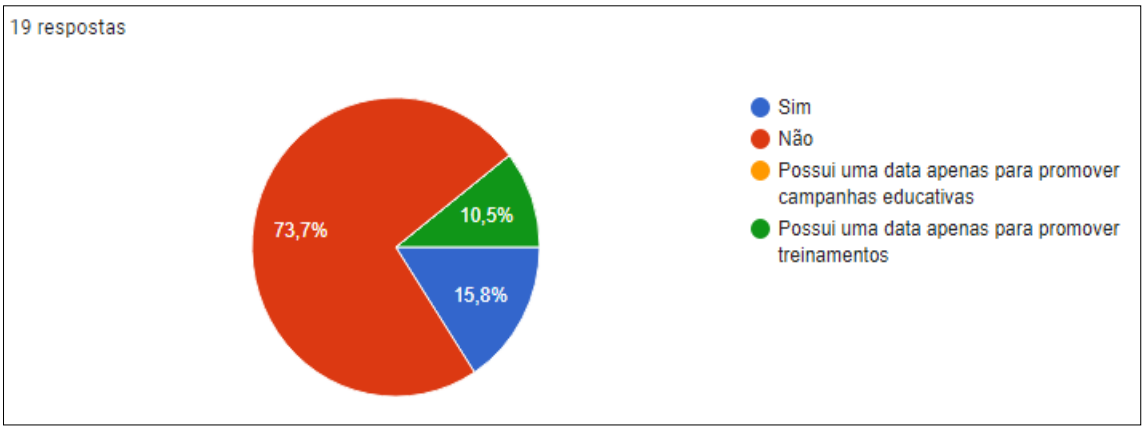
Fonte: Google Forms

A norma recomenda que seja implementado pelo setor de recursos humanos dentro de uma organização um programa para incentivar e motivar todos os colaboradores a praticarem a segurança da informação. “Pessoal motivado pode ser mais confiável e causar menos incidentes de segurança da informação” (ISO/IEC 27002, 2013, p.20). A mesma norma ainda recomenda que seja criado um canal de notificações, de forma anônima, com a finalidade de acolher informações de falha de segurança reportadas por seus colaboradores. “g) tenham disponíveis um canal de notificação, de forma anônima, para reportar violações nas políticas e procedimentos de segurança da informação” (ISO/IEC 27002, 2013, p.19).

A pesquisa ainda mostrou que 73.7% dos pesquisados relataram que não existe se quer campanhas educativas e treinamentos com todos os colaboradores com a finalidade de atualizar e divulgar boas práticas de seguranças da informação e apenas 10.5% dos pesquisados informaram que a escola possui uma data para promover apenas treinamentos. Ainda foi relatado por 15.8% dos pesquisados que, tais práticas questionadas na pergunta são adotadas pela escola, e não teve relatos de que as escolas

possuem uma data específica para promover campanhas educativas e treinamentos com todos os colaboradores com a finalidade de atualizar e divulgar boas práticas de segurança da informação, conforme mostra Figura 06 do gráfico a seguir.

Figura 06: Campanhas educativas e treinamento dos colaboradores



Fonte: Google Forms

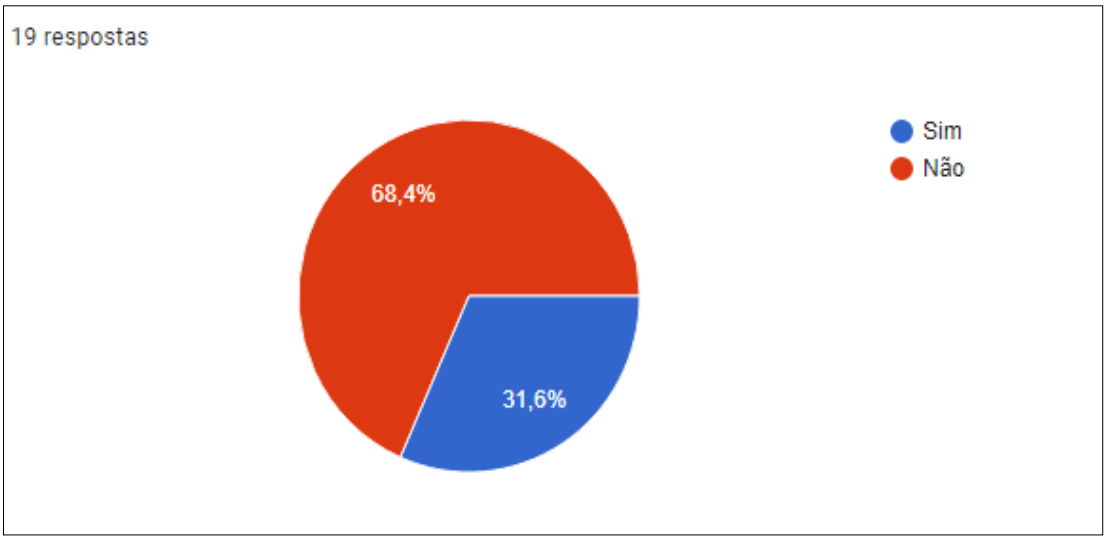
Programas de conscientização, treinamentos e campanhas educativas devem ser implementados pelo setor de recursos humanos na organização com a finalidade de promover a prática da segurança da informação, assim recomenda a ISO 27002 em sua seção sétima.

> Convém que o programa de conscientização considere um número de atividades de conscientização, tais como, campanhas (por exemplo, dia da segurança da informação) e a publicação de boletins ou folhetos (ISO/IEC 27002, 2013, p.20).

A escola pode considerar que o programa de conscientização está alcançando seu objetivo final se todos os seus colaboradores que participaram do treinamento estiverem convencidos e motivados por uma regra básica: “a noção de que a segurança das informações faz parte do seu trabalho” (MITNICK & SIMON, 2003; p.199).

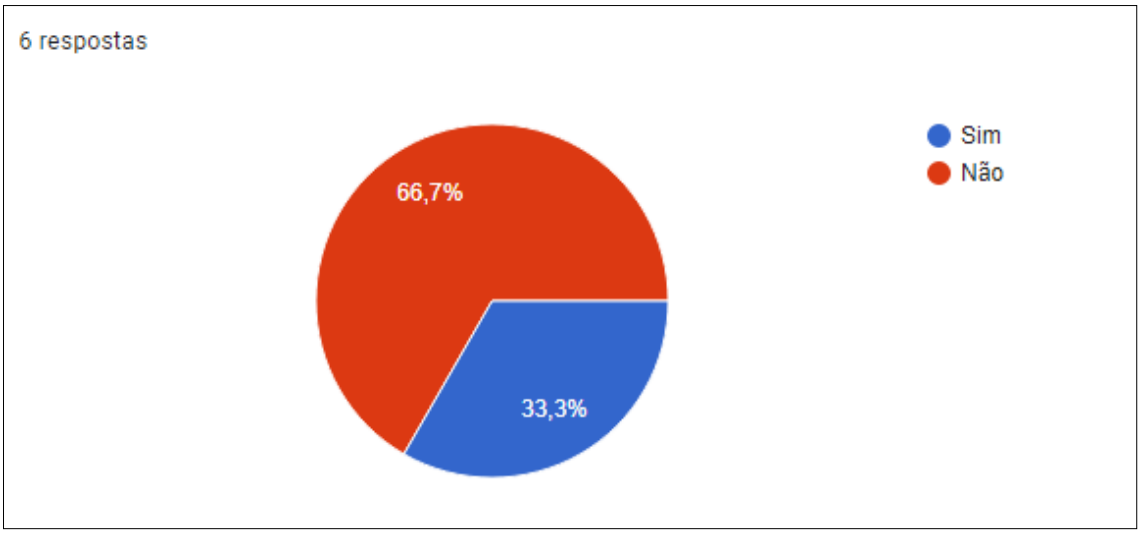
Ainda sobre o treinamento dos colaboradores 31.6% (6 dos 19 pesquisados) relataram que já foram remanejados de suas funções para assumir outra e a apenas 33.3% (2 dos 6 remanejados) deles receberam treinamento para assumir a nova função dentro da escola. Constatou-se também que 68.4% (13 dos 19 pesquisados) informaram que nunca foram remanejados de suas funções e 66.7% (4 dos 6 remanejados) informarão que não receberam treinamento para exercer a nova função, conforme mostra as Figura 07 e 08 dos gráficos a seguir.

Figura 07: Remanejados para exercer outra função



Fonte: Google Forms

Figura 08: Treinamento recebido para exercer a nova função



Fonte: Google Forms

A norma recomenda que sejam implementadas diretrizes para promover o treinamento não só de novos colaboradores, mas também daqueles que forem remanejados de função, transmitindo para todos eles atualizações das políticas de segurança da informação periodicamente.

> Convém que o treinamento e a educação em segurança da informação seja realizado periodicamente. Treinamento e educação iniciais se aplicam aqueles que são transferidos para novas posições ou atribuições com requisitos de segurança da informação completamente diferentes, e não apenas para os novos iniciantes e

> deve ser realizado antes das pessoas assumirem os seus papéis (ISO/IEC 27002, 2013, p.21).

De acordo com Mitnick e Simon (2003, p. 200), programa de treinamento e conscientização sobre segurança da informação “deve ser desenvolvido de modo que todos os empregados tenham de participar. Os novos empregados devem participar dele como parte de seu treinamento inicial”. Os mesmos autores também recomendam que nenhum colaborador tenha acesso ao sistema de informação de uma organização, sem que antes tenha participado de uma sessão básica de conscientização e um programa de treinamento.

4 REFLEXÕES CONCLUSIVAS

O atual cenário revelado pela pesquisa mostrou que a maioria das escolas de educação básica (séries iniciais) pesquisadas, apesar de serem as que mais coletam dados no ato da matrícula, não chegam a implementar diretrizes de controle que promova a pratica de segurança da informação para garantir a proteção de suas informações, e nem promovem campanhas educativas que visem incentivar ou motivar a prática da segurança da informação dentro da escola por todos os colaboradores.

Também foi possível observar que os controles de segurança, que tem por finalidade analisar o perfil e o histórico profissional do futuro colaborador, ainda não são muito utilizados, tornando assim a prática de segurança da informação dentro dessas escolas muito deficiente.

Acreditamos que a adoções de controles de seguranças que promovam a prática da segurança da informação dentro das escolas é de extrema importância, não só para as escolas, mas também para todos aqueles que fornecem e confiam seus dados a elas.

Este trabalho também trás contribuições para futuras investigações que busquem fazer uma abordagem mais ampla no tocante à acomodação de escolas em não praticar a segurança da informação.

Referências

ABNT NBR ISO/IEC 27002, Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação. Setembro de 2013.

BRASIL. Lei Federal Nº 13.709, de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 26 de outubro de 2021.

CANALTECH. Gartner revela que despesas em segurança devem chegar a US$ 96 bilhões em 2018. Disponível em < https://canaltech.com.br/seguranca/gartner-revela-que-despesas-em-seguranca-devem-chegar-a-us-96-bilhoes-em-2018>. Acesso em: 29 janeiro de 2022

CAPES. Portal de Periódicos da Capes. Disponível em: <www.periodicos. capes.gov.br>. Acesso em: 21 dezembro. 2021.

DIALOGANDO, Ataques de ransomware nas escolas e universidades. 21, agosto de 2017. Disponível em: < https://www.dialogando.com.br/seguranca/ataques-de-ransomware-nas-escolas-e-universidades> Acesso em: 06 de junho de 2021.

GODOY, A. S. Refletindo sobre critérios de qualidade da pesquisa qualitativa. GESTÃO.Org – Revista Eletrônica de Gestão Organizacional, v. 3, n. 2, mai./ago. 2005.

GATTI, B. A. A pesquisa em educação: pontuando algumas questões metodológicas, PUC-SP, 2006.

GIL, A. C. Como elaborar projetos de pesquisa. 3. ed. São Paulo: Atlas, 1991.

GIL, Antônio Carlos. Métodos e técnicas de pesquisa social. 5. ed. São Paulo: Atlas, 1999.

GOUVÊA, João Paulo Hora SANTOS, Cleone Francisco. SILVA, Deverton Santana. Ameaças à segurança da informação: os riscos humanos como fator prevenção. UNIT. Universidade Tiradentes. Coordenação Adjunta do Curso de Gestão em Tecnologia da Informação (TI) – EAD,2010

HELENA LEITE, Novidade na área! Google apresenta mais de 50 novos recursos para aulas online. 18, fevereiro de 2021. Disponível em: < https://paisefilhos.uol.com.br/familia/novidade-

na-area-google-apresenta-mais-de-50-novos-recursos-para-aulas-online/> Acesso em: 22 de junho de 2021.

LETÍCIA MACEDO, Vazamento de fichas de alunos gera protesto e punição no Bandeirantes. G1, 15, março de 2015. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2015/03/vazamento-de-fichas-de-alunos-gera-protesto-e-punicao-no-bandeirantes.html> Acesso em: 30 de maio de 2021.

MARCONI, Maria de Andrade; LAKATOS, Eva Maria. Técnicas de pesquisa. 3. Ed. São Paulo: Atlas, 1999.

MITNICK, K. D.; SIMON, W. L. Mitnick: A arte de enganar. São Paulo: Pearson Makron Books, 2003.

PROESC,Gestão da Secretaria Escolar: O Proesc é Especialista. Blog Proesc, 21, setembro de 2020. Disponível em: < http://www.proesc.com/blog/gestao-da-secretaria-escolar/> Acesso em: 30 de maio de 2021.

STALLINGS, W. Network Security Essentials. 1. Ed. [S.l.]: Prentice Hall, 1999. 366 p.

STEFANINI, Você e sua empresa correm risco. Disponível em: < https://stefanini.com/pt-br/trends/artigos/voce-e-sua-empresa-correm-risco> Acesso em 26 de dezembro de 2021.

TANENBAUM, Andrew S. Redes de Computadores. 4. Ed. Campus, 2003

THIAGO AMÂNCIO, Invasões de aulas online se espalham e constrangem alunos e professores. 29, maio de 2021. Disponível em: <https://www1.folha.uol.com.br/autores/thiago-amancio.shtml> Acesso em: 06 de junho de 2021.

RANGELRAFAEL, 6 erros para não cometer na segurança da informação da sua empresa.Disponível em: <https://xtech.com.br/Blog/6-Erros-Para-Nao-Cometer-Na-Seguranca-Da-Informacao-Da-Sua-Empresa> Acesso em: 14 de setembro de 2021.