FACULDADE DE TECNOLOGIA DE SÃO CAETANO DO SUL – ANTÔNIO RUSSO

YARA JOYCE MORENO RODRIGUES

SEGURANÇA DA INFORMAÇÃO AOS JOVENS: UMA CARTILHA SOBRE ARQUIVOS E DADOS PESSOAIS EM MICROCOMPUTADORES

SÃO PAULO/SP
2020

YARA JOYCE MORENO RODRIGUES

SEGURANÇA DA INFORMAÇÃO AOS JOVENS: UMA CARTILHA SOBRE ARQUIVOS E DADOS PESSOAIS EM MICROCOMPUTADORES

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de São Caetano do Sul, sob a orientação do Professor Dr Ricardo Baitz, como requisito parcial para a obtenção do diploma de Graduação no Curso de Segurança da Informação.

SÃO PAULO/SP
2020

À Socorro Moreno, Francisca Pereira e Maria de Jesus (in), mulheres da minha vida, à quem devo educação, caráter e essência.

Agradecimentos

Todo feito é fruto de esforço coletivo, sendo assim, ainda que meu trabalho tenha criação solo, não posso deixar de agradecer a quem contribuiu para sua realização.

Agradeço ao meu orientador, Prof. Dr. Ricardo Baitz, pela paciência em conduzir neste caminho, por sua didática e por me ensinar sobre autonomia e que o caminho é mais importante que a chegada.

Aos colegas que aceitaram ser parte do experimento, lendo e avaliando o produto deste TCC, entre estes meus irmãos, Raimundo Neto e Romildo Junior.

Ao meu companheiro, Vinícius Delaguardia, que tem me apoiado e auxiliado em todos esses anos de graduação, pessoal e academicamente.

Aos meus amigos e amigas, profissionais de Tecnologia e Segurança da Informação, que cederam material e conhecimento técnico para me apoiar neste desafio, entre estes as amigas Isabelle Ribeiro e Divina Vitorino.

Agradeço sobretudo a Deus, força superior que acredito ter me auxiliado e fortalecido nesta jornada.

“A educação, qualquer que seja ela, é sempre uma teoria do conhecimento posta em prática.”

(Paulo Freire)

LISTA DE SIGLAS E ABREVIAÇÕES

BACKGROUND: Termo em inglês para bagagem de vivência e aprendizado acadêmico, pessoal ou profissional.

BYOD: *Bring Your Own Device* – termo em inglês que define a liberação de companhias para que funcionários tragam seu próprio computador para trabalhar;

DESKTOP: Termo em inglês para computador de mesa;

HOME OFFICE: Definição em inglês para trabalhar de casa, transformar o ambiente privado em escritório;

ISO: *International Organization for Standardization* – sigla em inglês para Organização Internacional de Padronização;

ISO 27001: Norma Internacional que determina as boas práticas e controles de Segurança da Informação;

ISO 27002: Norma Internacional que prevê a forma de implementação de Segurança da Informação no ambiente corporativo;

LAPTOP: Termo em inglês para computador pessoal portátil;

RAM: *Random Acess Memory* – sigla em inglês para Memória de Acesso Randômico;

ROM: *Ready-only memory* – sigla para memória apenas de leitura;

OPEN SOURCE: Termo em inglês para código fonte aberto licenciado para uso livre;

PEN DRIVE: Na tradução literal, caneta de armazenamento. Termo em inglês para dispositivo removível e portátil de armazenamento de dados;

RANSOWARE: é um tipo de software que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate para que o aceso seja liberado;

SCAN: Termo em inglês para varredura, de um sistema ou superfície;

SI: Segurança da Informação.

RESUMO

RODRIGUES, Yara J. Segurança da Informação aos jovens: Uma cartilha sobre arquivos e dados pessoais em microcomputadores. 36 folhas. Trabalho de Graduação – Faculdade de Tecnologia de São Caetano do Sul, São Caetano do Sul, 2020.

O conteúdo deste trabalho aborda conscientização em segurança da informação, voltado para o armazenamento seguro de dados em computadores pessoais. Tem como público alvo pessoas de 18 a 35 anos que fazem o uso de *laptops* e *desktops* cotidianamente. Não é necessário estudar tecnologia para compreender este material, apenas buscar entendimento sobre um melhor uso de computadores. A produção do material final foi feita de forma independente, não visando fazer propaganda de nenhuma ferramenta de segurança específica, mas repassar os conceitos básicos de segurança da informação. A cartilha não tem o objetivo de avaliação quantitativa sobre seus leitores, mas de proporcioná-los conhecimento e autonomia para usar de boas práticas de segurança da informação em prol de suas informações privadas e ter um uso não alienado de seu computador pessoal.

Palavras chave: conscientização; dados pessoais; computador pessoal; segurança da informação; cartilha.

ABSTRACT

RODRIGUES, Yara J. Information Security for young people: A primer on personal files and data on microcomputers. 36 sheets. Graduation Work - São Caetano do Sul Faculty of Technology, São Caetano do Sul, 2020.

The content of this paper addresses to information security awareness focused on the safe storage of data on personal computers. The target audience are users from 18 to 35 years old who deal with laptops and desktops as something common in their daily lives. It is not necessary to study technology to understand this material just to seek understanding about a better use of computers. The production of the final material was done independently, not aiming to advertise any specific security tool, but to convey the basic concepts of Information Security. The booklet is not intended to provide a quantitative assessment of its readers, but to provide them with knowledge and autonomy to use good IS practices in favor of their private information, and to avoid unawareness when usingtheir personal computer.

Keywords: information security guide; awareness; personal data; personal devices; information security; booklet

SUMÁRIO

INTRODUÇÃO

A proposta deste TCC é apresentar um manual aos jovens. Trata-se de uma cartilha que ensina a armazenar arquivos e dados pessoais em computadores com técnicas de segurança da informação.

Sobre Segurança da Informação, Julie Hintzbergen (2010, pag.16) define como “a proteção das informações contra uma gama de ameaças, visando continuidade e redução de riscos e maximização de retorno em negócios”. Certamente este conceito se refere ao ambiente corporativo, entretanto nesta cartilha serão abordados os pilares que sustentam a proteção dessas informações, visando a redução de riscos para pessoas físicas durante o uso de seus computadores para armazenamento de arquivos pessoais.

Os pilares da segurança que abordaremos nesta cartilha são: Confidencialidade, Integridade e Disponibilidade. Estes conceitos são os princípios fundamentais de segurança da informação e embasam pilares complementares como a autenticidade.

Sobre os conceitos supramencionados, adotaremos as definições contidas nos documentos ISO 27001:2013 e 27002:2014, abordados por Hintzberg (et. Al 2010, pag12 -15) no livro “Fundamentos de Segurança da Informação”, contidos a seguir:

— Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;

— Integridade: propriedade de garantir que a informação não sofreu alterações durante seu processamento;

— Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;

— Autenticidade: propriedade de uma entidade ser o que afirma ser.

Estes e demais conceitos de Segurança da Informação, assim como técnicas de proteção serão abordados de forma didática, promovendo a conscientização dos leitores quanto ao uso seguro de seus microcomputadores pessoais.

A conscientização é um controle de prevenção em S.I. que visa mitigar os riscos de ataques que envolvem o fator humano, sejam esses ataques direcionados por meios tecnológicos ou diretamente por exploração de comportamentos, como os ataques de engenharia social (ataques que utilizam de informações obtidas através de uma relação de confiança estabelecida com a vítima, para facilitar a intrusão em ambientes físicos ou cibernéticos). Aplicando este controle na cartilha, temos a promoção de boas práticas que reduzam os riscos de um ataque que subtraia ou exponha dados que considerados confidenciais pelo leitor do material.

Não é o objetivo deste trabalho quantificar a mudança de comportamento dos leitores após o consumo do conteúdo a ser apresentado, mas sim disseminar as boas práticas de segurança da informação e disponibilizar a pessoas comuns informações confiáveis de como proteger-se contra possíveis ataques direcionados aos seus dados armazenados em microcomputadores pessoais.

1. DESENVOLVENDO UM MANUAL SOBRE SEGURANÇA DA INFORMAÇÃO

Para entendimento do trabalho, apresenta-se neste capítulo a metodologia abordada para pesquisa e criação do produto da cartilha, assim como todo o processo de construção e validação que torna o esforço acadêmico um produto tangível.

1.1 METODOLOGIA

Não estando eu apartada do contexto alvo de estudo deste trabalho, decidi utilizar como metodologia de pesquisa e escrita a Metodologia de Implicação.

Esta metodologia traz a técnica de escrita que demonstra a relação entre pesquisador e o âmbito estudado, ou seja, o pesquisador não é mero observador do seu objetivo de estudo, mas está inserido no contexto e se relaciona diretamente com o estudo, como nos demonstra o Dr. Ricardo Baitz em seu artigo “A Implicação: Um novo sedimento a se explorar na Geografia?”, publicado no Boletim Paulista de Geografia de n°84:

“Analisar os motivos mais íntimos de uma pesquisa implica deixar se examinar, deslocar o campo de coerência do objeto e incluir-se nele”

Por ter escolhido esta metodologia, todo o trabalho traz uma escrita dissertativa em primeira pessoa, pois a narrativa impessoal me faria apenas observadora e não integrante do alvo de estudo deste trabalho.

1.2 – PROCESSO DE DESENVOLVIMENTO

Primeiramente, decidi que o produto seria uma cartilha. Fiz feita a escolha do público alvo para desenvolvimento do conteúdo adaptação da linguagem. A faixa etária de 18 a 35 anos foi definida pelo fato de se tratar de uma geração que, em grande parte, já está inserida digitalmente e utiliza estes dispositivos para fins de estudo e trabalho.

Mesmo com facilidade de manipulação de dispositivos informáticos, é possível perceber, em simples conversas com pessoas dessa faixa etária, que o conceito de SI é algo muito remoto em seu dia a dia, e quando tem um conhecimento (exceto os que trabalham na área) é através do departamento de SI das empresas que trabalham, e enxergam este departamento exclusivamente como “bloqueadores de acesso” e não facilitadores de um acesso seguro.

Além do fator do desconhecimento do assunto, temos na sociedade moderna uso de dispositivos de informática com aplicação no trabalho e na vida pessoal de forma simultânea, como o *home office* ou o *BYOD (Bring Your Owmn Device),* que podem aumentar a vulnerabilidade dos dispositivos informáticos a ataques, sobretudo derivados de exploração comportamental.

Após a análise deste contexto, a criação de um material que abordasse conceitos básicos de Segurança da Informação, modos de proteção de microcomputadores, técnicas de prevenção e defesa contra ataques a dispositivos informáticos pessoais e boas práticas de uso seguro de microcomputadores mostrou-se uma solução bem interessante.

Para desenvolvimento do material foram estudados diversos modelos de cartilhas de conscientização em segurança da informação desenvolvidos por empresas de consultoria da área, artigos sobre ataques a microcomputadores, implementação de técnicas de prevenção a esses ataques e as normas internacionais que ditam a implantação e controles de SI.

Os tópicos foram definidos de modo que sejam abordados de forma fluida e coesa, alcançando o entendimento básico que o usuário precisa ter para usar seu dispositivo informático pessoal de forma segura.

Definidos os tópicos, a cartilha foi formulada com linguagem simples e livre de termos técnicos, exceto quando esses termos são indispensáveis ao entendimento e obrigatoriamente explicados dentro da cartilha.

O material possui artes visuais para facilitar a fixação do conteúdo e ser mais apelativa junto ao público jovem. Não se tem a intenção de desenvolver um material extenso, pois deve ser conciso e assertivo, a ponto de não ser enfadonho e desgastante ao seu leitor.

Por tratar-se de um trabalho de graduação o tema foi bem delimitado, de modo a ser esgotado. O uso da internet não será amplamente abordado, apenas citado, pois caso fosse abordado não seria possível esgotá-lo neste trabalho e para ser coerente quando se ensina algo é preciso ir desde a base.

Não se pode falar sobre o compartilhamento de dados na rede mundial de computadores, antes que alguém entenda como funciona o armazenamento em sua própria máquina e desenvolva um comportamento responsável quanto ao dispositivo que usa frequentemente.

Finalizado o material, este deve ser apresentado a representantes do público alvo a fim de verificar se o conteúdo escrito é compreensível a qualquer indivíduo entre 18 e 35 anos que use microcomputadores regularmente, mas não trabalhe ou estude na área de Tecnologia da Informação.

O objetivo deste trabalho é colocar os conceitos aprendidos durante o curso de Tecnologia em Segurança da Informação a serviço da sociedade, viabilizando de forma gratuita e acessível o texto final deste trabalho, de modo que alcance o maior número possível de interessados.

2. EMBASANDO TEORICAMENTE UMA CARTILHA SOBRE SEGURANÇA DA INFORMAÇÃO

Toda recomendação visando a mudança de hábitos na vida de terceiros deve ser feita com base científica. Para desenvolver um material assertivo e coerente, é necessário que este seja embasado em estudos feitos no campo de assunto abordado, garantido a confiança e efetividade das informações repassadas. Por se tratar de um trabalho de graduação, livros, artigos, normas e o conhecimento adquirido no decorrer do curso foram utilizados para construir o objetivo final. O conhecimento adquirido será estruturado aqui em tópicos e o assunto distribuído na construção da cartilha.

2.1 - BOAS PRÁTICAS DE ARMAZENAMENTO DE DADOS EM DISCO LOCAL

Antes de falarmos sobre boas práticas de armazenamento, precisamos entender o que é um dado. Segundo o dicionário *Oxford by Google* a definição de dado, no contexto da informática, é uma informação capaz de ser processada por um computador. Olhando para a estrutura de um computador temos dispositivos de entrada de dados, dispositivos de saída ou exibição e dispositivos de processamento de dados.

Quando um texto é digitado no teclado de um computador, dados binários são inseridos e temporariamente armazenados na memória ROM a fim de garantir seu processamento na unidade de processamento do microcomputador. Quando vou ao editor de texto e escolho salvar aquele arquivo, o editor me dará a opção de diretórios em que salvarei o meu texto. Esses diretórios são unidades de

partição da memória (unidade de memória duradoura do computador). Quando o diretório é escolhido, a informação digitada é alocada na partição selecionada. Neste simples processo de digitar e salvar um texto, dados foram inseridos, exibidos, processados e armazenados pelo microcomputador que executou as operações.

Pelo exemplo acima percebemos que o computador é um agente executor das decisões que tomamos para as informações que serão nele processadas, ou seja, a segurança dos dados inseridos nos computadores depende das ações que tomarmos para garanti-la.

Pensando nos pilares de segurança da informação apresentados anteriormente neste trabalho, podemos garantir que um dado seguro é aquele que mantem sua confidencialidade, disponibilidade e integridade.

Para garantir essas características ao armazenar dados em microcomputadores pessoais, é preciso tomar alguns cuidados tanto quanto a máquina quanto ao arquivo que será armazenado.

O primeiro cuidado quanto à máquina é de segurança física. É preciso que o laptop/desktop seja utilizado em ambiente onde a possibilidade de furto, roubo ou avaria do dispositivo seja reduzida. Quando transportado ou armazenado, estas mesmas condições devem ser levadas em questão.

A segunda decisão quanto à máquina é sobre o seu sistema operacional e acesso à área de trabalho. O sistema operacional deve ser recente, de licença original ou *open source* confiável, de modo que o computador possa receber atualizações de segurança sobre vulnerabilidades identificadas em seu sistema operacional. A não correção de vulnerabilidades de SO abre espaço para ataques mal intencionados como de *ransomwares.*

Quanto ao acesso, se o computador não for de uso exclusivo, deve haver configuração de usuário individual com autenticação por senha. Ainda que o computador seja utilizado apenas por uma pessoa o uso de senha para acesso a

área de trabalho é indispensável, pois ao usar senhas o princípio de confidencialidade é fortalecido e garante-se a identificação de ações tomadas dentro do sistema pelo usuário que estiver usando naquele momento.

Uma vez dentro do sistema operacional e apto a trabalhar na máquina é preciso fazer a classificação da informação que será armazenada. A classificação deve ser feita pelo dono da informação, que decidirá conforme o teor do conteúdo se é uma informação que pode ser de conhecimento público ou deve ser confidencial.

Para acesso organizado dos dados armazenados em um microcomputador, é recomendado a nomeação dos arquivos de modo que facilite a identificação e a criação de pastas que organizem os arquivos por comum assunto.

Se um arquivo for considerado confidencial é indispensável que o diretório a qual está armazenado seja protegido por senha, dificultando o acesso à informação, ainda que outra pessoa tenha obtido a senha de acesso à máquina.

Arquivos que são considerados de informação públicas podem ser armazenados em diretórios sem senha, ou ainda na área de trabalho para facilitar sua localização. Tanto para arquivos confidenciais quanto arquivos públicos é possível definir na máquina se os usuários poderão modificá-los ou apenas visualizá-los, garantindo o princípio de integridade da informação.

Os dados que forem transmitidos à máquina por meio de dispositivos removíveis (cartão de memória, *pendrive*) devem ser validados quanto ao seu teor e é indispensável que o computador tenha uma ferramenta que realize um *scan* no dispositivo portátil, reduzindo o risco de ataques por meio de arquivos maliciosos. Em caso de arquivos baixados diretamente da rede mundial de computadores, é preciso certificar-se que a origem é considerada segura e o caminho em que a informação trafegará também é seguro.

As práticas aqui descritas ajudam a reduzir de maneira significativa as chances de perda indesejada de arquivos, acesso indevido de informações

confidenciais e alteração errônea de dados previamente armazenados. Ferramentas e técnicas para implementação de Segurança da Informação, serão abordadas na cartilha.

CONSIDERAÇÕES FINAIS

O material consolidado deste trabalho resultou em uma cartilha gráfica didática sobre Segurança da Informação que foi apresentada a representantes do público alvo (jovens de 18 a 35 anos) de diferentes graus de instrução: do ensino médio completo até estudantes de pós graduação.

Após a leitura de todo o material, um questionário foi enviado aos leitores da cartilha para que pudessem avaliar o material, pertinência do conteúdo e se sentiam-se aptos a colocar em prática os novos conhecimentos adquiridos. O formulário coleta dados de perfil dos leitores como idade, grau de instrução, se já tiveram disciplinas que abordassem tecnologia ou acesso a cursos de informática e se já possuíam conhecimento prévio de fundamentos de Segurança da Informação.

Os leitores que possuem curso superior têm a formação diversificada entre graduados em Ciências Humanas, Ciências Exatas e Ciências Biológicas. Alguns tiveram em suas graduações disciplinas relacionadas à tecnologia/informática ou acesso a cursos que tratassem do tema. Outros possuíam algum entendimento prévio ao da cartilha sobre Fundamentos de Segurança da Informação. Pude observar que o entendimento do conteúdo não foi prejudicado pela área de estudo de cada um, mesmo os estudantes de Ciências Humanas que pouco contato têm com conceitos acadêmicos de tecnologia conseguiram compreender o conteúdo disposto na cartilha, entretanto a percepção do material foi subjetiva ao conhecimento que cada um já possuía.

Alguns sentiram necessidade de maior quantidade de elementos gráficos, outros sentiram-se confortáveis com a quantidade de texto, sem uma maior inserção de elementos visuais. Foi sugerido o uso de mais elementos visuais para instigar o interesse de leitura do conteúdo, sugestão que eu compreendo a relevância, mas não acatei neste primeiro momento. O receio de que o material se tornasse longo e moroso foi o motivo pelo qual eu não inseri uma quantidade maior de elementos visuais, porém para trabalhos de conscientização futuros com menor número de

tópicos a serem abordados, creio que seja possível fazer um maior uso de imagens e infográficos.

Todos os leitores da cartilha consideraram a linguagem usada na abordagem descomplicada, e a estrutura textual coesa, facilitando o aprendizado. O leiaute da cartilha foi elogiado por parecer com uma revista, e trazer comentários na borda que enfatizavam o conteúdo do tópico.

Alguns leitores consideraram que os termos técnicos e definições inseridas na cartilha os ajudaram a compreender o campo de segurança da informação com maior facilidade.

Todos os leitores da cartilha consideraram que o material os auxiliou no aprendizado sobre o assunto proposto e a maioria se considera apta a executar o que foi explicado.

As percepções acima descritas serão trazidas na planilha “Respostas do formulário” e observadas nos gráficos dispostos na lista de gráficos. Considerei importantes acrescentá-las a este trabalho como forma de demonstrar a eficiência do pilar de conscientização na aplicação cotidiana dos conceitos de Segurança da Informação.

Com base nas informações apresentadas neste documento sobre o experimento, podemos concluir que usuários de TI aprendem sobre Segurança da Informação, assim como qualquer assunto, quando isso lhes é apresentado de forma simples como uma ferramenta de ajuda em funções que desempenhem eu seu dia a dia. Podemos concluir, também, que o uso mais seguro de dispositivos informáticos está diretamente atrelado ao conhecimento que seus usuários têm de boas práticas em Segurança da Informação.

Penso que se pudéssemos abordar Fundamentos de Segurança da Informação como conteúdo base de cursinhos de informática, teríamos uma sociedade futura mais preparada para o nível de exposição de dados a que a informatização generalizada nos submete.

Para materiais futuros, recomendo levar em consideração o *background* do público alvo e estruturar o texto em uma linguagem mais próxima o possível a que o leitor tenha contato no cotidiano. Aos profissionais de artes, por exemplo, indico utilizar de mais recursos visuais, ou para profissionais de cursos de exatas não relacionados à tecnologia um uso de infográficos, pois pude perceber que mesmo a formação não impactando no entendimento do conteúdo apresentado, o *background* implica diretamente na forma de apreciação do material que o indivíduo fará.

REFERÊNCIAS

HINTZBERGEN, Jule. HINTZBERGEN, Kees. SMULDERS, André. BAARS, Hans. **Fundamentos de Segurança da Informação com base na ISO 27001 e na ISO 27002.** Tradução de Alan de Sá. Rio de Janeiro – Brasport, 2018.

Conceito de dado segundo o dicionário Oxford online. Disponível em: dicio.com.br/dado

BAITZ, Ricardo. **A implicação: Um novo sedimento a se explorar na Geografia.** Boletim Paulista de Geografia, n/84, São Paulo,2006.

GONÇALVES, Daniela, M.V. **Uso da metodologia de implicação em um experimento de Segurança da informação.** Trabalho de conclusão de curso apresentado à Fatec São Caetano. São Caetano do Sul, 2011.

KHATI, Louiza. MOUHA, Nicky. VERGNAUD, Damien. **Full Disk Encryption: Briding Theory and Practice.** Artigo submetido à École Normale Superieure – CNRS - Paris, 2015.

FERREIRA, Rubem E. **Linux: Guia do administrador do Sistema.** Novatec – 2° edição. São Paulo, 2008.

Em apêndice Cartilha, versão do formulário enviada aos leitores, Respostas ao formulário em tabela e consolidação das respostas ao formulário em gráficos

APENDICE 1: CARTILHA

PROTEGENDO O QUE GUARDO NO MEU COMPUTADOR

COMO GARANTIR A SEGURANÇA DOS DADOS ARMAZENADOS EM SEU COMPUTADOR PESSOAL.

Introdução

A nossa relação com dispositivos de informática é diária, de modo que produzimos, armazenamos e compartilhamos conteúdos através destes dispositivos a todo momento.

Toda foto, texto, planilha e documentos que criamos são informações que serão processadas por nossos computadores, gerando um resultado que nos tem valor. A este resultado, chamamos de informação.

Os dados que armazenamos em nossos computadores costumam ter importância pessoal, profissional ou até mesmo financeira. Mas o quanto essas informações importantes estão seguras?

Nesta cartilha você aprenderá o que é Segurança da Informação e como técnicas e boas práticas deste campo da tecnologia podem te ajudar a proteger o que você guarda em seu computador.

O QUE É INFORMAÇÃO?

Informação é o dado que tem significado em algum contexto para quem o recebe. Quando essa informação é inserida ou armazenada em um computador, recebe o nome de dado.
Ao processar dados, temos novamente a percepção de informação. Deste modo os dois termos não são a mesma coisa, mas estão intimamente relacionados.

Para exemplificar a definição acima, tenhamos como exemplo o planejamento de gastos de uma família:

- As entradas e despesas fixas são informações básicas para iniciar o planejamento. Quando usamos uma planilha no computador para organizar e otimizar o planejamento, estas informações passam a ser dados da planilha de gastos.
- Ao processar os dados na planilha e obter a previsão de gastos futuros e saldo remanescente mensal, temos novamente informações sobre as finanças da família em questão.

Informação e dado não representam a mesma coisa, entretanto estão relacionados.

O QUE É SEGURANÇA DA INFORMAÇÃO?

Segurança da Informação (SI) é o campo de estudos da Tecnologia da Informação que visa proteger conjuntos de dados durante seu processamento, armazenamento e/ou transferência. As técnicas e processos utilizados para alcançar essa proteção, são baseadas nos pilares de SI: Confidencialidade, Integridade e Disponibilidade (CID).
Quando um meio de armazenamento, ou meio de transmissão garante estes pilares ao conjunto de dados que nele está contido, consideramos que os dados estão seguros.

Sobre o CID, temos as seguintes definições:

- Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;
- Integridade: propriedade de proteger a exatidão da informação, a fim de prevenir modificações não autorizadas;
- Disponibilidade: Propriedade de ser acessível e utilizável por quem/o que tenha autorização para fazê-lo.

Esses conceitos servem para armazenamento, processamento e transferência de dados, devendo ser respeitado em todos os ambientes que a informação passar.

Consideramos uma informação segura quando o meio que a contém garante o CID.

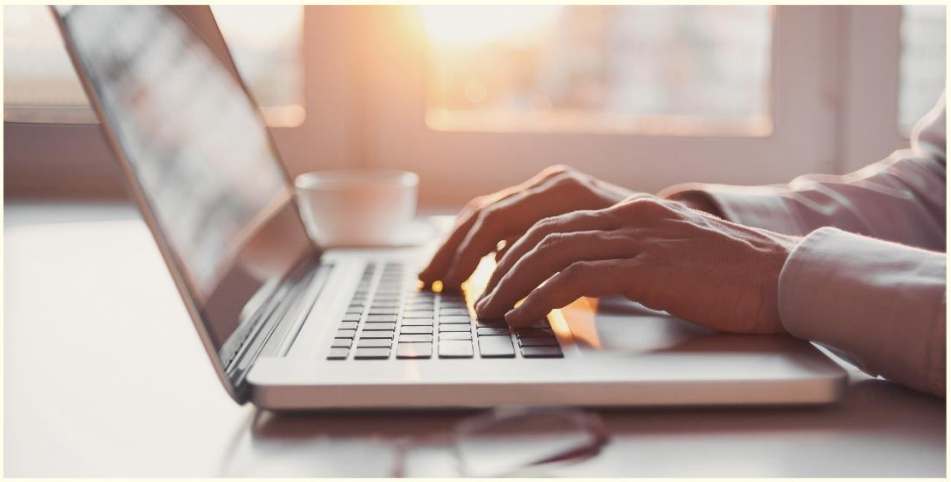
EXEMPLOS PRÁTICOS DE CID

Confidencialidade: Pense em um diário. Neste diário contém informações pessoais que somente quem as escreve deve ler. Ao colocar um cadeado no diário um controle de confidencialidade é implementado, somente quem tiver a chave terá acesso ao que está escrito. Se apenas o escritor tiver a chave do cadeado, a confidencialidade será mantida.
A confidencialidade só é quebrada se a chave for subtraída ou o cadeado extraviado.

Integridade: Um bom exemplo de quebra de integridade é a brincadeira "telefone sem fio". Nesta brincadeira raramente a mensagem inicial é entregue ao destinatário final. Caso a mensagem fosse enviada de forma direta e por um canal sem interferências, onde só o destinatário e o remetente tivessem acesso, as chances de a mensagem recebida ser a mesma enviada que foi enviada, seriam bem maiores.

Disponibilidade: Quando você tenta usar sua internet e ela está fora de serviço, é um exemplo de quebra de disponibilidade. Caso você tenha mais de um meio de conexão à internet, as chances de que você fique totalmente sem conexão são menores, aumentando assim a garantia de disponibilidade do recurso internet.

Quando você tenta usar sua internet e ela está fora de serviço, é um exemplo de quebra de disponibilidade



CONHECENDO O SEU COMPUTADOR

Antes que possamos aplicar os conceitos de SI nas informações de seu computador, é preciso conhece-lo melhor.
O computador é composto por uma parte física e uma parte sistêmica.
A parte física é o conjunto dos dispositivos de entrada e saida da informação no computador: mouse, teclado, portas USB, portas para cabos HDMI e de rede, etc. A este conjunto damos o nome de hardware.
A parte sistêmica é composta pelo conjunto de programas que permitem o uso do hardware para processamento das informações: sistema operacional, programas de navegação na internet, editores de texto, reprodutores de mídia, etc. A este conjunto damos o nome de software.
Os dados são armazenados e processados na parte física, mas são acessados através do sistema.
O sistema operacional (SO) é quem divide a memória no que conhecemos como pastas para acesso: meu computador, documentos, pasta de imagens. A estas pastas dá-se o nome de diretório.
Usando o SO é que aplicaremos boa parte das técnicas de proteção aos dados, entretanto para que as técnicas funcionem adequadamente o hardware deve suportar as técnicas aplicadas em seu disco de memória e ter um bom desempenho de processamento.

O computador é composto por parte física e sistêmica. À parte sistêmica damos o nome de software e à parte física damos o nome de hardware.

CLASSIFICANDO A INFORMAÇÃO

Para empregar adequadamente controles de segurança a uma informação, é preciso atribuir um valor, ou seja, identificar se a informação é importante, muito importante, ou sem importância. Para atribuir este valor é precso levar em consideração a aplicação da informação, as implicações de uma possível perda e o se o teor é de carater pessoal.
A partir destes requisitos é possível classificar a informação em pública ou confidencial:

- Uma informação pública qualquer pessoa ou programa do computador pode ter acesso;
- Informações confidenciais apenas um grupo de usuários ou programas devem ter acesso;

Uma vez a informação classificada é possível dimensionar os controles de segurança necessários para protege-la

A classificação da informação definirá os controles necessários para protege-la.

ALGUNS CONCEITOS EM SEGURANÇA DA INFORMAÇÃO

Além dos pilares de Segurança da Informação (CID), há outros conceitos em SI cujo o entendimento ajuda a alcançar a conformidade com os pilares:

- Ameaça: causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema;
- Ataque: uma tentativa de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado a uma informação ou dispositivo;
- Autenticidade: propriedade de uma entidade ser o que afirma que é;
- Confiabilidade: propriedade de consistência dos comportamentos e resultados desejados;
- Risco: efeito da incerteza sobre os objetivos. É a combinação da probabilidade de um evento e sua consequência;
- Não repúdio: habilidade de provar a ocorrência de um suposto evento ou ação e suas entidades de origem.

O entendimento destes conceitos é essencial para as formas de proteção que serão abordadas nesta cartilha.

Além do CID há outros conceitos em SI que auxiliam a alcançar a conformidade com os pilares de SI.

O QUE SALVAR NO SEU COMPUTADOR

Além de classificar a informação é importante observar o que será salvo computador, tanto pela relevância, quanto pelo desempenho do equipamento. Um computador com programas que exigem alto desempenho e arquivos muito extensos, pode ter um desempenho prejudicado, dificultando seu uso.

Ao decidir o que manter na memória do computador é necessário levar em conta a origem do arquivo. Busque fazer downloads de sites conhecidos e que possuam certificado (Busque no rodapé do site a informação de site certificado),sites certificados tem uma entidade que garantem sua validade. Ao fazer downloads de sites suspeitos ou transferir arquivos de mídias desconhecidas coloca-se em risco a integridade do computador, podendo contrair um software malicioso que venha a causar danos na máquina ou ter acesso a dados confidenciais de forma não autorizada.

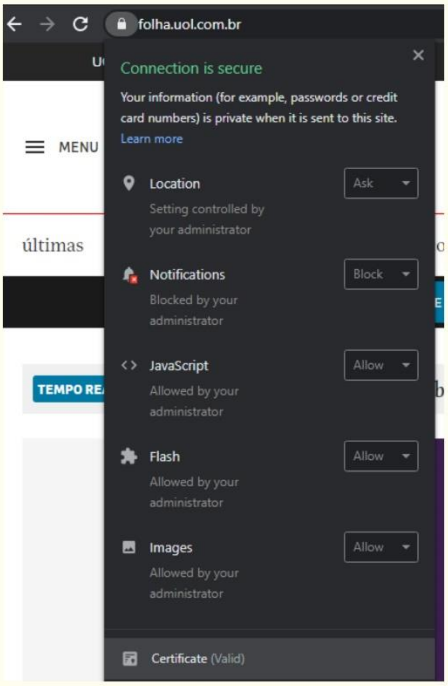
A mesma observação vale para softwares pirateados. Ao usar este tipo de software, além de cometer uma infração sobre direito autoral, quem o faz corre o risco de comprometer a possibilidade de uso total dos recursos do dispositivo informático.

Além da classificação da informação é necessário atentar-se a origem e teor da informação a ser armazenada.

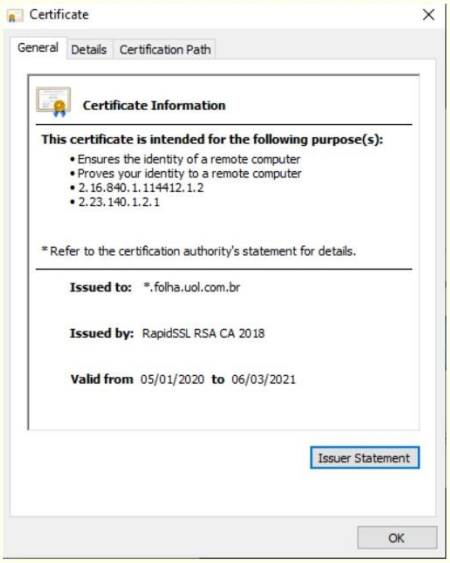
Verificando se o site é certificado

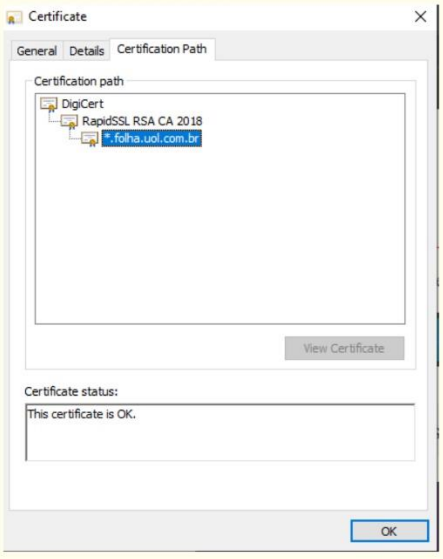
Digite o endereço do site:

Busque e clique no ícone do cadeado. Selecione a opção certificado:



Veja se o certificado é valido e correspondente ao site buscado





TÉCNICAS E FERRAMENTAS DE SI PARA COMPUTADORES

Algumas técnicas e ferramentas de SI podem tornar o seu computador um ambiente mais seguro para armazenar informaçãoes:

- Antimalware: software que varre o sistema operacional e os arquivos transferidos para o computador, a fim de detectar arquivos com códigos de execução maliciosa, exploração de conexão com a internet, ou uso demasiado de processamento. Uma vez detectada a ameaça é possível removê-la;

- Criptografia: técnica que utiliza de calculos mátemáticos para gerar chaves que embaralhem informações de forma que não seja legivel a qualquer um, apenas a quem/o que tiver a chave que desembaralhe a informação.

- Perfil de usuário com senha: é imprescindível o uso de senha para acessar o computador. Caso o computador seja usado por mais de uma pessoa é necesária a criação de múltiplos usuários com senha distintas.

- Backup: criar uma cópia de segurança de arquivos importantes é uma tecnica para evitar perde-los definitivamente. Este backup pode ser feito em um HD externo, ou em uma conta da nuvem, de uso pessoal e com senha. Deve haver uma periodicidade para incrementar informações ao backup e garantir que na necessidade de usar uma cópia de segurança esteja o mais atualizada possível. No caso do backup em nuvem, é possível usar backups automáticos como do Google Drive e do One Drive.

Algumas técnicas de SI podem tornar o computador um ambiente mais seguro para armazenar dados.

Escolhendo um antimalware

- Busque uma das soluções conhecidas no mercado;
- Compre as licenças de sites oficiais;
- Siga o passo a passo de instalação do fabricante;
- Atente-se ao prazo de validade do plano escolhido.

Criptografando o seu computador

Para criptografar o disco (memória do seu computador) é necessário um software que execute essa função.
É possível adquirir soluções de criptografia dos mesmos fabricantes de antimalwares ou de fabricantes de sistemas operacionais como a Microsoft. Estas licenças podem ser adquiridas para até mais de uma máquina, o preço é variável por quantidade de computadores que a licença abrange e fabricante.
Uma alternativa gratuita e segura de criptografar o seu disco é o VeraCrypt. A aplicação é opensource, de fácil instalação e pode ser utilizada por computadores Windows, MacOS e Linux. É possível fazer o download no site oficial da aplicação: https://www.veracrypt.fr/en/Home.html.
É possível também criptografar dispositivos de memória portátil como HD externo e pendrive.

Criando diretórios compactados com senha

Para colocar senhas em pastas no Windows é nexessário baixar programas como o WinRar.
Para criar pastas com senhas usando o WinRar siga o passo a passo:

- Baixe o WinRAR no site oficial;
- Crie uma pasta e adicione os arquivos que desejar;
- Clique com o botão direito do mouse abriá um menu;
- Escolha a opção “Add to archive” (Adicionar para o arquivo);
- Será aberta uma nova janela, clique em “Set Password” (Definir senha);
- Escolha uma senha e clique em “show password” para verificá-la;
- Clique em “OK” e será criada uma nova pasta compactada com senha.

Para criar arquivos compactados com senha no Linux basta utilizar no modo sudo o comando $ zip -e arquivo_depois_de_compactado.zip arquivo_a_compactar e será pedida a senha para compactar o arquivo.

BOAS PRÁTICAS PARA UM USO MAIS SEGURO DO COMPUTADOR

Além da implementação das técnicas acima, mudanças comportamentais também são necessárias para garantir a segurança das informações armazenadas em seu dispositivo:

- Senha complexas e de uso único: não compartilhar senhas com terceiros, não usar dados como nome ou data de nascimento para compor as senhas. Importante trocar as senhas regularmente e além de usar no login de acesso ao computador, colocar senhas nas pastas onde armazena arquivos confidenciais também;

- Dispositivos de mídia removível: não compartilhar HD externo ou pendrive com outras pessoas; não colocar no computador dispositivos de mídia removível que seja de uso coletivo ou de dono desconhecido; usar o scanner do antimalware no dispositivo e criptografar o dispositivo de mídia removível para acessar os dados da máquina;

- Trabalho separado de vida pessoal: caso faça home office ou utilize do computador pessoal para trabalhar, criar usuários distintos para as atividades e jamais salvar arquivos pessoais no computador da empresa, pois este pode ser monitorado a qualquer momento.

Boas práticas práticas são essenciais para a SI tanto quanto técnicas e ferramentas de Segurança da Informação.

Conclusão

Nesta cartilha foram apresentadas técnicas, boas práticas e ferramentas que auxiliem no alcance de um armazenamento seguro e de um uso mais responsável do computador pessoal. Tendo estes conhecimentos colocados em prática, as chances que seja você seja vítima de um ataque que subtraia ou "sequestre dados" é bem menor do que se nenhum controle de SI for implementado.

A nossa relação com a tecnologia vai além do que armazenamos em nossos computadores, portanto é importante que a partir deste material você busque outros materiais complementares sobre demais tópicos relevantes, como uso seguro da internet, aprofundar-se no uso do sistema operacional do seu computador e como ter uma rede wifi doméstica mais segura. Esse conhecimento é necessário em seu nível mais básico ainda que tecnologia não seja sua área de atuação.

Referências

Fundamentos de Segurança da Informação, 2018. Novatec. Jule Hintzberg, André Smuldres, Kees Hintzbergn, Haans Baars.

Full Disk Encriptation: Bridging Theory and Practice, 2017. Louiza Khati, Nicky Mouha, Damien Vergnaud.

Guia Linux do administrador do sistema, 2008. Novatec. Rubem E. Ferreira.

Tecnoblog. net: Artigo "Como colocar senha em pastas [Windows]". Acesso em junho/2020.

APÊNDICE 2: FORMULÁRIO

Cartilha - Protegendo o que guardo no meu computador

Avaliação de compreensão e eficácia da Cartilha de Segurança da Informação. Questionário destinado aos leitores.

*Obrigatório

1. Sua idade *

Marcar apenas uma oval.

- 18 a 23
- 24 a 29
- 30 a 35

2. Escolaridade *

Marcar apenas uma oval.

- Fundamental completo
- Ensino médio Completo
- Ensino superior incompleto
- Ensino superior completo
- Pós graduação incompleta
- Pós graduação completa

3. Caso tenha curso superior, completo ou incompleto, por favor destaque a área macro de estudo: *

Marcar apenas uma oval.

- Ciências Biológicas
- Ciências Exatas
- Ciências Humanas

4. Você utiliza computador pessoal no seu cotidiano (desktop/laptop)? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

5. Já estudou disciplina ou curso relacionados à Informática/Tecnologia? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

6. Tem familiaridade prévia a esta cartilha com conceitos de Segurança da Informação? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

7. Leu a cartilha completa? *

Marcar apenas uma oval.

- ◯ Não
- ◯ Sim

8. Quanto a cartilha, classifique o material de apresentação: *

Marcar apenas uma oval.

	1	2	3	4	
Inadequado	◯	◯	◯	◯	Muito adequado

9. Considera a linguagem utilizada de fácil compreensão? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

10. Considera que os recursos gráficos tinham relação com o texto? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

11. Considera que a leitura do material contribuiu para melhorar seus conhecimentos sobre Segurança da Informação? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

12. Se considera apto a aplicar as boas práticas e técnicas de SI abordadas na Cartilha? *

Marcar apenas uma oval.

- ◯ Sim
- ◯ Não

13. Deixe aqui suas considerações sobre o conjunto do material e sugestões de melhoria: *

APÊNDICE 3: RESPOSTAS EM TABELAS

Tabela 1 - Respostas ao Formulário - Registro de resposta, idade e escolaridade:

Carimbo de hora	Sua idade	Escolaridade
29/6/20 5:24	18 a 23	Ensino superior incompleto
29/6/20 7:16	18 a 23	Ensino superior incompleto
29/6/20 7:17	30 a 35	Pós graduação incompleta
29/6/20 8:25	24 a 29	Ensino médio Completo
29/6/20 10:06	24 a 29	Ensino superior completo
29/6/20 16:22	18 a 23	Ensino superior completo
29/6/20 17:57	24 a 29	Ensino superior completo

Tabela 2 - Respostas ao formulário – Área macro de estudos, uso do computador pessoal:

Caso tenha curso superior, completo ou incompleto, por favor destaque a área macro de estudo:	Você utiliza computador pessoal no seu cotidiano (desktop/laptop)?
Ciências Humanas	Sim
Ciências Exatas	Sim
Ciências Exatas	Sim
Ciências Biológicas	Não
Ciências Exatas	Sim
Ciências Humanas	Sim
Ciências Humanas	Sim

Tabela 3 – Respostas ao formulário – Conhecimentos em Tecnologia e SI, leitura da cartilha:

Já estudou disciplina ou curso relacionados à Informática/Tecnologia?	Tem familiaridade prévia a esta cartilha com conceitos de Segurança da Informação?	Leu a cartilha completa?
Sim	Não	Sim
Sim	Não	Sim
Sim	Sim	Sim
Sim	Não	Sim
Sim	Sim	Sim
Sim	Sim	Sim
Sim	Sim	Sim

Tabela 4 – Respostas ao formulário – Avaliação de apresentação, linguagem e recurso gráfico:

Quanto a cartilha, classifique o material de apresentação:	Considera a linguagem utilizada de fácil compreensão?	Considera que os recursos gráficos tinham relação com o texto?
4	Sim	Sim
4	Sim	Sim
4	Sim	Sim
4	Sim	Sim
4	Sim	Sim
4	Sim	Sim
4	Sim	Sim

Tabela 5 – Respostas ao formulário – Avaliação de retenção de conteúdo:

Considera que a leitura do material contribuiu para melhorar seus conhecimentos sobre Segurança da Informação?	Se considera apto a aplicar as boas práticas e técnicas de SI abordadas na Cartilha?
Sim	Sim
Sim	Sim
Sim	Sim
Sim	Não
Sim	Sim
Sim	Sim
Sim	Sim

Tabela 6 – Respostas ao formulário – Considerações e sugestões dos leitores

Deixe aqui suas considerações sobre o conjunto do material e sugestões de melhoria:
O material tem linguagem acessível e conceitos bem explicados e resumidos. Excelente!
A diagramação é amigável e a organização de conceitos em tópicos facilita posterior consulta. Compreensível e didático
Nada a declarar
Bom material para compreensão do leitor, não melhoraria em absolutamente nada pois é de um conteúdo único e muito inteligente.
Achei o material super completo, abordando temas de extrema relevância para todos, de fácil entendimento para pessoas mais leigas, mas como um ponto a acrescenta, eu colocaria mais figuras para não desanimar a leitura do texto comprido, que sabemos que é a grande dificuldade da área de tecnologia em trazer novos leitores. Em resumo, para mim o trabalho foi um sucesso e registro aqui os meus parabéns.
A cartilha apresenta bons textos, bons conteúdos gráficos e é de fácil compreensão. Uma pessoa que é pouco adepta a informática consegue compreende-la bem.
O material ficou incrível, de muito fácil acesso ao leitor que não tem conhecimento prévio. Parabéns amiga!

APENDICE 4: RESPOSTAS EM GRÁFICOS

Consolidação das Respostas do formulário em gráficos:

Gráfico 1: Idade

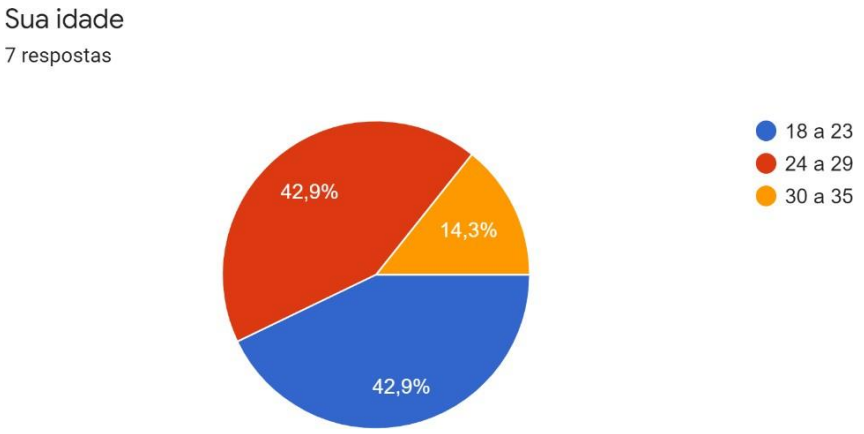


Gráfico 2: Escolaridade

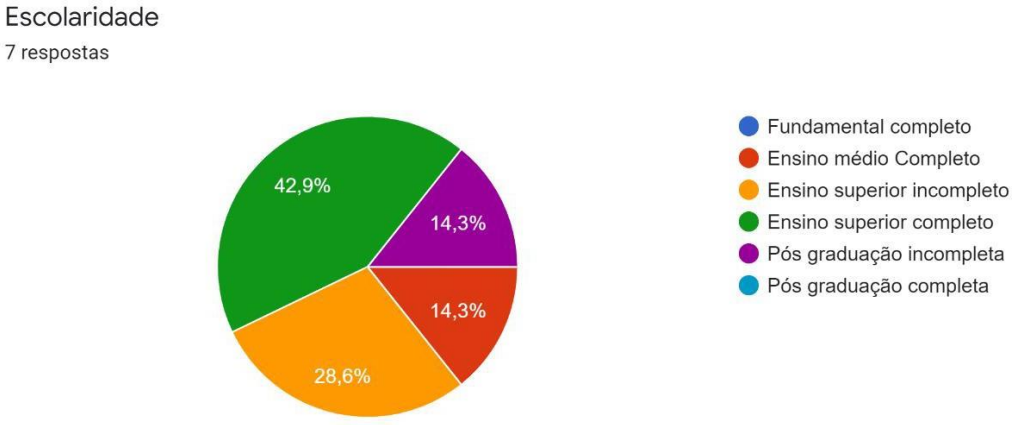


Gráfico 3: Área Macro de estudo

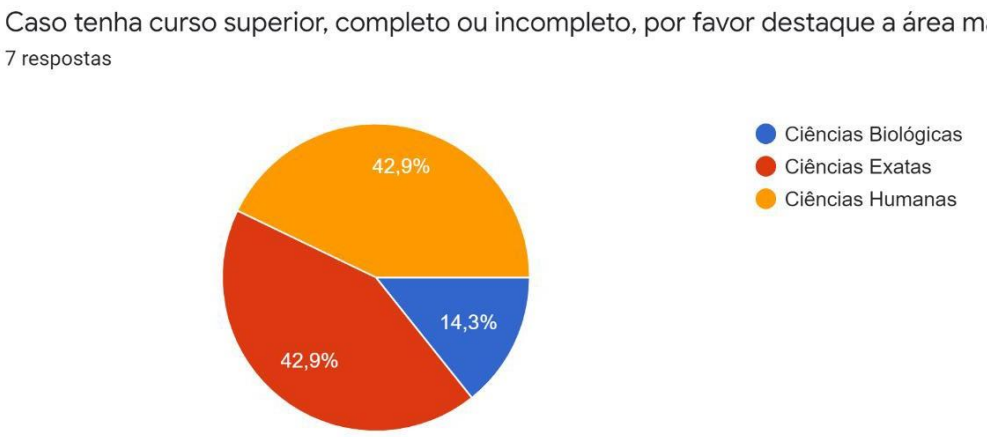


Gráfico 4: Uso do Computador pessoal:

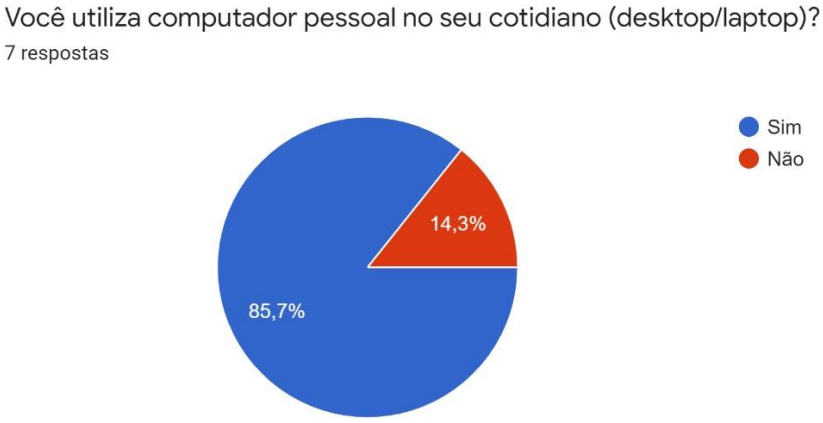


Gráfico 5: Conhecimentos de Informática/Tecnologia:

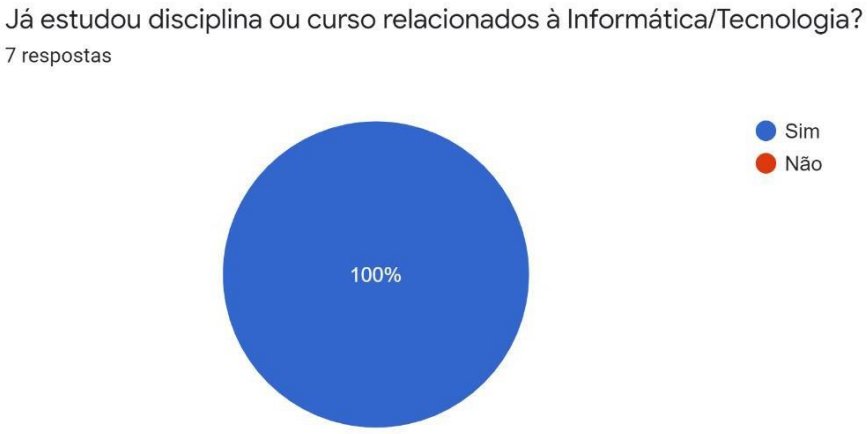


Gráfico 6: Conhecimento de Segurança da Informação anteriores à cartilha:

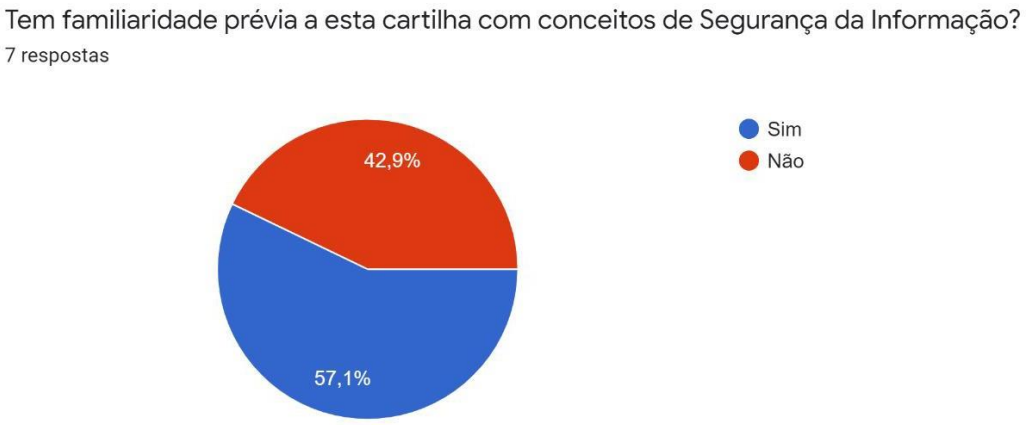


Gráfico 7: Leitura completa da cartilha

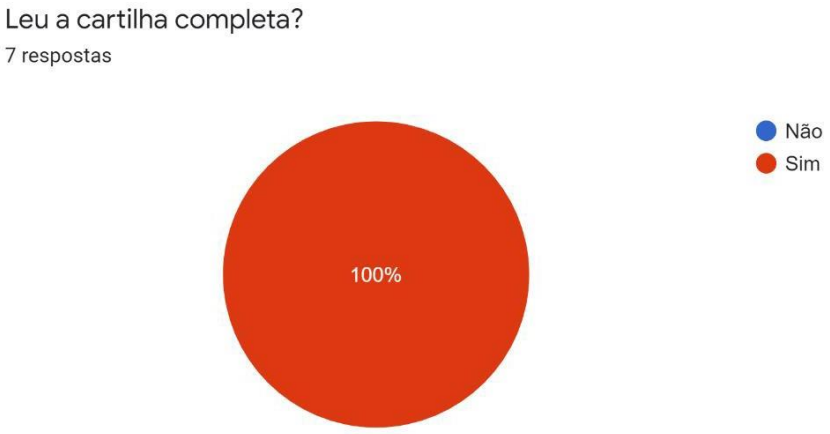


Gráfico 8: Classificação do material apresentado de “ 1 – Inadequado” a “4 – muito Adequado”

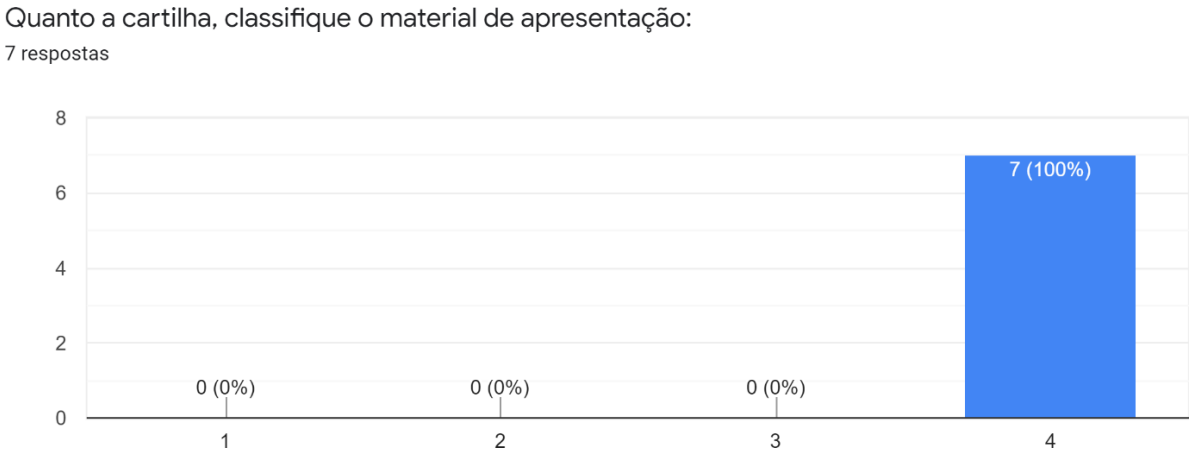


Gráfico 9: Compreensão da linguagem empregada

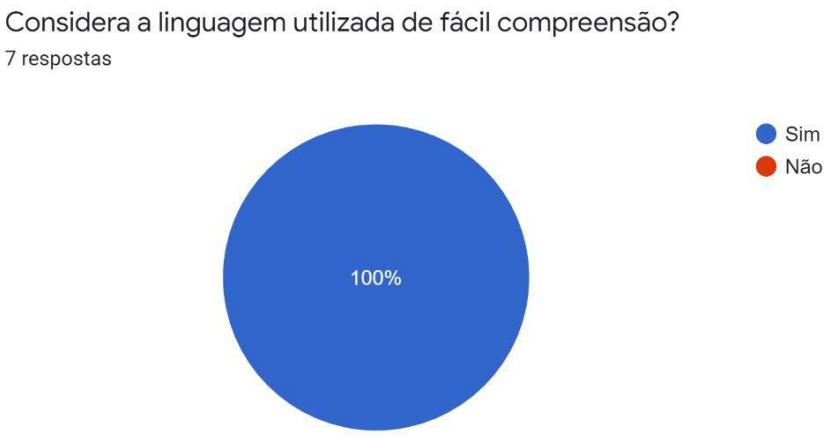


Gráfico 10: Relação dos recursos gráficos o texto

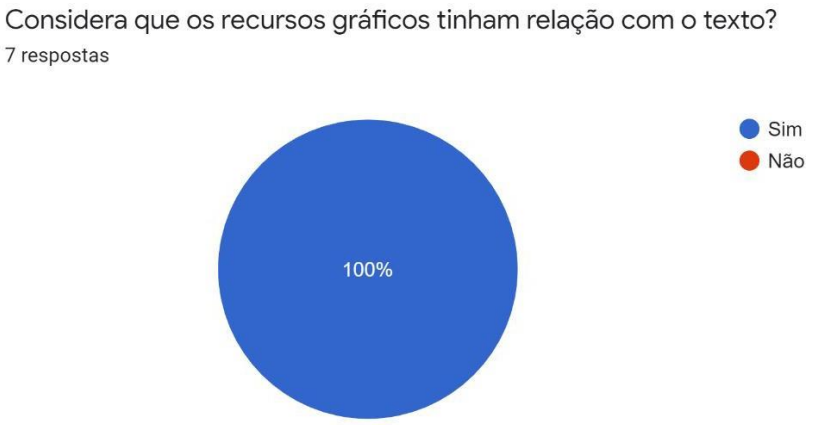


Gráfico 11: Contribuição da Cartilha para melhoria dos conhecimentos em Segurança da Informação

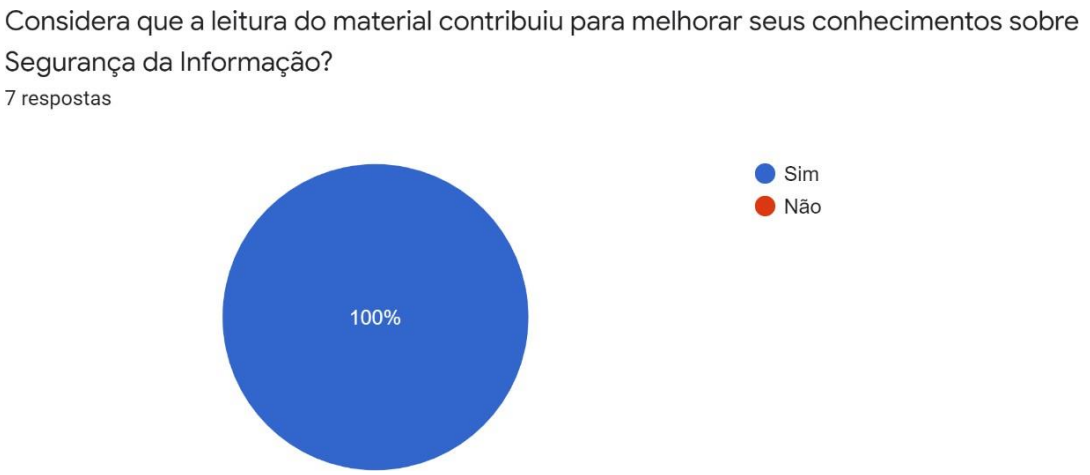


Gráfico 12: Aptidão à aplicação do conteúdo abordado na cartilha