CENTRO UNIVERSITÁRIO SAGRADO CORAÇÃO

WELERSON CASSAMASSO BARBE

APLICAÇÕES DA ARQUITETURA ZERO TRUST BASEADA NAS NORMAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

BAURU
2022

WELERSON CASSAMASSO BARBE

APLICAÇÕES DA ARQUITETURA ZERO TRUST BASEADA NAS NORMAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

Monografia de Iniciação Científica apresentada à Pró-Reitoria de Pesquisa e Pós-Graduação como parte dos pré-requisitos para aprovação do conselho, sob orientação do Prof. Me. Henrique Pachioni Martins.

BAURU
2022

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

Barbe, Welerson Cassamasso

S586d

APLICAÇÕES DA ARQUITETURA ZERO TRUST BASEADA NAS NORMAS DE SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES / Welerson Cassamasso Barbe. – 2022.

63 f. : il. color

Orientador: Prof. Me. Henrique Pachioni Martins.

Monografia (Iniciação Científica em Ciência da Computação) - Centro Universitário Sagrado Coração - UNISAGRADO - Bauru - SP

1. Zero Trust. 2. Segurança da Informação. 3.Normas. 4. Política de Segurança. 5. Organizações. I. Título.

DEDICATÓRIA

Dedico este projeto de pesquisa totalmente a Deus, onde sem Ele eu não poderia ter chegado até aqui.

Aos meus amados pais, Monica Regina Cassamasso Barbe e Delton Aparecido Barbe, onde em todo o processo me incentivaram a realizá-lo, e em todas as dificuldades enfrentá-las da melhor forma.

AGRADECIMENTOS

Agradeço ao meu professor e inspirador, Henrique Pachioni Martins, por ter aceitado acompanhar-me neste, onde, com sabedoria e determinação me orientou durante a realização do projeto de pesquisa. O seu empenho foi essencial para a minha motivação à medida que as dificuldades iam surgindo ao período de realização.

RESUMO

A integração da tecnologia na sociedade moderna está cada vez mais presente e necessária, com isso as brechas, sejam no mundo virtual ou “fisicamente”, estão sendo invadidas e violadas constantemente. Visto tal necessidade de alocarmos o nosso “campo físico” no virtual, é inegável que a exigência de uma política de segurança rígida dentro de uma organização é de grande necessidade, evitando assim descuidos e cuidado com a informação em todo seu processo de movimentação. Uma organização estar protegida, é indiscutivelmente necessário criar um plano de conscientização para a implantação/mudança quanto as prevenções e cuidados com a informação e suas etapas de utilização. Em síntese, o desenvolvimento deste projeto foi realizar uma análise/identificação e disseminação quanto a aplicação do modelo de segurança Zero Trust, baseando-se nas normas de Segurança da Informação, trazendo através de elementos visuais (elaborados no Canva) no Instagram e a elaboração de uma cartilha informativa, podendo assim serem encontradas diretamente a organizações que sentem a necessidade de uma mudança preventiva, caso não tenham uma estrutura de política de segurança, ou necessitem de uma mudança organizacional.

Palavras-chave: Zero Trust. Segurança da Informação. Normas. Política de Segurança. Organizações.

ABSTRACT

The integration of technology in modern society is increasingly present and necessary, with that the gaps, whether in the virtual world or "physically", are being invaded and violated constantly. Given this need to allocate our “physical field” to the virtual, it is undeniable that the requirement of a strict security policy within an organization is of great necessity, thus avoiding carelessness and care with the information throughout its movement process. For an organization to be protected, it is indisputably necessary to create an awareness plan for the implementation/change regarding prevention and care with information and its stages of use. In summary, the development of this project was to carry out an analysis/identification and dissemination regarding the application of the Zero Trust security model, based on Information Security standards, bringing through visual elements (designed in Canva) on Instagram and the elaboration of an informative booklet, so they can be found directly to organizations that feel the need for a preventive change, if they do not have a security policy structure, or if they need an organizational change.

Keywords: Zero Trust. Information Security. Standards. Security Policy. Organizations.

SUMÁRIO

ÍNDICE DE FIGURAS

1. INTRODUÇÃO

A integração da tecnologia na sociedade moderna está cada vez mais presente e necessária, com isso as possibilidades são diversas. Há diversas formas de utilizarmos esta tecnologia, já que a Internet é um dos principais pontos por onde a informação é distribuída de forma constante, seja para gerenciar organizações e grandes quantidades de informações, coordenar finanças, lucros e automatizar as tarefas cotidianas em apenas um clique.

Justamente, com tantos dados disponíveis em poucos acessos, a Segurança da informação é mais que necessária. O termo é usado se referindo à defesa de dados e a prática que assegura informações sigilosas e suas determinadas classificações. Por isso, a segurança da informação é uma grande aliada de organizações, pois é inteiramente responsável por evitar que quaisquer dados se distribuam, de forma indevida, seja por vendas, margem de lucro, entre outras informações, ou seja, a falta de política de segurança controlada pelo departamento de Tecnologia da Informação (TI) de uma organização se faz de extrema necessidade.

O “mundo virtual” é a entrada de muitas ameaças perigosas – através da má gestão de segurança – muitas vezes, causando danos incalculáveis. Quanto maior a ligação do mundo físico e suas importantes informações estiverem ligadas ao mundo virtual, maiores as chances dadas a serem acessados.

Nesse sentido, a arquitetura Zero Trust baseia-se em segurança cibernética e a privacidade de dados, cujo conceito principal é não confiar em nada dentro ou fora da rede da infraestrutura onde é aplicada. Entretanto, a intenção não é encorajar as organizações a não confiar em quem acessa os sistemas de informação, mas ter como objetivo principal rastrear o tráfego da rede, auditar e controlar os acessos para garantir maior segurança do ambiente de uma organização.

Se estamos conectados, estamos vulneráveis. E evitar os acessos indesejados e ataques cibernéticos cada vez mais complexos, requer uma vigilância permanente. É de senso comum sermos um “firewall humano”, tendo maior intelectualidade do que o próprio invasor.

Portanto, é necessário desenvolver um projeto de pesquisa buscando identificar e reconhecer a aplicação da arquitetura Zero Trust, baseando-se nas normas de Segurança da Informação nas organizações, auxiliando para que todos façam um uso mais consciente e assertivo da tecnologia e a informação - estando

atentos e protegidos de acessos indesejados e exposição dos dados na rede de uma organização, bem como:

- Analisar e aderir conhecimento em sites, artigos científicos já existentes, conteúdos essenciais para o desenvolvimento da proposta, levando em pauta tópicos relacionados à Segurança da Informação, Política de Segurança, arquitetura Zero Trust e sobre as normas de Segurança da Informação.
- Analisar o Sistema de Gestão da Segurança da Informação (SGSI) na estrutura organizacional.
- Analisar e identificar a aplicação e funcionamento da arquitetura Zero Trust, baseando-se nas normas de Segurança da Informação, nas organizações
- Criar uma conta no Instagram para promover e divulgar um plano de conscientização de existir uma política de segurança em uma organização, com foco na arquitetura Zero Trust e a sua aplicação, juntamente com a criação de uma cartilha informativa contendo todos os assuntos pesquisados e estudados sobre o assunto determinante.

1.1. REFERENCIAL TEÓRICO

Uma pesquisa exploratória ajuda o pesquisador, a saber, quais das várias opções se aplicam ao problema de pesquisa. Além disso, poderá também auxiliar a estabelecer as prioridades durante a pesquisa. As prioridades poderão ser estabelecidas porque uma particular hipótese explicativa surgida durante a pesquisa exploratória parecerá mais promissora que as outras. Além do mais, a pesquisa exploratória poderá gerar informações sobre as possibilidades práticas da condução de pesquisas específicas (MATTAR, 2012).

Assim, este projeto inicialmente foi construído por uma pesquisa exploratória, que buscou estudar os termos principais que norteiam a proposta desta pesquisa.

Os materiais teóricos estudados foram diversos, os quais estão relacionados com a ideia total do trabalho, envolvendo estudos e coleta de dados sobre segurança da informação e os processos organizacionais com a aplicação da arquitetura Zero Trust baseada nas normas de Segurança da Informação.

A constituição da maior parte do projeto de pesquisa tem como base teórica, e já estruturada para fim de ser utilizada em publicações confeccionadas no Canva e publicadas no Instagram, juntamente com a criação da cartilha informativa no final do projeto de pesquisa, onde serão realizadas futuramente neste projeto presente.

1.1.1. SEGURANÇA DA INFORMAÇÃO

Na etapa introdutória da pesquisa foi realizado pesquisa integra e levantamento bibliográfico acerca de Segurança da Informação e toda a sua estrutura nos conceitos teóricos em pesquisas de internet, artigos científicos etc.

A Segurança da Informação é alcançada através da implementação de um conjunto adequado de controles, incluindo uma política de segurança, processos, procedimentos, estruturas organizacionais, implementados, monitorados, revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança do negócio da organização sejam atendidos. Andando em conjunto com outros processos de gerenciamento de negócio, baseando-se tudo na informação.

De acordo com Peixoto (2006, p. 37), “O termo segurança da informação pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade”.

Segurança da informação está relacionada num todo à proteção de um conjunto de dados, um conjunto simples de palavras, mas fundamental importância para qualquer empresa, em ênfase ao setor de TI.

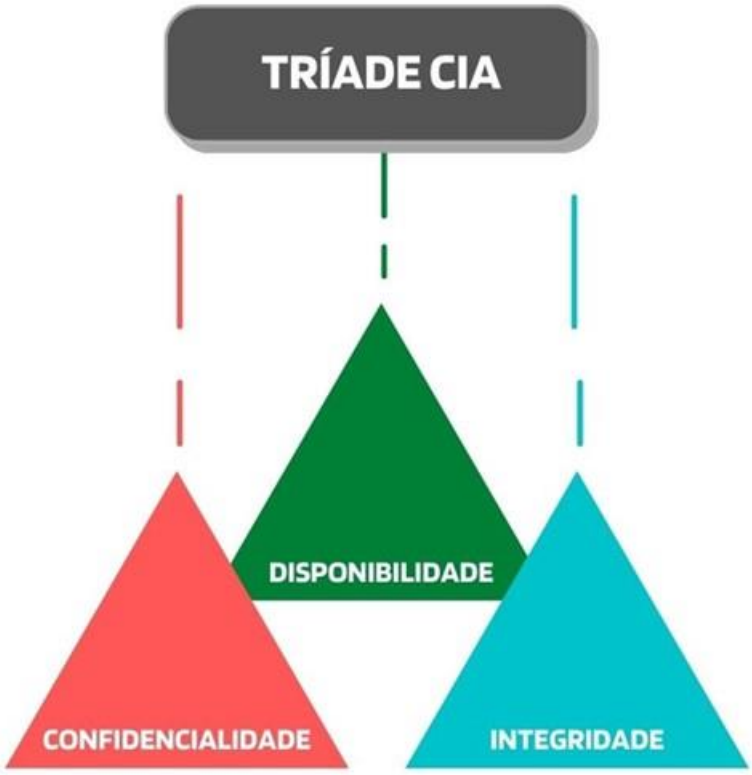
> A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às informações corporativas quanto aos pessoais. (FRAGA, 2019, p. 14).

Constitui-se em características básicas os atributos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, não sendo aplicada somente a sistemas computacionais, eletrônicas ou sistemas de armazenamento. O conceito se aplica a qualquer aspecto onde há proteção de informações de dados de usuários.

A tríade CIA (Confidentiality, Integrity and Availability) – Confidencialidade, Integridade e Disponibilidade representa os atributos que orientam a análise, o

planejamento e a implementação da segurança da informação. A Figura 1 a seguir representa e facilita a visualização o tripé principal da segurança da informação:

Figura 1: Tríade CIA



Fonte: Elaborada pelo autor, 2021

- Confidencialidade consiste em limitar o acesso à informação tão somente aos usuários legítimos, aqueles no qual são autorizados pelo proprietário da informação requerida.
- Integridade se define e garante que um serviço/informação será completa e genuína, ou seja, contra a personificação de intrusos, sem que haja partes faltantes.
- Disponibilidade, como o próprio nome sugere, é manter as informações sempre que disponíveis para o uso legítimo, ou seja, pelo proprietário da informação. O nível de segurança desejado é limitado pela “política de segurança”, que é seguida pela organização ou pessoa.
- Autenticidade é a propriedade que assegura que toda informação está correta, sem alterações.

- Legalidade define que toda informação e toda qualquer manipulação/alteração referente a mesma, está de acordo com a legislação determinada pelo país local.

1.1.2. O FATOR HUMANO

Segundo Kevin Mitnick (2003):

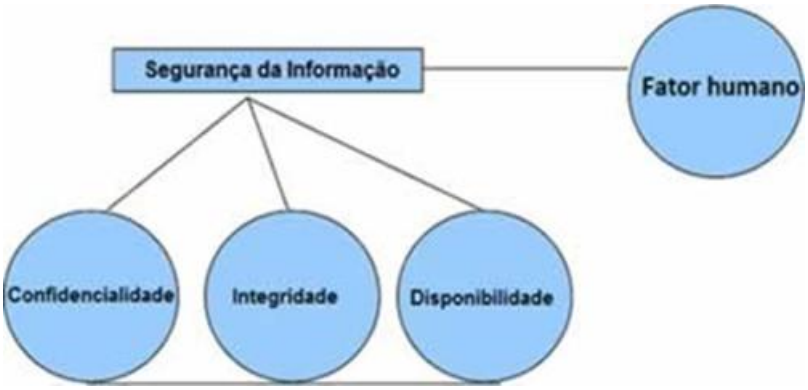
> Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).

Por maior que seja a segurança em uma organização, sempre haverá um fator de desequilibro chamado “fator humano”. Os maiores engenheiros sociais tiram proveito das fraquezas, incluindo gostos pessoais, costumes etc.

Um dos maiores problemas, se não o maior, na segurança da informação está relacionado ao ser humano e a sua falta de conhecimento – ignorância. Práticas não saudáveis ao sistema, em acessos não autorizados a dados, lugares, objetos, entre outros vulnerabiliza qualquer sistema de segurança da informação, abrindo brechas.

Existem propostas de modelos, onde a tríade CIA, citada anteriormente, é composta por mais um fator, sendo ele primordial: fator humano. Hoje é considerado como um fator nível não base – não sendo considerado fundamental, bem como representado na Figura 2, onde é representada a parte da tríade CIA. Por ser considerado um pondo fundamental, a propostas de se tornar parte da tríade da Segurança da Informação, representada também na Figura 3.

Figura 2: Atual modelo de Segurança da Informação



Fonte: (SILVA, M; COSTA, 2009)

Figura 3: Proposta de modelo de segurança da informação

Fonte: (SILVA, M; COSTA, 2009).

1.1.3. POLÍTICA DE SEGURANÇA

> Como diz o ditado; até mesmo os verdadeiros paranoicos provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus — os atacantes que visam a infraestrutura da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados. (MITNICK; SIMON, 2003, p. 23).

É necessário que haja uma série de procedimentos estabelecidos dentro de uma organização, para evitar – ou diminuir – o risco de que as informações sejam acessadas indevidamente, perdidas ou até mesmos alterados.

Política de segurança da informação pode ser definida como uma série de instruções bem claras a fim de fornecer orientação para preservar as informações. Esse é um elemento essencial para o controle efetivo da segurança da informação de maneira a combater e prevenir possíveis ameaças ou ataques que venham a comprometer a segurança da informação nas empresas ou organizações.

Ao estabelecer uma política para a Segurança da Informação, a administração provê as diretivas e o apoio para a organização. Essa política deve ser escrita em conformidade com os requisitos dos negócios, bem como as leis e os regulamentos relevantes. A Política de Segurança da Informação deve ser aprovada pelo conselho de administração e publicada para todo o seu pessoal e todos os parceiros externos relevantes, tais como clientes e fornecedores. Na prática, ela é distribuída normalmente como uma versão resumida delineando os principais pontos. Essa distribuição pode ser feita na forma de um folheto emitido para todos os funcionários. A versão completa pode ser publicada na intranet da empresa ou em algum outro lugar que seja facilmente acessível para todos os funcionários. Entretanto, somente a publicação na intranet não é garantia de que será lida para todos os funcionários. Deve haver algum programa de conscientização bem balanceado para alcançar todos os funcionários. Deve haver algum programa da conscientização bem balanceado para alcançar a todos.

É comum um documento de políticas ter uma estrutura hierárquica. Vários documentos de política são desenvolvidos, tendo como base uma política de segurança corporativa de alto nível. Eles devem estar sempre em conformidade com a política corporativa e prover diretrizes mais detalhadas para uma área específica. Um exemplo disso é um documento de política sobre o uso de criptografia.

De acordo com o que diz Fonseca (2009), é necessário que haja um treinamento de capacitação com os funcionários, e claro, as políticas e procedimentos devem ser muito bem documentadas. É importante pontuar que a política de segurança não elimina as possibilidades de um ataque de engenharia social, pois pode não ser seguida corretamente por todos os funcionários da organização, nem eliminar os pensamentos deles.

A Figura 4 representa como é importante um ambiente com políticas de segurança, pois a postura de uma pessoa pode não ser de boa intenção, seja com uma proposta enganosa, ou até mesmo por descuido próprio. Pois caso não tenha cuidado, as situações podem ser bem preocupantes:

Figura 4: Falta de Política de Segurança

Fonte: (PEIXOTO, 2006).

1.1.4. ESTRUTURA ORGANIZACIONAL

> O SGSI não é uma ferramenta tecnológica, como o nome pode levar a crer; é um instru-mento completo de gestão que inclui, por exemplo, definição da estrutura organizacional, definição de papéis e políticas de segurança. (MORAIS; ANGÉLICA, 2021).

A princípio, foi visto tópicos de importância no qual a Segurança da Informação está atrelada dentro de uma estrutura organizacional:

- Compreender os requisitos de segurança da informação da organização e a necessidade de estabelecer políticas e objetivos para a segurança da informação.
- Implementar e operar controles parar gerenciar os riscos de segurança da informação da organização no contexto dos riscos gerais de negócio da organização.
- Monitorar e revisas o desempenho e a eficácia do Sistema de Gerenciamento de Segurança da Informação (Information Security Management System – ISMS).

- Melhoria contínua baseada em medições objetivas.

1.1.5. SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Nesta etapa da pesquisa foi notório a essencialidade do Sistema de Gestão de Segurança da Informação (SGSI) para que uma política de segurança seja aplicada e continuada dentro de uma organização

O SGSI é basicamente um ecossistema inteiro de todas as estratégias, políticas, medidas de controle, contidas na Segurança da Informação. O sistema de gestão corporativo inclui toda a abordagem organizacional usados para proteger a informação empresarial e seus critérios de Confidencialidade, Integridade e Disponibilidade, e é descritivo em sua totalidade na ISO 27.001:2005.

Inicialmente, a organização definirá um escopo do sistema, como por exemplo, quais processos organizacionais, departamentos e partes interessadas se aplica. Tendo como objetivo os controles selecionados, já que a empresa deve a empresa deve declarar quais medidas foram selecionadas para tratar a segurança da informação, ou seja, uma declaração de aplicabilidade, com os objetivos de controle selecionados.

A organização deve definir os limites e a aplicabilidade do sistema de gerenciamento de Segurança da Informação, a fim de estabelecer seu escopo. Ao definir o seu escopo, a organização deve considerar as questões internas e externas. O escopo deve estar disponível como informação documentada.

1.1.6. O MODELO PDCA

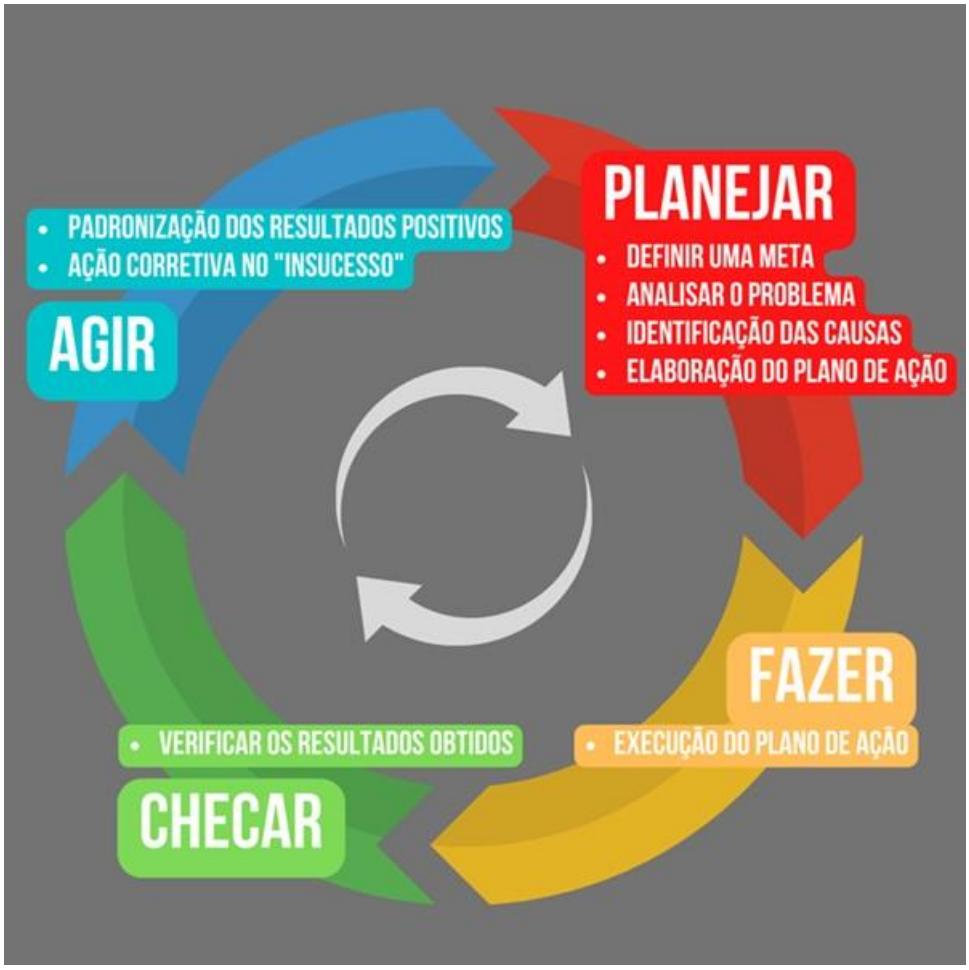
O modelo Planejar-Executar-Chegar-Agir (Plan-Do-Check-Act – PDCA), também chamado de ciclo de qualidade de Deming, forma a base para determinar, implementar, monitorar, controlar e manter o sistema de gerenciamento da segurança da informação.

A ISO 27.001:2005 exigia o modelo PDCA como base geral para implementação e a manutenção do ciclo de gestão, porém, na ISO 27001:2013 foi realizado uma alteração, pois a ISO percebeu que a maioria das empresas e

organizações já possuía seu próprio ciclo de gestão de negócios, sendo ou não baseado no PDCA.

As etapas a serem seguidas são: Planejar, Fazer, Checar e Agir, bem como representadas na Figura 5, juntamente com o ciclo a ser realizado.

Figura 5: Modelo PDCA



Fonte: Elaborada pelo autor, 2022

- PLAN (Planejar) – Neste primeiro passo para a aplicação, deverá ser elaborado um plano. Desenvolvendo, com base nas diretrizes e políticas da sua empresa, uma estratégia que se proponha a resolver problemas pautados. Como ocorre em qualquer planejamento, a elaboração desta etapa serve para evitar falhar e perdas de tempo desnecessárias nas próximas fases do ciclo PDCA.

- DO (Fazer) – Após o planejamento for feito, neste ponto ele será colocado em prática, consistindo em treinar os envolvidos para prepará-los para o método que será proposto.
- CHECK (Checar) – O terceiro passo é a análise/verificação dos resultados alcançados e dos dados coletados. Quando verificado se o trabalho está sendo feito da forma devida – quanto após a execução, quando são feitas as análises estatísticas dos dados e a verificação de todos os itens, sendo como principal objetivo desta fase é detectar eventuais erros ou falhas.
- ACT ou Adjust (Agir, Corrigir) – A última fase consiste na correção com base no que foi verificado, ou seja, deve-se corrigir as falhar encontradas no passo anterior. Após a realizada investigação das causas destas falhas ou desvios no processo, irá ter um reinício. Um ciclo PDA deve ser retomado sempre para que, as práticas e os processos se aprimorem continuamente.

1.1.7. CLASSIFICAÇÃO DA INFORMAÇÃO

É possível definir qualquer elemento que for identificado em sua forma bruta o dado, onde, por si só não conduz o entendimento e compreensão do tema. Seguindo pela informação. Após esses dados serem processados e trabalhados, podemos se obter a informação, onde é gerado um conjunto de dados interligados entre si, trazendo o significado sobre um determinado assunto. A palavra informação tem origem do latim *informationem*, que significa “delinear”, conceber uma ideia", ou seja, moldar na mente. Segundo Rezende e Abreu (2000), informação é um dado com interpretação lógica ou natural agregada pelo usuário. A informação pode ser um bem ou ativo, como qualquer outro bem físico, importante para negócios e trâmites, que possuem um determinado valor, consequentemente, necessita ser adequadamente protegido, conforme recomenta a ABNT NBR ISO/IEC 17799 de 2005.

Segundo Laureano e Moraes (2005), nem toda informação precisa de cuidados especiais. Já por outro lado, uma determinada informação pode ser vital o suficiente a custo de ser exposta em um determinado nível, pode prejudicar organizações de

uma forma crucial. A informação pode ser classificada de acordo com o seu nível de sigilo, priorizando o conteúdo estabelecido:

- Pública: sua integridade não é vital, não oferecendo um risco a um sistema/organização, podendo ser divulgada em redes sociais, popularizando o negócio e/ou imagem, ou seja, essa informação, se exposta, traz vantagens.
- Corporativa/interna: integridade de uso interno a corporação, tendo como consequência não tão séria, se porventura ocorrer acesso não autorizado. Mesmo não sendo vital, é muito importante.
- Confidencial: neste nível, o cuidado com a determinada informação é fundamental, pois dentro de um sistema/organização, pode-se obter vantagens competitivas, gerando na mesma um desequilíbrio operacional. Acompanhado de perdas de informações financeiras, podendo ocasionar situações gravíssimas de perda.
- Secreta: esse tipo de informação jamais deverá ser exposto, pelo seu nível de vital importância, trazendo riscos políticos e/ou estratégicos.

1.1.8. CICLO DE VIDA DA INFORMAÇÃO

É necessário que as informações estejam rotuladas de uma forma clara, classificadas tal como pertencentes a uma organização. Segundo apontam Laureano e Moraes (2005), algumas informações são cruciais para uma organização, se divulgadas, podem ter uma repercussão, cujo efeito poderá ser irreversível para ela. Por isso, se faz necessário a CIA, como citado anteriormente.

A informação é o item com maior importância dentro de uma organização, com isso, torna-se indispensável a devida proteção para o seu ciclo de vida, principalmente em sua criação. O momento de criação de uma informação é extremamente importante validar uma atenção especial, pois é ali onde processos e decisões possam a ter um início. Com isso, a informação tem o seu ciclo de vida, tendo como início a criação/manipulação, armazenamento, transporte e descarte. As fases do ciclo se dão da seguinte forma, de acordo com Oliveira (2011):

- Manipulação: este ponto reúne os processos iniciais da informação, a sua criação, alteração e processamento inicial dela. Nesta fase, pode ocorrer um grande marco com relação a segurança, pois a informação está exposta a entidades que a utilizam.
- Armazenamento: refere-se ao armazenamento da informação, seja físico, digital, magnéticos ou qualquer outro suporte. Nesta fase, vale ressaltar a importância dos pilares de segurança da informação, já dito anteriormente, a tríade C.I.A. A fase de arquivamento é um processo de guarda das informações que não estão mais em uso, ou se transformaram em arquivos mortos para a organização.
- Transporte: deve-se a transferência e movimentação dos dados, entre processos, e-mails, pasta de arquivos na rede, pen drives, inclusive o diálogo falado, deixando vazar informações valiosas. É importante este ponto para que nada seja revelado de forma descuidada.
- Descarte: ações de descarte e destruição das informações. Os documentos que não tiverem mais utilidades devem ser triturados, já os documentos eletrônicos devem ser transferidos para uma mídia transportável, chamadas firewalls.

1.2. ANÁLISE DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO

A análise das normas de Segurança da Informação abrangeu todo o campo das existentes, mas nenhuma em específico, já que todas são importantes para o funcionamento.

O motivo da análise das normas se deu pela base onde toda política de segurança se faz através de estruturas já associadas e já utilizadas por muitos, baseando-se nas normas, seja qual for. A abrangência das normas cobre toda uma organização, pessoas e instalações. Um grande exemplo que temos como base, por exemplo, é a NBR ISO/IEC 27.002:2013, trazendo uma certificação de aceitação global para quem a realiza, ou seja, uma empresa que possui um profissional baseado nesta ISO e um plano de conscientização (SGSI) muito bem estruturado, tornará a

empresa mais competitiva no mercado, ganhando confiança no fechamento de contratos, por exemplo.

Os benefícios do uso de normas de Segurança da Informação dentro de uma empresa são diversos, pois as normas auxiliarão a criação de uma nova política, reduzindo os riscos. Seja qual for a estrutura de uma empresa/organização, pequena ou grande, uma política de segurança só trará benefícios e segurança para quaisquer informações que serão tratadas e movimentadas, não especificamente dentro da tecnologia, mas em todas as áreas e ocupações. Auxiliando assim na determinação de políticas e procedimentos, bem como a seguir os pontos identificados ao decorrer desta etapa:

- Focada amplamente na responsabilidade dos colaboradores, não focando apenas em levantar o problema, mas também responsabilizar os colaboradores para que haja uma colaboração entre as pessoas dentro de uma organização.
- Melhoria contínua: oportunidade não só de corrigir os pontos fracos, mas melhorar os pontos fortes.
- Utilizada para medir o sucesso e aplicabilidade do Sistema de Gestão de Segurança da Informação (SGSI).
- Concede mais credibilidade e confiança aos parceiros, clientes e demais relacionamentos.

1.3. ARQUITETURA ZERO TRUST

O mundo da tecnologia está mudando, juntamente, as aplicações estão migrando para a nuvem, como por exemplo: os trabalhos em home office (remoto). Empresas de todo o mundo estão permitindo que os funcionários usem dispositivos pessoas para acessar informações corporativas. Embora as empresas ainda precisem suportar sistemas legados, hospedados no data center e acessados via VPN (Virtual Private Network), elas também precisam de soluções de acesso diferentes para cada tipo de aplicação e uso, sendo de uma forma obrigatória a registrar seus dispositivos em um programa de gerenciamento de dispositivos, para que assim os controles de segurança possam ser aplicados. Contudo, essas soluções não oferecem segurança

absoluta para a organização, já que confiam automaticamente no usuário ou no dispositivo gerenciado dentro da rede corporativa. O dispositivo pode estar comprometido ou o usuário ser um invasor/engenheiro social.

O conceito de Zero Trust foi criado por John Kindervag, durante sua gestão como vice-presidente e analista principal da Forrester Research, baseando-se na percepção de que os modelos de segurança tradicionais operam com base no pressuposto de que tudo dentro da rede de uma organização deve ser confiável. Este modelo reconhece que a confiança é uma vulnerabilidade. Uma vez na rede, os usuários mal-intencionados - são livres para mover-se e transferir quaisquer dados no qual tem acesso.

Segundo Golubev (2020), a arquitetura Zero Trust é um modelo de segurança para o mundo. Ele traz como princípio não confiar em nenhum usuário, dispositivo ou rede. Ele monitora e verifica continuamente a identidade do usuário e suas ações, mesmo após o login. Esse modelo consolida várias técnicas de segurança e provê uma melhor experiência do usuário. Tendo início dessa ideia que a confiança deve ser conquistada em fatores como contexto, identidade, postura do dispositivo, período do dia e perfil de risco do usuário, o sistema concede ou restringe o acesso aos recursos corporativos. Uma prática popular de Zero Trust é o acesso contextual e adaptativo aos dados corporativos, o usuário é autenticado usando políticas de acesso contextual no momento do login. Ele é monitorado continuamente e ganha confiança com base em suas ações dentro do sistema, uma forma de recompensa pela sua postura, já por outro lado, qualquer atividade maliciosa, alerta o sistema para realizar ações como uma nova autenticação, sendo gravada a sessão ou notificação de um administrador, para que assim ele monitore o usuário e intervenha nas ações. Em suma, para o usuário final, isso significa poder se concentrar no trabalho, com tranquilidade.

2. MATERIAIS E MÉTODOS

A princípio, este trabalho caracteriza-se como uma pesquisa exploratória e tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses (GIL, 2002).

A definição do problema foi alicerçada através de levantamento bibliográfico, constituído principalmente de livros e artigos de periódicos científicos, bem como na experiência do autor.

De acordo com Lakatos e Marconi (1992, p. 43), a finalidade da pesquisa bibliográfica é colocar o pesquisador em contato com tudo aquilo que já foi escrito sobre determinado assunto. A pesquisa bibliográfica não é mera repetição do que já foi dito ou escrito sobre determinado assunto, mas “oferece meios para definir, resolver, não somente problemas já conhecidos, como também explorar novas áreas, onde os problemas ainda não se cristalizam suficientemente” (MANZO, 1971 citado por LAKATOS; MARCONI, 1992, p. 43).

No levantamento bibliográfico, foram abordadas teorias necessárias ao desenvolvimento deste projeto. Este levantamento bibliográfico foi baseado em consultar à literatura especializada e de alta relevância científica, incluindo: monografias, dissertações, teses, livros, sites e documentos e artigos científicos.

Após concluir a pesquisa bibliográfica, foi realizada uma seleção de conteúdos relacionados ao tema do projeto, com o intuito de auxiliar o desenvolvimento da proposta.

Como continuidade na pesquisa, foi definido quais os pontos fundamentais acerca da aplicação da Arquitetura Zero Trust sendo aplicada como uma Política de Segurança dentro de uma organização.

Por fim, foi elaborado postagens em uma página no Instagram, confeccionadas no Canva, com a conscientização e a importância da criação/renovação de uma Política de Segurança acerca da Arquitetura Zero Trust. Consequentemente, feito uma cartilha informativa com o mesmo local de divulgação.

O projeto será apresentado no Fórum de Iniciação Cientifica do UNISAGADO, bem como, submetido a eventos/revistas científicas da área (em caso de oportunidades propostas).

2.1. ANÁLISE DE RESULTADOS

Ao final da pesquisa, foi possível compreender o funcionamento da aplicação da Arquitetura Zero Trust dentro de uma organização, bem como a sua integridade, avaliados os seguintes aspectos dentro da Segurança da Informação e suas normas:

a) Confidencialidade;
b) Integridade;
c) Disponibilidade;

2.2. FERRAMENTAS UTILIZADAS – CANVA E INSTAGRAM

As ferramentas utilizadas neste projeto deveram-se a escolha pela praticidade de uso, tendo ambas com o objetivo de realizar a confecção e divulgação do material proposto.

A escolha do Canva deveu-se a ser uma plataforma de conhecimento prévio do pesquisador e acessível a todos, principalmente com planos para estudantes (e-mail institucional), onde foi possível aderir o Canva Pro, já que as possibilidades de templates e resoluções para banners são diversas. Contando também com o fácil manuseio (didático) a novos usuários.

No outro extremo, o Instagram foi utilizado para ser realizada as divulgações, já que é uma plataforma conhecida e utilizada por muitos, inclusive organizações. Trazendo também a possibilidade de vários meios de postagem, seja temporária ou fixa, sendo também de conhecimento prévio do pesquisador.

2.3. HARDWARE UTILIZADO

O projeto foi desenvolvido utilizando como principal ferramenta um computador pessoal, com o sistema operacional Windows 11 Home – 64 bits, processador Intel® Core™ i7-8565U CPU @ 1.80GHz 1.99GHz, Memória RAM de 8,00 GB, NVIDIA GeForce MX110. O fundamento da escolha do computador se deve pela razão de pertencer ao pesquisador, além de, em primeiro momento, suprir as necessidades de pesquisas teóricas e práticas.

3. RESULTADOS

Neste tópico são apresentados os resultados que foram alcançados no desenvolvimento do projeto de pesquisa. Os resultados foram baseados na análise e levantamento bibliográfico, em conjunto com a coleta de dados sobre o funcionamento e aplicação da arquitetura Zero Trust baseada em normas de Segurança da Informação em organizações. Sendo dividida entre os resultados obtidos através das postagens e a cartilha informativa de conscientização realizadas no Instagram.

3.1. COLETA DE DADOS

Previamente as postagens de conscientização e a cartilha realizadas, foi realizada pesquisas e levantamento bibliográfico sobre a aplicação arquitetura Zero Trust, baseando-se nas normas de Segurança da Informação nas organizações, auxiliando para que o uso da tecnologia e a informação seja consciente e assertivo, protegendo assim a exposição dos dados na rede de uma organização.

3.2. REDE SOCIAL DE DIVULGAÇÃO

O Instagram foi selecionado para realizar a divulgação da conscientização, por ser uma plataforma conhecida e utilizada por muitos do meio organizacional, e por ser de conhecimento prévio do pesquisador.

3.3. NOMEAÇÃO DO PERFIL E LOGOTIPO

Foi realizado a criação de um perfil somente para as publicações do projeto de pesquisa, nomeado de *Security Verse* (@securityverse) – *“Conscientização & Segurança em seu universo!”*.

Figura 6: Perfil no Instagram

Fonte: Elaborada pelo autor, 2022

Figura 7: Logotipo

Fonte: Elaborada pelo autor, 2022

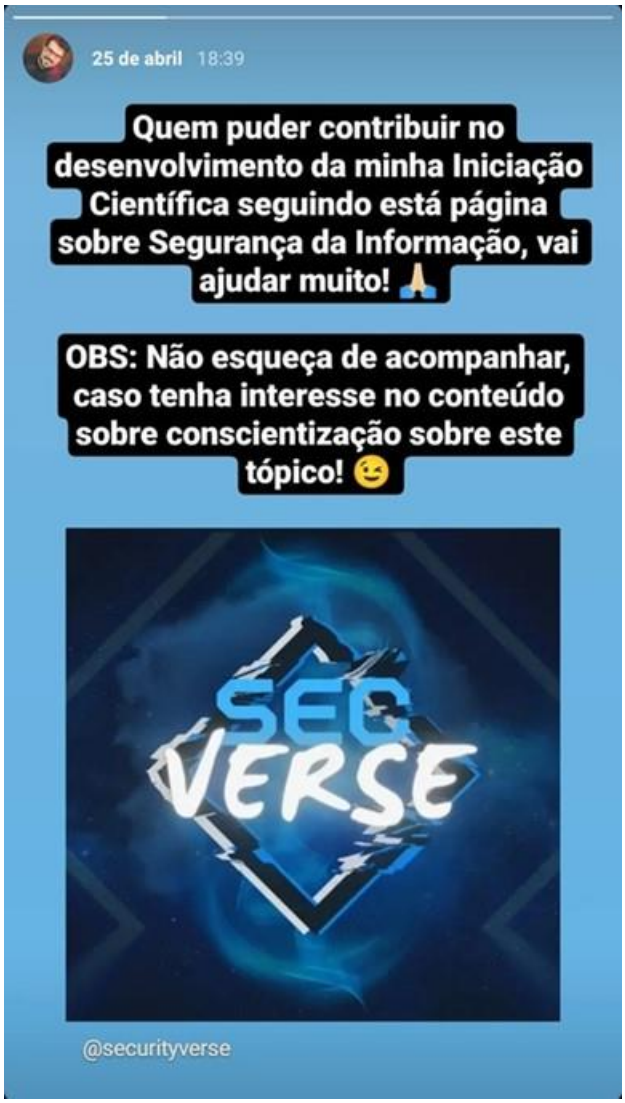
3.4. PLANO DE CONSCIENTIZAÇÃO APLICADO

O principal objetivo deste projeto de pesquisa foi o plano de conscientização realizado por postagens realizadas na rede social do Instagram, com intuito trazer o conhecimento não só apenas da arquitetura Zero Trust, mas da conscientização de

proteção de uma organização, levando em pauta tópicos relacionados à Segurança da Informação, Política de Segurança, e Segurança da Informação.

Posteriormente as publicações no Instagram, foi realizado a divulgação nos *stories* e enviado as postagens via *direct* na rede social, juntamente com o envio realizado no WhatsApp e verbalmente, registrados na Figura 8 e 9 a seguir:

Figura 8: Divulgação do @securityverse



Fonte: Elaborada pelo autor, 2022

Figura 9: Divulgação de post via *story*

Fonte: Elaborada pelo autor, 2022

3.4.1. PLANO DE CONSCIENTIZAÇÃO: ZERO TRUST

A publicação principal e a primeira foram sobre o Zero Trust, onde foi abordado sobre a sua origem, significado, intenções e princípios. Pontos essenciais para que uma pessoa que não possuía conhecimento prévio tenha facilidade para compreensão das abordagens sobre os tópicos, iniciando-se na Figura 10 e 11:

Figura 10: Conscientização Zero Trust

Fonte: Elaborada pelo autor, 2022

Figura 11: O que é Zero Trust?

Fonte: Elaborada pelo autor, 2022

Foi necessário explicar a origem do Zero Trust para se obter um embasamento teórico por trás da arquitetura trazer credibilidade para o usuário, sendo representado pela Figura 12:

Figura 12: Origem do Zero Trust

Fonte: Elaborada pelo autor, 2022

A desperimetrização é uma estratégia de Segurança da Informação para remover a segurança padrão de “limite” que separa uma rede da Internet e, em vez disso, criar um sistema de segurança segmentado por multicamadas baseado em criptografia e autenticação, ou seja, o Zero Trust fornece segurança em camadas por meio de autenticação constante e desconfiança inerente de todos os dispositivos, usuários e ações, estando dentro do perímetro organizacional ou não. Desta maneira, é necessário que o usuário compreenda a base da segurança, representado pela Figura 13:

Figura 13: A base do Zero Trust, De-perimeterization

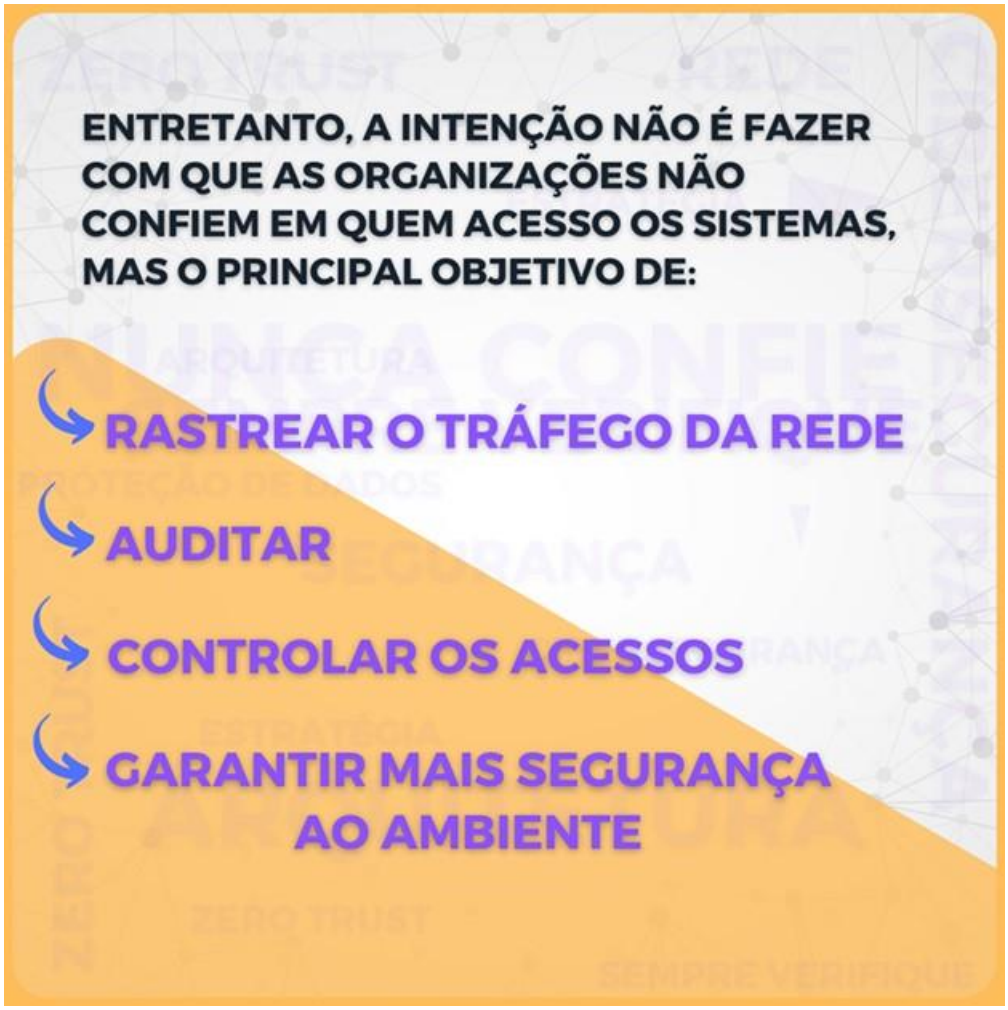
Fonte: Elaborada pelo autor, 2022

Na Figura 14 e 15 foi apresentado para o leitor o significado e o principal conceito do Zero Trust em uma organização, bem como suas intenções.

Figura 14: Significado do Zero Trust

Fonte: Elaborada pelo autor, 2022

Figura 15: Intenções do Zero Trust



Fonte: Elaborada pelo autor, 2022

Na Figura 16 foi finalizado a postagem sobre o Zero Trust com a frase mais conhecida no meio desta arquitetura, de nunca confiar e sempre verificar.

Figura 16: Princípio do Zero Trust

Fonte: Elaborada pelo autor, 2022

3.4.2. PLANO DE CONSCIENTIZAÇÃO: CICLO DE VIDA DA INFORMAÇÃO

A importância e o cuidado com a informação (Figura 17 e 18), seja ela qual for em seu nível de importância ou de curto prazo, a conscientização deste foi imprescindível de sua realização, para em conjunto o usuário ter ciência dos cuidados a se realizar em sua organização.

Figura 17: Conscientização da Informação

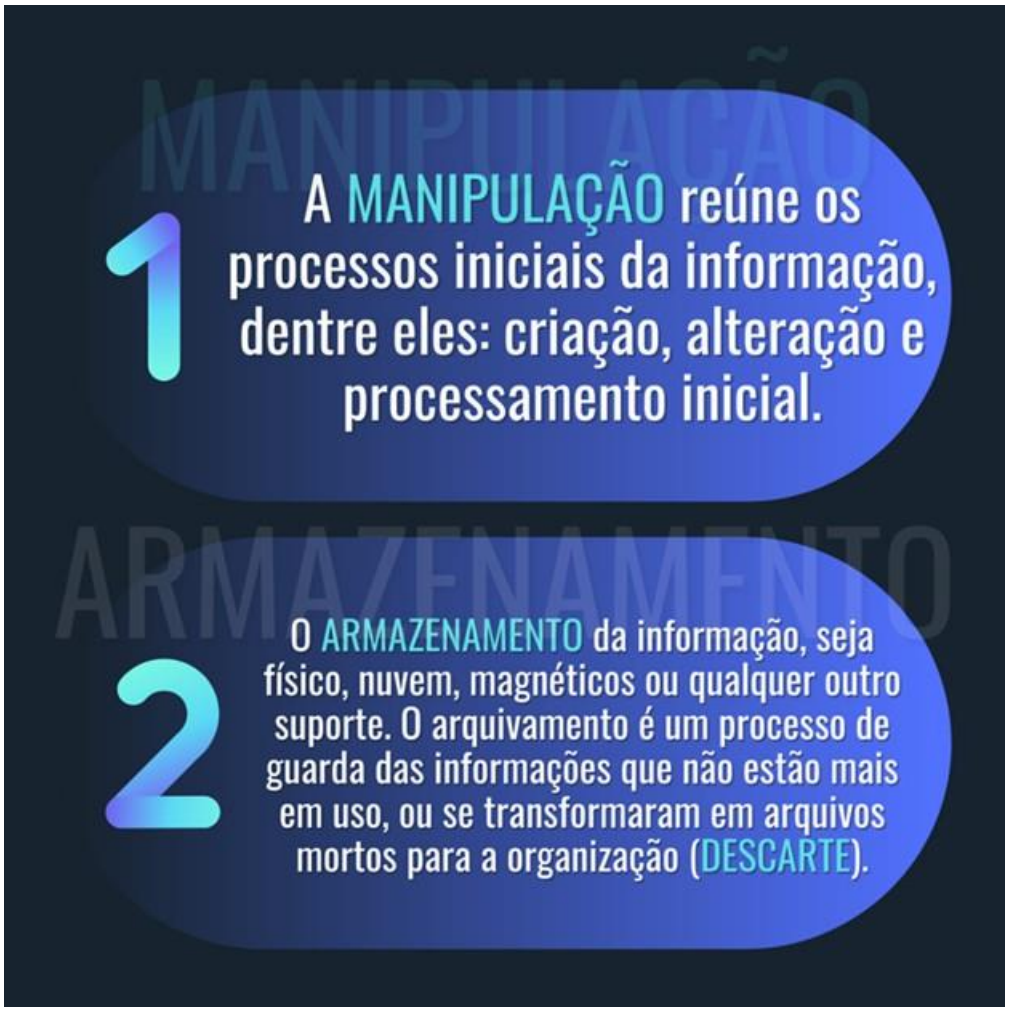
Fonte: Elaborada pelo autor, 2022

Figura 18: Ciclo de Vida da Informação

Fonte: Elaborada pelo autor, 2022

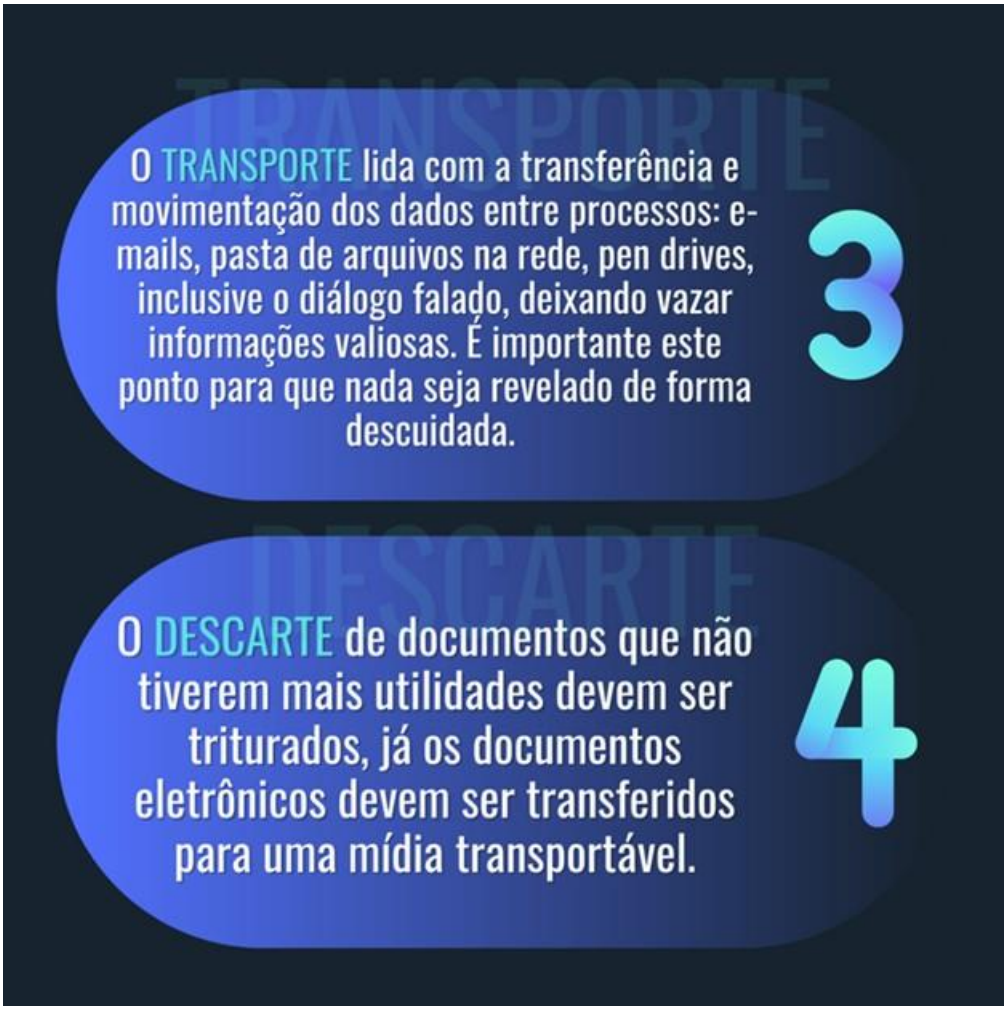
Nas figuras 19 e 20 foram apresentados os 4 ciclos de vida da informação com base em todo o seu processo, da criação até a exclusão. Em cada um dos pontos o cuidado com a informação se torna essencial.

Figura 19: Manipulação e Armazenamento



Fonte: Elaborada pelo autor, 2022

Figura 20: Transporte e Descarte



Fonte: Elaborada pelo autor, 2022

Com o intuito de alcançar o maior número de pessoas com a conscientização, foi realizado uma dinâmica com os recursos da rede social solicitando a interação dos seguidores da página no Instagram (Figura 21):

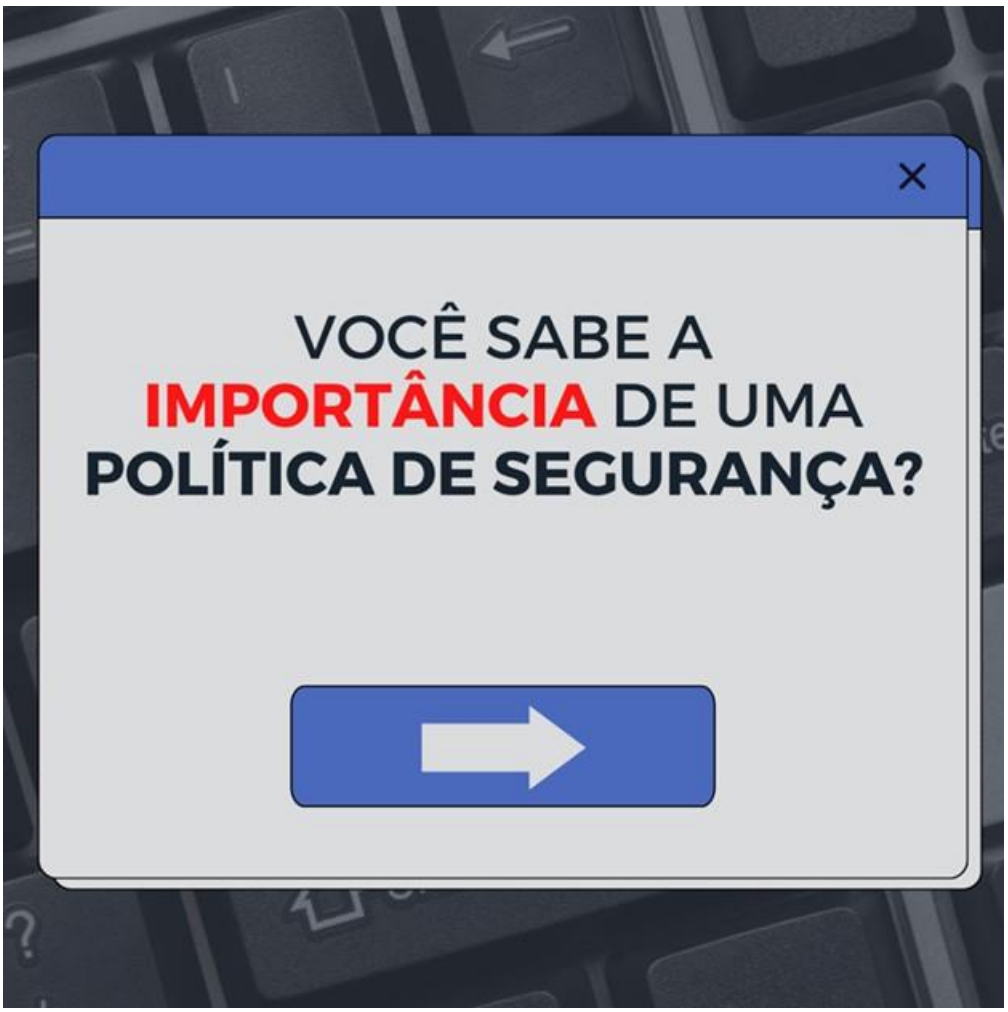
Figura 21: Auxílio para a divulgação

Fonte: Elaborada pelo autor, 2022

3.4.3. PLANO DE CONSCIENTIZAÇÃO: POLÍTICA DE SEGURANÇA

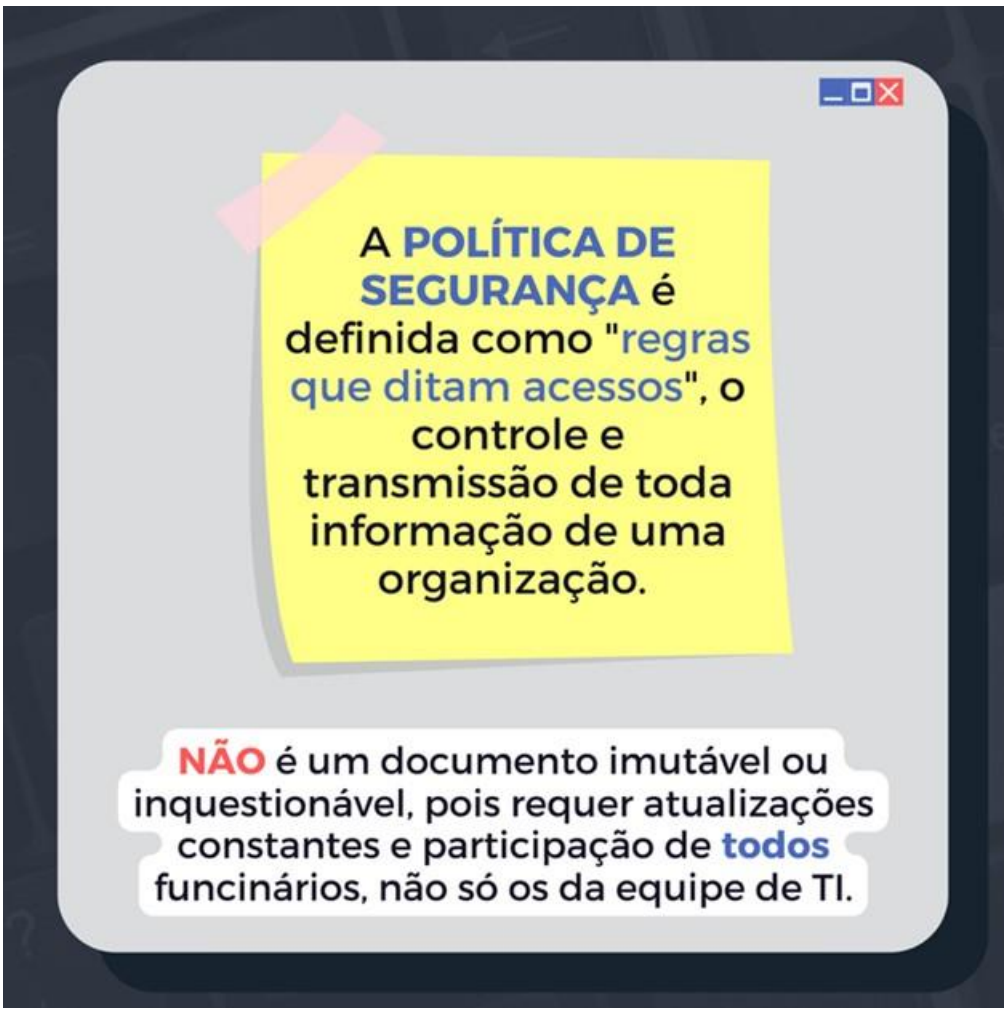
Pelo fato de que é necessário que haja uma série de procedimentos estabelecidos dentro de uma organização, foi apresentado (Figura 22 e 23) a importância de se ter uma Política de Segurança em uma organização, bem como a sua estrutura e orientações.

Figura 22: Você sabe a importância de uma Política de e Segurança?



Fonte: Elaborada pelo autor, 2022

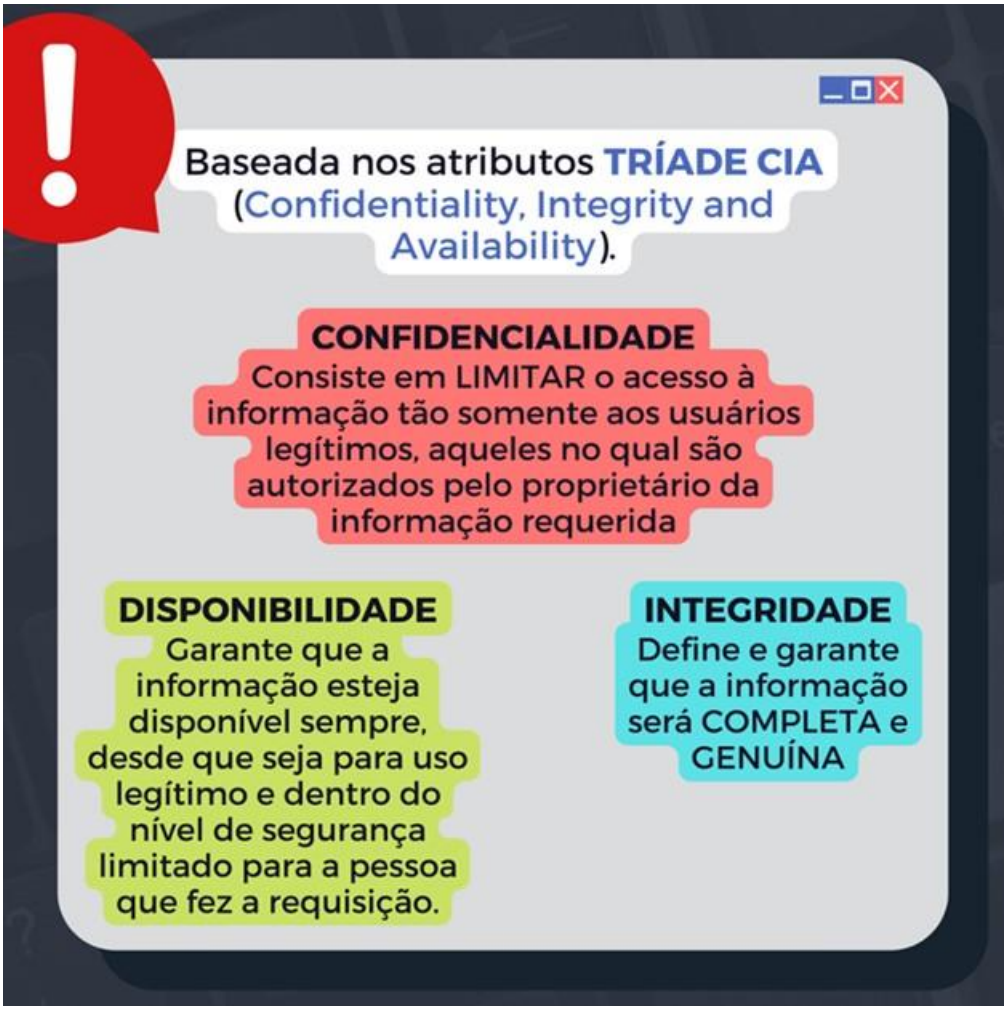
Figura 23: Definição da Política de Segurança



Fonte: Elaborada pelo autor, 2022

Não é possível retratarmos Política de Segurança sem a sua base na Tríade CIA (Confidencialidade, Integridade e Disponibilidade), consistindo em retratar o que cada um define, consiste e garante no processo (Figura 24), seja de implementação ou já na ação da política.

Figura 24: Confidencialidade, Integridade e Disponibilidade



Fonte: Elaborada pelo autor, 2022

O foco da Política de Segurança é reduzir as vulnerabilidades e proteger os dados da organização, desta forma, foi apresentado esta importância aos leitores (Figura 25).

Figura 25: Importância sobre uma Política de Segurança

Fonte: Elaborada pelo autor, 2022

Com o intuito de alcançar o maior número de pessoas com a conscientização, foi realizado uma dinâmica com os recursos da rede social solicitando a interação dos seguidores da página no Instagram (Figura 26):

Figura 26: Auxílio para divulgação

Fonte: Elaborada pelo autor, 2022

3.4.4. CARTILHA INFORMATIVA

A cartilha informativa foi realizada com intuito de reunir todos os tópicos principais pesquisados durante o projeto de pesquisa no momento do levantamento bibliográfico.

O conteúdo foi visado explanar sobre toda a fundamentação teórica e aplicar-se de modo dinâmico e intuitivo para o leitor, com o intuito de engajar a aproximação gerada por uma curiosidade temporária, trazendo assim conscientização e conhecimento sobre os assuntos em tópicos.

Figura 27: Capa - Cartilha informativa

Fonte: Elaborada pelo autor, 2022

O objetivo do conteúdo inicial da cartilha foi trazer o leitor para o conhecimento sobre o que é a Segurança da Informação e os subtópicos principal que a constituem, como a Tríade CIA, Política de Segurança e o Fator Humano por trás de uma organização no meio de sua segurança tecnológica (Figura 28):

Figura 28: Segurança da Informação, Tríade CIA, Política de Segurança e o Fator Humano

Fonte: Elaborada pelo autor, 2022

O conteúdo da segunda página foi um pouco mais denso, trazendo informações sobre o tópico principal do projeto de pesquisa, o modelo Zero Trust e o Sistema de Gestão da Segurança da Informação (SGSI). Juntos, trazem o embasamento e a aplicação (Figura 29):

Figura 29: Zero Trust e Sistema de Gestão da Segurança da Informação (SGSI)

Fonte: Elaborada pelo autor, 2022

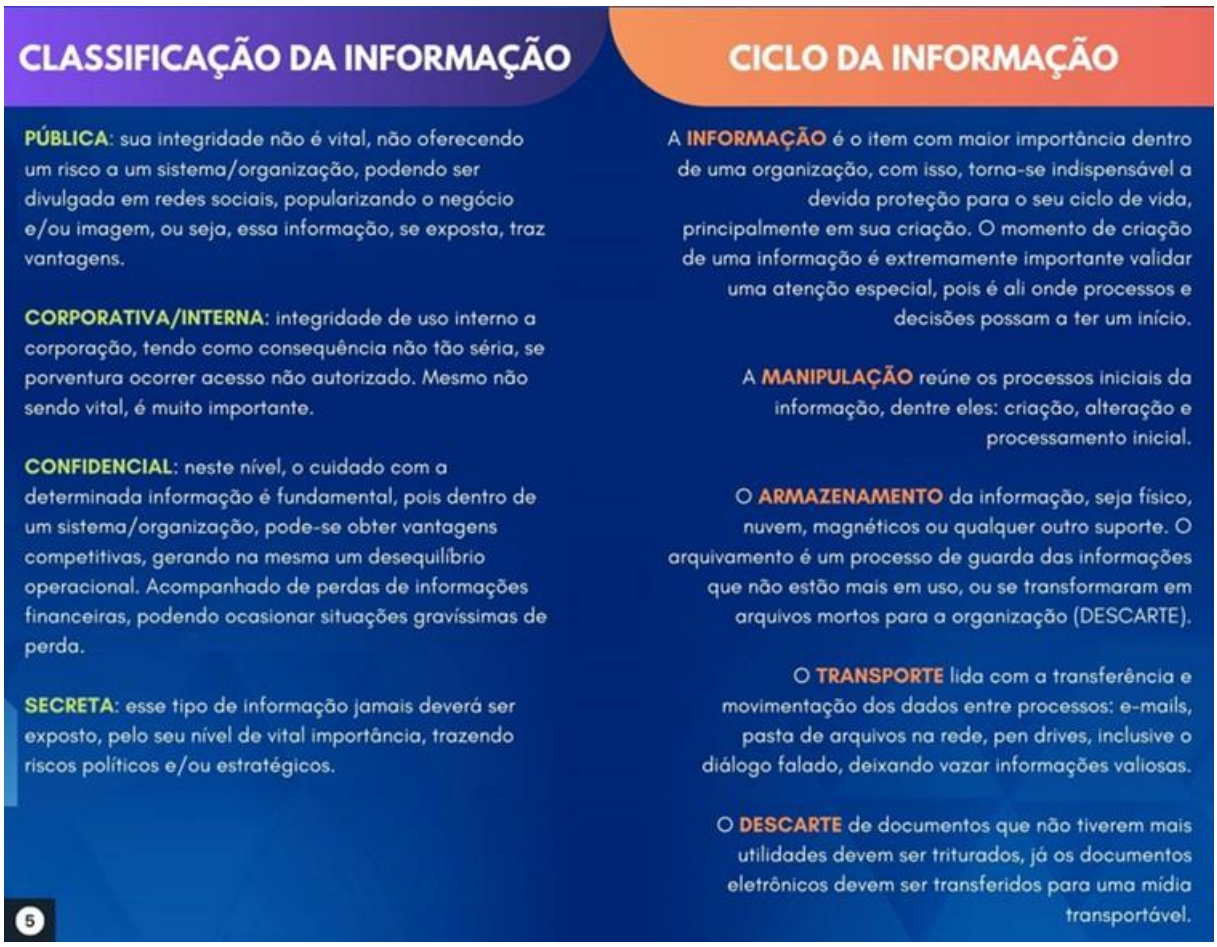
A necessidade de explanar sobre um modelo de execução se faz de importante necessidade ser incluída nesta parte do projeto. O Modelo PDCA, por mais que deixou de ser exigido na ISO 27001:2013, se faz de suma importância para uma organização no qual ainda não há um ciclo de gestão, auxiliando assim novos leitores na área (Figura 30):

Figura 30: Modelo PDCA

Fonte: Elaborada pelo autor, 2022

Um dos pontos mais importantes desta presente cartilha é a explicação sobre todo o ciclo e classificação da informação. Há grande necessidade o leitor se conscientizar do que tem em mãos e o processo no qual se encontra (Figura 31):

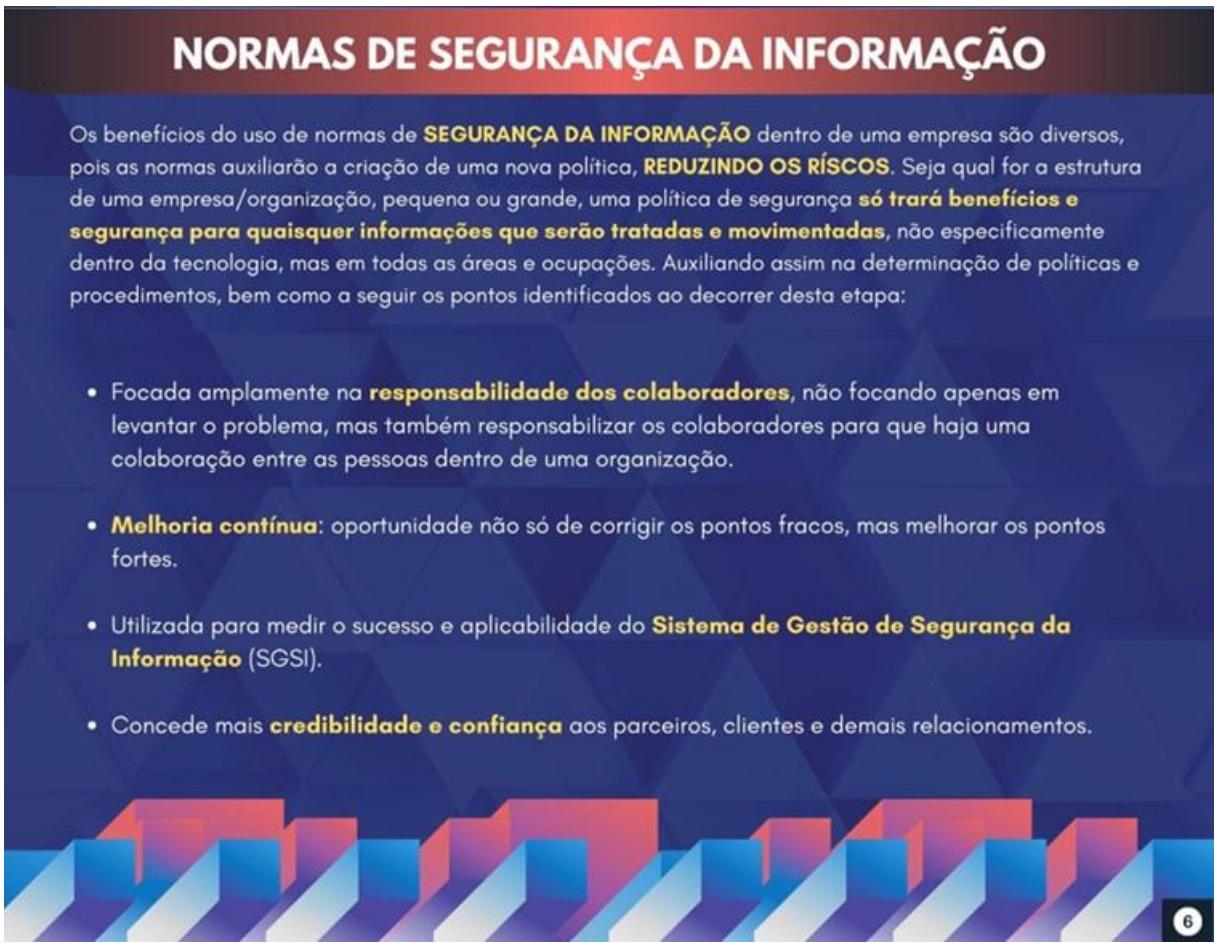
Figura 31: Classificação e Ciclo da Informação



Fonte: Elaborada pelo autor, 2022

O último tópico, e não menos importante, foi relacionado as Normas de Segurança da Informação, ou melhor, a base de todo conteúdo pesquisado e aplicado neste projeto de pesquisa (Figura 32):

Figura 32: Normas de Segurança da Informação



Fonte: Elaborada pelo autor, 2022

A divulgação e postagem da cartilha foi realizada no próprio Instagram, com o intuito de uma divulgação ampla, também foi feito uma arte para a realização (Figura 33, 34 e 35):

Figura 33: Link na bio do Instagram

Fonte: Elaborada pelo autor, 2022

Figura 34: Postagem da Cartilha Informativa

Fonte: Elaborada pelo autor, 2022

Figura 35: Divulgação da Cartilha Informativa

Fonte: Elaborada pelo autor, 2022

4. DISCUSSÃO DOS RESULTADOS

O presente projeto de pesquisa teve como objetivo, inicialmente, a coleta de dados em pesquisas bibliográficas sobre o modelo e arquitetura Zero Trust, Segurança da Informação, Política de Segurança, tomando a maior parte de construção do projeto até os resultados. Além de todo o levantamento bibliográfico utilizado, os materiais e métodos empregados para a elaboração do relatório final, os resultados alcançados, as discussões e considerações sobre as técnicas estudadas e testadas, as referências utilizadas e todos os demais anexos indispensáveis para a reprodução e continuação desta pesquisa.

Durante a coleta de dados foi notável a ausência de materiais sobre o Zero Trust em específico, sendo possível encontrar o básico sobre o que se refere, porém, o mais denso apenas em *blueprints* e *e-books*.

Em síntese, a coleta de feedbacks das divulgações através de comentários dos posts, via direct e WhattsApp foram positivos. O objetivo de alcançar pessoas onde a maior parte não havia informação sobre o Zero Trust e não tinham obtido uma conscientização, seja no meio organizacional onde poucas organizações fiscalizam de forma rigorosa todos os processos de um usuário, ou até mesmo pessoal, sobre uma Política de Segurança e os cuidados a serem tomados, tendo a necessidade de extrema de adotar um modelo de Segurança.

4.1. APLICAÇÃO DA ARQUITETURA ZERO TRUST

Utilizado no Cisco Zero Trust, Steve Martino (2020) diz que a segurança está mudando constantemente, e à medida que a tecnologia avança, é necessário um capacitador fundamental para permitir ter a confiança zero.

Com esta aplicação, é notável, juntamente com os dados encontrados durante o levantamento bibliográfico, explicando as vantagens que a aplicação do Zero Trust trará, caso utilizada. Tendo ciência de que os softwares podem ser diversos, não há um único para realizar determinada funcionalidade e soluções, como:

- Acesso seguro à rede;
- Segmentação de rede;
- Análise de tráfego criptografada;
- Visibilidade dinâmica;
- Contenção automatizada de ameaças;
- Aplicação da política;

5. CONSIDERAÇÕES FINAIS

Atualmente, é cada vez mais frequente as organizações sofrerem ataques (seja interno ou externo) no campo da informação que deveria estar protegida de uma

maneira mais rigorosa, por trás de uma política de segurança adotada e um modelo a ser seguido. Por isso, neste projeto de pesquisa, foi desenvolvido uma divulgação e conscientização através de recursos visuais criados no Canva e publicados na rede social do Instagram.

A nitidez e ciência que as pessoas que gerenciam uma organização possuem o dia a dia mais corrido, nada melhor de que lerem publicações rápidas para gerar um pensamento de proteção organizacional, e a cartilha informativa nos tempos oportunos.

No primeiro momento, foi realizado a pesquisa e levantamento bibliográfico em todo o campo da Segurança da Informação, com foco da aplicação do modelo e arquitetura Zero Trust baseado nas normas de Segurança da Informação nas organizações. Posteriormente, as publicações rápidas e a cartilha informativa no perfil do Instagram (@securityverse), com divulgação para contatos próximos através de envio de mensagens e verbalmente.

O resultado do projeto de pesquisa foi bastante positivo, conseguindo realizar a divulgação no círculo de pessoas mais próximas, consequentemente, atingindo as no qual gerenciam organizações. Tendo o *feedback* de alguns no qual não sabiam das informações repassadas, e por consequência, tiveram a curiosidade de pesquisar sobre o assunto referido.

Futuramente, é de pretensão do pesquisador continuar a conscientização sobre a proteção da informação, seja no meio organizacional ou individual, já que é algo presente de forma notável.

REFERÊNCIAS

Análise Comportamental: o que é e benefícios para a sua empresa. FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO. Disponível em: <https://fia.com.br/blog/analise-comportamental/>. Acesso em: 28 de mar. de 2021.

CANVA. Disponível em: <https://www.canva.com/>. Acesso em: 28 de mar. de 2021.

FONSECA, Paula F. Gestão de Segurança da Informação: O Fator Humano. 2009. 16 f. Monografia (Especialização)– Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009.

FRAGA, B. Técnicas de Invasão: aprenda as técnicas usadas por hackers em invasões reais. São Paulo: Editora Labrador, 2019.

GIL, A. C. Como Elaborar Projetos de Pesquisa. 5. Ed. São Paulo: Atlas, 2010.

GOLUBEV, S. Nunca confie, sempre verifique: O modelo de segurança Zero Trust. Kaspersky. Disponível em: <https://www.kaspersky.com.br/blog/zero-trust-security/15805/>. Acesso em: 28 ago. de 2021.

HINTZBERGEN, Jule. HINTZBERGEN, Kees. SMULDERS, André. BAARS, Hans. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 3. ed. Rio de Janeiro: BRASPORT, 2018.

INSTAGRAM. Disponível em: <https://instagram.com> Acesso em: 28 de mar. de 2021.

LAKATOS, E. M.; MARCONI, M. A. Metodologia do Trabalho Científico. 3ª ed. São Paulo: Atlas, 1992. 214 p.

LAUREANO, M. A. P.; MORAES, P. E. S. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia, Paraná, v. 8, n. 3, p. 38-44, jan./mar. 2005.

MAGELLA, Gustavo. Segurança da Informação [Guia Básico] [NBR ISO/IEC 27.002]. UDEMY. Disponível em: <https://www.udemy.com/course/seguranca-da-informacao-guia-basico-nbr-isoiec-27002/. Acesso em: 18 de fev. de 2022.

MITNICK, Kevin D.; SIMON, William L. A arte de enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MORAIS, Angélica. CESELLI, Paulo. SANTOS, Jessé. ELIAKIM, Carlos. Quais os componentes de uma estrutura organizacional para a segurança e controle? SISTEMAS DE INFORMAÇÃO. Disponível em: < https://sites.google.com/site/equipegbsiifce/home/fsi---fundamento-de-sistemas-informacao/FSI/quais-os-componentes-de-uma-estrutura-organizacional-para-segurana-e-controle>. Acesso em: 05 de mar. de 2022.

MORANDI, M. I. W. M.; CAMARGO, L. F. R. Revisão sistemática da literatura. In: DRESCH, A.; LACERDA, D. P.; ANTUNES JÚNIOR, J. A. V. Design Science Research: método de pesquisa para avanço da ciência e tecnologia. Porto Alegre: Bookman, 2015.

OLIVEIRA, S. Ciclo de vida da Informação – Gestão da Segurança da informação. 2011. Disponível em: <http://pt.scribd.com/doc/52566307/42/Ciclo-de-vida-da-informacao>. Acesso em 26 ago. de 2021.

PDCA: a prática levando sua gestão à perfeição. ENDEAVOR. Disponível em: <https://endeavor.org.br/estrategia-e-gestao/pdca/>. Acesso em: 27 de fev. de 2022.

PEIXOTO, Mário C. P. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006.

PEIXOTO, Mário C. P. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport, 2006.

REZENDE, D. A.; ABREU, A. F. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. São Paulo: Atlas, 2000.

SEGURANÇA DA INFORMAÇÃO VS. ENGENHARIA SOCIAL – COMO SE PROTEGER PARA NÃO SER MAIS UMA VÍTIMA. Monografias Brasil Escola. Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/seguranca-informacao-vs-engenharia-social-como-se-proteger.htm#>. Acesso em: 26 mar. de 2021.

Tudo sobre Instagram – História e Notícias. CANAL TECH. Disponível em: <https://canaltech.com.br/empresa/instagram/>. Acesso em: 28 de mar. de 2021.

Zero Trust Model: Garanta mais segurança ao ambiente de TI. SEC4U. Disponível em: <https://www.sec4u.com.br/blog-zero-trust-model>. Acesso em: 27 fev. de 2022.

Zero Trust Security. Akamai. Disponível em: <https://www.akamai.com/pt/resources/zero-trust-security-model>. Acesso em: 05 set. de 2021.