REVISTA SCIENTIA ALPHA
REVISTA CIENTÍFICA MULTIDISCIPLINAR DA FACULDADE ALFA UMUARAMA
>> REVISTA.ALFAUMUARAMA.EDU.BR
FACULDADE ALFA

USUÁRIO, O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Fabio Benedito de Souza[1]

[1] – Especialista em Segurança da Informação pelo CENES, Especialista em Docência do Ensino Superior pela UNIPAR. MBA em Executivo em Estratégias Empresarial pela UNIVEL. Graduado em Sistemas de Informação pela UNIPAR. – e-mail: fabio@fabiobenedito.com

RESUMO

Atualmente a tecnologia alterou e vem alterando a forma de administração nas organizações, com esta evolução da tecnologia na economia mundial as empresas passaram a dar valor e importância à informação, sendo considerada hoje como um dos principais bens da organização. Com o uso da internet, tornou-se um desafio filtrar e garantir a segurança de todas essas informações. Apesar do aumento das preocupações das organizações com a Segurança da Informação, vemos que somente os investimentos em mecanismos para o controle de informações isoladamente, podem não ser eficazes. É necessário um conjunto, em camadas, que deve ser implementados, como Firewalls, Antivírus, níveis e restrições de acesso a sistemas e arquivos, AntiSpam, backups, além de um Programa de Segurança da Informação, capaz de instruir e conscientizar toda a equipe de colaboradores da organização sobre a importância das informações, sua manipulação e do papel de cada um com a Segurança da Informação. Pois muitas vezes o papel do usuário na Segurança da Informação é negligenciando. O presente artigo fez uso de estudos bibliográficos para analisar os elementos que afetam a Segurança da Informação nas organizações brasileiras, para demostrar a importância da disseminação do assunto entre todos e a elaboração de Políticas Internas de Segurança da Informação, que demonstrem a conduta esperada pela Organização em relação aos cuidados com a informação e às medidas mais adequadas para sua proteção, também, as consequências e punições quando da falta de uso das medidas recomendadas.

Palavras-chave: Segurança da Informação; Usuários; Política de Segurança; Tecnologia da Informação; usuário.

1 INTRODUÇÃO

Neste artigo através de pesquisas bibliográficas, vamos abordar a Segurança da Informação junto com a Tecnologia da Informação, com o objetivo de avaliar estes riscos e trazer conhecimentos a respeito da segurança dos dados relativos ao fator humano.

Com o aumento crescente das Tecnologias de Informação e a sua disseminação vertiginosa, também cresceram os crimes relacionados com elas, assim surgindo, a necessidade de se manterem as informações empresariais e pessoais livres de vulnerabilidades e perigos, nas quais possam danificá-las ou compromete-las de alguma forma, como a sua exposição ou perca, e assim como a sua própria confiabilidade e a integridade.

As organizações estão cada vez mais expostas as ameaças que surgem, realizam investimentos em segurança física (controles de acesso, filmagem e alarmes, sistemas de

combate a incêndio), e a segurança lógica (como antivírus, AntiSpam e firewalls) para dificultar acessos não autorizados aos ambientes e sistemas.

Contudo, se seus principais manipuladores, que podemos denominar como usuários, devem estar capacitados, treinados e conscientizados sobre seu papel no processo de proteção das informações da organização, senão todos os investimentos em sistemas e proteções não serão justificados. [SÊMOLA, 2014]

> 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, 2003)

O fator humano ainda é o responsável pela grande parte dos vazamentos e percas das informações, seja por descontentamento dos usuários com a organização, falta de conhecimento e por técnicas de Engenharia Social.[MITNICK, 2003]

Com isso se torna uma necessidade a implantação de Políticas de Segurança, para minimizar essas exposições das organizações, desta forma as organizações adotam normas e procedimentos claros que sejam constantemente atualizados e disseminadas a todos os seus usuários através de programas e treinamentos e de conscientização.

Assim este artigo tem por finalidade apresentar os conceitos, princípios e finalidades da Gestão da Segurança da Informação, na qual está diretamente ligada com a proteção de dados, a final a informação é um fator importante em nosso dia-a-dia, pois estamos atualmente imersos nela e a todos os instantes recebemos uma avalanche de dados e informações.

2 A INFORMAÇÃO

A informação é tida hoje como um dos maiores e mais importantes patrimônios de uma organização. Com o surgimento das organizações “pontocom”, (em inglês dot.com), que baseavam todo o seu modelo de negócios em número de acessos, visibilidade ou mesmo na criação de comunidades virtuais, e quase não tendo ativos tangíveis e ainda assim valendo bilhões de dólares.

Para entender melhor o que é dados e informação temos que fazer algumas definições, mesmo lidando com todos esses conceitos diariamente. [KOTLER; KELLER, 2006]

Dados, são códigos que constituem a matéria prima da informação, ou seja, é a informação não tratada, de forma “bruta”. Os dados representam um ou mais significados que isoladamente não fazem sentido, e não podem transmitir uma mensagem ou representar algum conhecimento.

Exemplo: 20.

Informações, são dados tratados, é o resultado do processamento de dados em informações. As informações têm significado, e que podem ser tomadas decisões ou fazer afirmações considerando estas informações.

Exemplo: 20° C de temperatura.

Conhecimento, vai além de informações, pois ele além de ter um significado tem uma aplicação. As informações são valiosas, mas o conhecimento constitui um saber. Produz ideias e experiências que as informações por si só não será capaz de mostrar. Se informação é dado trabalhado, então conhecimento e informação trabalhada.

Exemplo: a Câmara fria está 20° C de temperatura.

E é por meio do conhecimento é que podemos saber onde colocar esforços ou diminui-los conforme necessidades, as decisões de uma organização se baseiam em informações, portanto ela tem que ser precisas, tendo uma importância e um valor. [SILVA, 2021]

> A informação são valiosas na compreensão dos sistemas, mas o conhecimento constitui um estágio superior. O conhecimento é capaz de contribuir na produção de novas ideias, por outro lado a informação por si só não é suficiente para ampliar o saber o humano. Portanto o conhecimento exige do sujeito cognoscitivo a capacidade de identificar o que é importante e assim gerar o saber. Se informação é dado trabalhado, então conhecimento e informação trabalhada. (SILVA, 2021)

3 SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação é basicamente a preservação da confidencialidade, integridade, disponibilidade, autenticidade e o não repudio de todas informações e dados que são indispensáveis para uma organização ou para um indivíduo.

Essa preservação passa por um ambiente físico, logico e de gestão de pessoas, e é uma área de extremo interesse dentro das organizações que realmente se importam com a qualidade e continuidade dos seus negócios.

Segundo SÊMOLA, 2014 “Podemos definir segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados,

alterações indevidas ou sua indisponibilidade.”.

Esta área tem um grande desafio, que é a conscientização dos colaboradores e usuários, sobre a importância da Segurança da Informação, para garantir conforme escrito no início, sua confidencialidade, integridade, disponibilidade e autenticidade das informações da organização. [SÊMOLA, 2014]

A Segurança da Informação pode trazer para a empresa benefícios, como a continuidade ao seu negócio.

E caso não seja usada de forma correta, a organização pode ter prejuízos, dependendo no nível de seriedade do problema, pode ficar dias sem sistemas ou até mesmo perder todas as suas informações.

Lembrando que todos os usuários e colaboradores da empresa precisam estar cientes e de acordo com a importância das informações da empresa, para estar atendo e cuidar da segurança da organização.

4 O OBJETIVO DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação tem como objetivo a proteção dos dados e das informações de uma empresa ou pessoa de qualquer tipo de ameaça.

Os pilares da segurança da informação são a Confidencialidade, Integridade, Disponibilidade, Autenticidade, Não Repudio, estes cinco pilares sustentam a estrutura das soluções, metodologias e ferramentas colocadas em prática para garantir a segurança e a proteção da informação, para evitar a perdas, sequestros e violações dos dados em diferentes tipos de cenários.

Vamos ver cada um dos Pilares da Segurança da Informação:

- **Confidencialidade**

É assegurar a proteção da informação contra o acesso não autorizado, fazendo um controle de acesso rigoroso, ter o conteúdo protegido por autenticação por senha e garantir que apenas pessoas autorizadas consigam acessar os dados.

Muitas organizações aplicam políticas que contribuem com o princípio da confidencialidade, como somete permitir que funcionários de cargos mais elevados tenham mais acessos, restringindo a informação conforme a hierarquia de cada colaborador e limitar o acesso a dados

conforme as necessidades de cada setor.

Implementar sistemas de verificação biométrica e criptografia também é um exemplo de medida de infraestrutura que promove bons resultados. [COMO, 2021]

- **Integridade**

É assegurar que os dados mantenham suas características originais, tais como foram salvas pelo seu criador, ficando assim protegida contra a alterações não autorizadas.

As informações devem estar sempre exatas e completas quando acessadas, caso contrário, quando um dado é alterado indevidamente, podemos dizer que existe perda da integridade e isso pode gerar grandes prejuízos. [COMO, 2021]

- **Disponibilidade**

É assegurar que as informações estejam à disposição do usuários e colaboradores para consulta no momento que for necessário, neste caso tem a ver com a sua acessibilidade. Neste pilar tem a ver com o funcionamento adequado da rede, dos servidores, sistemas de armazenamento e da eficácia dos sistemas, garantindo que a informação possa ser acessada quando for necessário.

Também deve contar com um plano de recuperação de desastres e uma política de backup eficiente, pois ela será essencial caso haja problemas com a integridade dos softwares e dos hardwares. [COMO, 2021]

- **Autenticidade**

É assegurar a legitimidade dos proprietários da informação, garantindo que os dados são de fato procedentes de uma determinada origem, assegurando que foram criados, expedidos, alterados por alguém ou por um sistema, e isso garante a verdadeira autoria e alteração da informação.

- **Não repúdio**

Também chamada de Irretratabilidade, visa assegurar a veracidade e a legitimidade do autor da informação, para que um indivíduo ou entidade não negue a autoria de uma ação específica como, ao se enviar uma mensagem o emissor ou o receptor não pode dizer que não enviou ou que não recebeu tal mensagem.

Isso visa proteger as partes de uma provável desistência de um negócio, de assinaturas de contratos digitais e até mesmo de e-mails, para que depois não venham alegar que não realizou tal procedimento. [SILVA, 2003]

4.1 A SEGURANÇA FISICA

Tem como objetivo de restringir acessos de pessoas não autorizadas aos ambientes que contenham os servidores e sistemas de armazenamento de dados.

Um Data Center ou como eram chamados antigamente de CPD (Centro de Processamento de Dados), é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de ativos de rede, como switches, roteadores entre outros, é considerado o sistema nervoso das empresas, uns dos itens determinantes da segurança física é com relação à localização, o Data Center deve ser construído em um local que não haja risco de desabamento, inundações, excesso de calor, poeira e umidade, que não tenha risco de serem danificados em caso de vandalismo e depredação. [COMO, 2021]

O acesso ao Data Center deve ser feito somente por pessoas com autorização, restringindo assim a entrada de quaisquer outras pessoas, o acesso e permanência de pessoas que não sejam funcionários do Data Center devem ser registrados e feitos somente com acompanhamento de algum funcionário do setor.

O controle pode ser feito por auxílio de ferramentas de controle de acesso como: crachás, senhas, trancas, biometrias, câmeras de vídeo e cartões magnéticos. Ter atenção com as portas e trancas de acesso é sempre necessário, mais também deve ter cuidado com as janelas, pode ser usado filmes de proteção, cortinas e grades, para evitar problemas com a luz do Sol, “olhares curiosos” e invasões. [COMO, 2021]

Muitas empresas possuem um segundo Data Center, que é um reserva ou secundário, que no qual são replicadas as informações neste, se caso seu o Data Center principal venha a falhar por qualquer motivo, como problemas elétricos, alagamento ou incêndio, o Data Center reserva pode assumir para que aja a continuidade do negócio.

Podem também ter sala de backup separada do Data Center principal, que no caso de um incêndio ou outro problema, pode ao menos garantir que os backups estão seguros. Também pode usar sistemas de replicação e de backup em Cloud dependendo da empresa.

4.2 SEGURANÇA LÓGICA

Já esse tipo de segurança, é a forma como os sistemas são protegidos, sejam por softwares ou regras de restrições de acesso, também significa proteção de sistemas contra erros não

intencionais, como remoção acidental de arquivos de sistema ou aplicação.

Em geral são utilizadas várias tipos e camadas de software para tentar garantir a proteção, assim desta forma podem ser utilizados firewalls, LDAP, backup, antivírus, anti-spam, etc. [KLETTENBERG, 2016]

As principais ameaças nesta área estão ligadas aos acessos indevidos, erros provocados, falhas na rede provocadas por softwares estranhos, fraudes e sabotagens, que pode comprometer o funcionamento e a disponibilidades dos sistemas e arquivos.

Há a necessidade de se fazer o controle de acesso assim como na segurança física. A diferença é que o controle de acesso lógico visa proteger dados e programas contra tentativas de acesso não autorizados. Seja o acesso feito por pessoas ou programas. [COMO, 2021]

O controle de acesso lógico procura garantir que:

- Somente pessoas autorizadas tenham acesso às informações e recursos;
- Que o acesso do usuário será feito somente a recursos que ele tenha permissão;
- O acesso a recursos mais importantes será feito apenas por pessoas autorizadas, sendo que os acessos são sempre monitorados.

Para ser feita a implantação dos controles de acesso lógico o usuário deve estar ciente de suas responsabilidades e obrigações com relação a manutenção de senhas e a segurança dos equipamentos de informática utilizados por ele. [COMO, 2021]

5 POLITICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança, são instruções claras, em linguagem natural, para não serem interpretadas de forma ambígua, que fornecem as orientações para os colaboradores e usuários de como se deve guardar, modificar, excluir e compartilhar as informações, sendo apresentadas como códigos de conduta, aos quais os usuários devem se adequar integralmente, sendo um componente fundamental no desenvolvimento de controles eficazes para conter as possíveis ameaças à segurança, sendo uma das melhores práticas no que diz respeito de evitar e detectar os ataques de Engenharia Social. [MARCIANO E LIMA-MARQUES, 2006]

A Política de Segurança que devem abranger de forma adequada as mais variadas áreas do contexto da organização, passando por recursos computacionais e de infraestrutura e de logística, além dos recursos humanos, deve também existir um equilíbrio nos aspectos humanos e técnicos da segurança da informação, pois em geral sempre é mais voltado as questões

tecnológicas e não para humanas. [MARCIANO E LIMA-MARQUES, 2006]

Vale ressaltar, que mesmo com uma Política de Segurança bem realizada, ajustada para empresa, segura, e rigorosamente seguida por todos os usuários, não evita todos os ataques de Engenharia Social, lembrando que também nada é 100% seguro, e a Política de Segurança tem como objetivo de minimizar os riscos até um nível aceitável. [PEIXOTO, 2006]

Um estudo sobre a segurança da informação deve começar com uma avaliação de risco que visa determinar alguns pontos, que tem como objetivo primário a priorização das informações que precisam de proteção imediata, e se essa proteção será eficaz em termos de custo, com base em uma análise do custo/benefício.

> A proteção para os ataques envolve o treinamento nas políticas e procedimentos, mas também – e provavelmente mais importante – um programa constante de conscientização. Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização. (MITNICK, 2003)

Para que seja bem-sucedido é essencial que os níveis mais altos da gerencia da empresa, realmente adotem e apoiem com firmeza o desenvolvimento destas Políticas de Segurança, assim os usuários e colaboradores de níveis mais baixos terão consciência de que verdadeiramente essencial e importante para a operação da empresa, e somente assim terá sucesso na implementação e manutenção da Políticas de Segurança.

É importante que o documento com as Políticas de Segurança seja claro, que não tenha sentidos ambíguos, e também informar a importância e o sentido de cada política, caso contrário os usuários podem encará-las como perda de tempo e não as cumprir. Os usuários devem ser avisados sobre as consequências do não-cumprimento das políticas e dos procedimentos de segurança, e divulgar as consequências das violações das políticas em toda empresa.

Também pode ser implementando um programa de recompensa, para que os usuários que reconhecem e/ou relatem um incidente de segurança, assim sempre que um colaborador frustrar uma quebra de segurança deve ser recompensado, isso também pode ser divulgado em toda a empresa, como um exemplo de que as Políticas de Segurança estão funcionando.

É da responsabilidade da gerencia da empresa essa conscientização sobre a Segurança da Informação é a comunicação da importância das Políticas de Segurança assim como os danos que podem ocorrer se estas regras não forem seguidas. As Políticas de Segurança das informações não podem ser inflexíveis, elas devem ser alteradas à medida que surgem novas tecnologias e novas vulnerabilidades, com um processo regular de revisão e atualização.

As Políticas de Segurança variam de organização para organização, devem ser analisadas

e estudadas quais políticas são apropriadas com base no ambiente e nos objetivos de negócios de cada organização, cada organização tem os seus requisitos de segurança, baseados nas suas necessidades, nos requisitos legais, na cultura organizacional e nos sistemas de informações utilizados.

6 SEGURANÇA DA INFORMAÇÃO DO PONTO DE VISTA HUMANO

A preservação da confidencialidade e da segurança das informações da empresa é de responsabilidade de todos os usuários e colaboradores, e que infelizmente na sua grande maioria, não estão ou que não foram preparados para lidar e reconhecer as diversas situações de riscos.

No ponto de vista humano a Engenharia Social é um dos maiores problemas da Segurança da Informação, pois através dela o engenheiro social pode utilizar diversos métodos para obter acesso as informações confidenciais das empresas.

Os colaboradores devem ser treinados e conscientizados sobre a importância da Segurança da Informação e do seu papel na empresa, da área da Segurança da Informação e de como proteger essas informações, assim serão capazes a identificar situações de riscos e minimizar problemas.

Outro exemplo importante é de um colaborador insatisfeito, ele pode propositalmente clicar em links, e-mails e sites não confiáveis, somente para ver se causa algum prejuízo, também pode revelar segredos, estratégias e informações da empresa e com isso causar impactos financeiras e/ou na imagem da empresa.

Assim devesse criar e disseminar essas informações nas organizações, as organizações devem criar e divulgar as Políticas de Segurança, suas Normas e Procedimentos de Segurança da Informação através de treinamentos e conscientizações constantes.

7 ENGENHARIA SOCIAL

São técnicas empregadas por criminosos virtuais para induzir usuários para revelar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados, explorando a boa vontade e a falta de conhecimento do usuário. [MARCIANO E LIMA-MARQUES, 2006]

> Engenharia social usa a influência e a persuasão para enganar as pessoas e convence-las de que o engenheiro social é alguém que ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia. (MITNICK, 2003)

O engenheiro social evita a criptografia, segurança de computador, a segurança de rede, o antivírus e o firewall, e tudo o mais que for tecnológico. Ele vai diretamente para o elo mais fraco de qualquer sistema de segurança, o usuário.

Infelizmente muitos usuários e colaboradores não percebem o verdadeiro valor dos dados pessoais e comerciais, não sabendo exatamente como proteger essas informações. [PEIXOTO, 2006]

Praticamente todo tipo de ataque contém algum método de engenharia social, desde o clássico e-mail de "phishing" e os golpes com vírus, por exemplo, são repletos de insinuações de conotação social. [ENGENHARIA, 2021]

> Engenharia social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de engenharia social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). (PEIXOTO, 2006)

Os e-mails de phishing tentam convencer os usuários de que são, de fato, de fontes legítimas, na esperança de conseguir obter qualquer dado pessoal ou corporativos, por menor que seja. Os e-mails que contêm anexos cheios de vírus, por sua vez, muitas vezes alegam ser de contatos confiáveis ou oferecem conteúdo de mídia que parece inofensivo, como currículos, propostas comercias ou coisas divertidas. [ENGENHARIA, 2021]

Um Hacker também pode usar métodos mais simples de engenharia social para conseguir acessar a rede ou o computador, um exemplo seria, que um hacker pode frequentar a praça de alimentação de um edifício corporativo e bisbilhotar os usuários que trabalham com tablets ou laptops. Assim, pode conseguir um grande número de senhas e nomes de usuários, sem enviar sequer um e-mail ou escrever uma linha de código de vírus. [ENGENHARIA, 2021]

Outros ataques dependem da comunicação real entre invasores e vítimas. Nesse caso, o invasor pressiona o usuário a conceder acesso à rede com a alegação de um problema sério que requer ação imediata. Pôde-se usada emoções com raiva, culpa e tristeza, para tentar convencer de alguma forma os usuários de que sua ajuda é necessária e que eles não podem recusar. [MARCIANO E LIMA-MARQUES, 2006]

A proteção contra a engenharia social começa com capacitação e treinamento. Os usuários devem ser condicionados a nunca clicar em links suspeitos e a sempre proteger suas credenciais de login, seja em casa ou no trabalho. Se as táticas sociais derem certo, no entanto, o resultado

provável será uma infecção por malware ou um vazamento de informações. [ENGENHARIA, 2021]

8. RESULTADOS

Para conseguir minimizar os riscos de vazamento e perda das informações, as quais podem acarretar prejuízos, seja na imagem da instituição, ao seu patrimônio ou financeiramente, as organizações devem criar procedimentos claros para todos os processos onde essas informações possam circular. [SÊMOLA, 2014]

É necessário implementar medidas de treinamento e conscientização constantes dos seus colaboradores quando a Segurança da Informação.

Existem vários riscos, um seria o acesso indevido aos ambientes da empresa, assim as organizações devem adotar procedimentos que permitam a seus usuários reconhecer se uma determinada pessoa é realmente quem diz ser, senão, pessoas mal-intencionadas podem obter, através técnicas de Engenharia Social, acesso aos ambientes da organização, roubando informação e causando danos.

Outro risco é o fornecimento de usuário e senha de acesso aos sistemas da organização, através de um e-mail de phishing ou um simples telefonema, usando de Engenharia Social pode obter informações com o usuário e a senha de um colaborador, que o permitirá ter acesso aos sistemas internos na organização sem maiores problemas.

Existe também o risco do descarte físico das informações, as organizações devem adotar procedimentos de descarte das informações físicas, através de meios seguros como por exemplo, fragmentadoras ou queima em caldeiras, pois informações importantes relativas ao negócio da empresa, como projetos, clientes, fornecedores, contratos, e outros tipos de informação não podem ser encontradas facilmente no lixo por pessoas que pretendem de alguma forma utilizá-las para benefício próprio. [KLETTENBERG, 2016]

Para que estes tipos de acontecimentos não surjam, os usuários e colaboradores devem ser treinados e conscientizados sobre quais são as informações ele pode passar ou não, assim como o acesso de pessoas e o descarte de informações.

Desta forma, é necessário criar e acompanhar as Políticas de Segurança da Informação, criando e divulgando estas normas de procedimentos que digam ao usuário qual é a postura que

deve ser tomada de forma simples, diante dos diferentes tipos de situação que possam ser encontradas.

9. CONSIDERAÇÕES FINAIS

O trabalhado demostra que as organizações podem realizam grandes investimentos em tecnologias para proteção dos seus ambientes e sistemas de informações contra acessos não-autorizados, porém, de nada adiantará se o elo mais fraco da segurança da informação for negligenciado, o usuário.

Para isso precisamos compreender o que é Informação, qual o seu valor, quais são as informações necessárias ou prioritárias para a organização proteger, assim como os conceitos da Segurança da Informação e os seus objetivos, igualmente permanece necessário todos estarem cientes tanto da segurança física quanto da segurança lógica.

Com todas estas definições é necessário montar uma Política de Segurança da Informação que deve fornecer as orientações para os colaboradores e usuários de como se deve guardar, modificar, excluir e compartilhar as informações, assim como um manual de conduta, constituindo um componente fundamental no desenvolvimento de controles eficazes para conter as possíveis ameaças à segurança, como os seus procedimentos e responsabilidades da guarda e divulgações das informações, assim como também as penalidades caso o descumprimento das mesmas.

Mesmo entendendo todos estes fatores, existe ainda o ponto de vista humano na Segurança da informação, que pode ser burlado com simples ataque de Engenharia Social. Portanto a Engenharia Social pode ser utilizada com grande sucesso, atuando para ter acesso aos os sistemas e arquivos das organizações e de usuários despreparados.

Desta forma para evitar ou diminuir os acessos não autorizados e o vazamento de dados, através da Engenharia Social é necessária criação das Políticas de Segurança, difundir e fazer cumprir, para que seus colaboradores e usuários tenham uma noção sobre o que é Segurança da Informação, quais informações são confidenciais, o que podem fazer e a quem recorrerem em caso de dúvida sobre os riscos presentes em determinadas situações.tendência pedagógica do "aprender a aprender" voltada à construção do conhecimento visa formar indivíduos mais autonômos no processo de aprendizagem, isso somado ao avanço da tecnologia no século XXI e o crescimento da educação a distância, é onde surge então a metodologia híbrida para aprendizagem, que combina as modalidades de ensino presencial e a distância.

No Brasil a metodologia híbrida vem sendo colocada em prática em especial no ensino superior e em cursos que são ofertados via modalidade a distância, dessa forma a universidade que oferta este tipo de curso, oferece mais momentos presenciais, além dos avaliativos e obrigatórios.

Diante dessa contextualização, a questão central da pesquisa que se coloca é: como o *Ba* promove a construção do conhecimento na metodologia de ensino híbrido no contexto da Educação Superior?

Para buscar responder o problema de pesquisa, esse estudo tem por objetivo geral: analisar a construção do conhecimento na metodologia de ensino híbrido no contexto da Educação Superior sob a perspectiva do *Ba*.

Para tanto, este trabalho está organizado da seguinte forma: além desta introdução, a fundamentação teórica, caracterizando o ensino híbrido, as teorias de criação do conhecimento sob a perspectiva do *Ba* e na seguinte seção a metodologia utilizada, em seguida o estudo de caso, resultados e discussões, e por fim, a conclusão.

REFERÊNCIAS

COMO fortalecer os 5 pilares da segurança da informação nas empresas, 2021, Disponível em: <https://www.gat.digital/blog/5-pilares-da-seguranca-da-informacao>. Acesso em: 30 mai. 2022.

ENGENHARIA social – Definição. 2021 Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering>. Acesso em: 16 jun. 2022.

KLETTENBERG, Josiane Klettenberg. **SEGURANÇA DA INFORMAÇÃO: Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias**. 2016. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/172575/343623.pdf?sequence=1&isAllowed=y>. Acesso em: 08 jul. 2022.

MARCIANO, João Luiz Marciano e LIMA-MARQUES, Mamede Lima-Marques. **O enfoque social da segurança da informação**. 2006. Disponível em: <https://www.scielo.br/j/ci/a/L8CqcznptmQK3jyqGqNpWMQ/?format=pdf&lang=pt> Acesso em: 08 jul. 2022.

MITNICK, Kevin D.; SIMON, William L. Mitnick: **A Arte de Enganar**. São Paulo: Pearson Makron Books, 2003.

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

SÊMOLA, M. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA VISÃO EXECUTIVA - 2 ed.** São Paulo: Elsevier, 2014.

SILVA, Lino Sarlo da Silva. **Mantendo em lugar seguro suas provas e contraprovas digitais**. 13 de Agosto de 2003. Disponível em: <http://www.dicas-l.com.br/dicas-l/20030813.php>. Acesso em: 30 mai. 2022.

SILVA, Heide Miranda da Silva. **SOCIEDADE DA INFORMAÇÃO**, Disponível: <http://www.profcordella.com.br/unisanta/textos/tgs21_dados_info_conhec.htm>. Acesso em: 26 maio 2022.

KOTLER, Philip; KELLER, Kevin Lane**. ADMINISTRAÇÃO DE MARKETING - 12 ed**. São Paulo: Pearson Education do Brasil, 2006.