Journal of Technology & Information

O Mito do Elo Mais Fraco: Fator Humano na Segurança da Informação

The Myth of The Weakest Link: Human Factor In Information Security

Recebido/*Received*: 09/04/2024 | Revisado/*Revised*: 27/04/2024 | Aceito/*Accepted*: 23/07/2024 | Publicado/*Publish*: 25/11/2024
https://www.doi.org/10.5281/zenodo.14215708

Ana Rita Akayama Kanagusku
Fatec Americana
https://orcid.org/0009-0000-8248-5109
rita.kanagusku@gmail.com

Edson Roberto Gaseta
Fatec Americana
https://orcid.org/0000-0003-0778-7937
edson.gaseta01@fatec.sp.gov.br

Resumo

O papel do fator humano na segurança da informação é indiscutível, e este estudo tem como objetivo investigar as razões que o tornaram o elo mais vulnerável, ao mesmo tempo em que propõe uma nova abordagem, focada na possibilidade de implementar medidas para desafiar essa percepção quase que universal. Embora a evolução da tecnologia tenha trazido inúmeras facilidades para o mundo contemporâneo, a privacidade dos dados nunca esteve tão ameaçada como nos dias atuais, onde os ataques cibernéticos se tornaram corriqueiros, muitos explorando potenciais falhas humanas. A superação desse estigma de elo mais fraco certamente passa pela conscientização e por treinamentos criteriosos, realizados de maneira contínua, com o intuito de promover uma cultura de valorização da informação. Nesse contexto, diante da complexidade das ameaças atuais, é necessário não apenas adotar medidas técnicas robustas, mas também cultivar uma mentalidade de segurança em todos os estratos da sociedade, desde o cidadão comum até as mais altas esferas corporativas. O método utilizado nesta pesquisa é dedutivo, fundamentado em extensa revisão bibliográfica e documental. Foi possível avaliar pelos dados analisados a necessidade da elaboração de planos de conscientização, além de processos e procedimentos, de forma que as partes interessadas internas de uma organização contribuam com o propósito de manter as informações seguras.

Palavras-chave: fator humano, privacidade, informação.

Journal of Technology & Information

Abstract

The importance of the human factor in information security is unquestionable, and this study aims to investigate the reasons that made it the most vulnerable link, while at the same time proposing a new approach, focused on the possibility of implementing measures to challenge this perception almost How universal. Although the evolution of technology has brought countless facilities to the contemporary world, data privacy has never been as threatened as it is today, where cyber attacks have become commonplace, many exploiting potential human errors. Overcoming this weakest link stigma certainly involves raising awareness and careful training, carried out on an ongoing basis, with the aim of promoting a culture of valuing information. In this context, given the complexity of current threats, it is necessary not only to adopt robust technical measures, but also to cultivate a security mentality in all strata of society, from ordinary citizens to the highest corporate spheres. The method used in this research is deductive, based on an extensive bibliographic and documentary review. It was possible to evaluate from the data analyzed the need to develop awareness plans, in addition to processes and procedures, so that an organization's internal stakeholders contribute to the purpose of keeping information secure.

Keywords: *human factor, privacy, information*.

1. Introdução

O século XXI marca uma era em que as informações estão se valorizando exponencialmente, o que traz como consequência o crescimento dos riscos de vazamentos dessas verdadeiras preciosidades. Segundo Fontes (2017), a informação seja qual for sua forma, representa um recurso valioso para a empresa. Em contrapartida, a cultura de valorização das informações não acompanha o mesmo ritmo, especialmente em empresas de pequeno e médio porte, ao contrário, caminha a passos lentos.

A proteção de dados é embasada em duas principais vertentes: questões tecnológicas e falhas humanas, conforme observado pelo ITforum (2022), a defesa contra "ameaças humanas" é abordada de forma holística, combinando soluções especializadas e medidas de gestão.

A Segurança da Informação é baseada em três pilares conhecidos pela sigla CID: Confidencialidade, Integridade e Disponibilidade, por definição, qualquer fator ou ação que possa causar danos a eles recebe a denominação de ameaça, e o fator humano se enquadra nessa categoria. Temos ainda a questão das vulnerabilidades em segurança da informação, segundo definição da norma ISO/IEC 27005:2022, a fraqueza de um ativo

ou controle que pode ser explorada para que um evento com consequências negativas ocorra.

E é nesse sentido que o fator humano frequentemente é citado como o elo mais fraco na gestão e atividades que envolvem segurança da informação, pela sua complexidade ao envolver emoções, questões comportamentais, cultura, entre outros. Ao passo que a tratativa para os fatores técnicos e físicos é mais objetiva, que apresentam soluções em forma de barreiras e ferramentas de defesa.

O objetivo do presente estudo é investigar o fator humano na segurança da informação, colocar em discussão o rótulo adquirido de "elo mais fraco" da proteção dos dados e os possíveis caminhos para sua redenção através de uma cultura de proteção de dados baseada em uma educação digital.

A palavra-chave para sedimentação de uma cultura de reconhecimento do valor das informações é a conscientização, um processo educativo que traga o real entendimento da relevância dos dados, o quão responsável é preciso ser na tratativa das informações, as implicações que um vazamento de dados pode trazer, especialmente em tempos de regulamentos como o vigente na União Europeia, General Data Protection Regulation (GDPR) e leis como a Lei Geral de Proteção de Dados (LGPD), no Brasil.

Esse processo necessita ser conduzido de forma contínua, estar em constante movimento e atualização, envolvendo treinamentos, palestras, informativos, estabelecimento de códigos de conduta, bem como implementação de ferramentas de proteção e controle de acesso aos dados.

2. Referencial Teórico

O termo "fator humano" data dos anos de 1950, quando Theodore W. Schultz, professor da Universidade de Chicago, desenvolveu a teoria do capital humano que o levaria a receber o prêmio Nobel de Economia, após cerca de uma década. (MINTO,

2021). Desde então, com o avanço tecnológico, o conceito evoluiu e aparece como item de destaque e importância nas organizações.

Segundo a agência de pesquisa do Reino Unido *Health and Safety Executive* (HSE, 2021), "os fatores humanos referem-se a questões ambientais, organizacionais e profissionais, características humanas e individuais que influenciam o comportamento no local de trabalho de uma forma que pode afetar a saúde e a segurança".

Este conceito traz como desdobramento a inter-relação entre o trabalho (o que fazer, quais tarefas executar), o indivíduo (as habilidades, as competências) e as organizações (onde o indivíduo vai executar o trabalho). Dessa forma, estão envolvidos aspectos comportamentais individuais e do grupo, que influenciam diretamente na formação da cultura organizacional, a qual não é estática, precisa ser atualizada constantemente, cabendo aqui a necessidade da consolidação de uma cultura digital que acompanhe todo o avanço tecnológico.

2.1. O Fator Humano na Segurança da Informação

A interconectividade de informações avança a passos largos em um caminho sem volta por todas as facilidades que possibilita aos indivíduos e organizações. Ao mesmo tempo, a garantia de sua proteção é motivo de constante preocupação, e a cada dia surgem discussões a respeito da necessidade de novos controles de segurança da informação.

De acordo com Camillo & Hess (2020), à medida que o cenário de ameaças cibernéticas cresce e evolui, as organizações resilientes serão aquelas que enfrentarem as ameaças contemplando tanto o nível tecnológico quanto o comportamental, trabalhando de forma colaborativa com adesão de todos os níveis hierárquicos.

As empresas travam uma luta constante para proteção de seus dados, as ameaças tecnológicas se aprimoram a cada dia, dificultando o combate ao vazamento de informações, acrescido ao fato de que uma pessoa mal-intencionada ou carente de conscientização pode causar danos de mesma magnitude. Os funcionários podem, por

uma imprudência, cometer erros que resultam em violações de segurança: compartilhamento de senhas, a abertura de anexos de e-mails maliciosos ou a perda de dispositivos que contêm informações sensíveis.

Um levantamento feito com dados da plataforma *Egress Prevent* (EGRESS, 2021) aponta que o erro humano é o gatilho mais comum para seus comandos de prevenção de perda de dados (*Data Loss Prevention* – DLP) em tempo real.

Dentre as causas pelas quais o fator humano é sinalizado como preocupante para a segurança da informação está a falta de conhecimento sobre práticas de segurança, por isso, os cibercriminosos frequentemente utilizam técnicas de engenharia social - processo pelo qual se tenta convencer alguém de algo fictício, explorando as vulnerabilidades emocionais -, para manipulação dos usuários com o intuito de obter acesso não autorizado a sistemas ou informações confidenciais, as táticas mais comuns se dão por meio de ligações telefônicas falsas e e-mails de *phishing* (tentativas de fraude para obter ilegalmente informações, por meio de e-mail com conteúdo duvidoso).

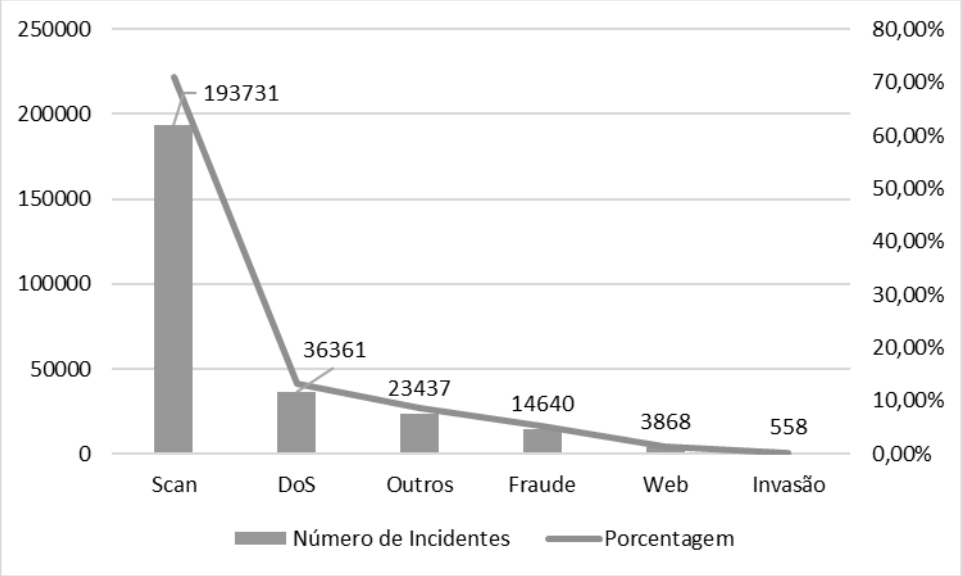
Segundo Steves, Greene, Theofanos (NIST, 2019), devido à crescente relevância do papel do comportamento humano na segurança cibernética, as empresas estão aumentando seus investimentos em iniciativas de conscientização sobre segurança digital para seus funcionários, frequentemente incluindo programas de treinamento contra phishing. O treinamento corporativo em conscientização contra phishing é amplamente adotado, e em muitos casos, obrigatório, abrangendo diversos setores como finanças, governo, saúde e educação.

O estudo *Data Breach Investigations Report (*Verizon, 2021) revela que a maioria das violações de dados, como *Ransomware* (sequestro de dados) e *Phishing*, envolveu um fator humano, e ainda, das violações de dados contabilizadas no ano de 2020, 85% envolveram algum tipo de interação humana.

No Brasil, de acordo com dados publicados pelo CERT.br (2023), dos 272.595 incidentes notificados no período de janeiro a maio de 2023, as fraudes correspondem a 14.640 ocorrências, ou seja, 5,37% do total conforme ilustra a figura 1, cabe aqui acrescentar o fato de que o *phishing* corresponde a 98% dessas fraudes.

Esses dados não representam a totalidade das ocorrências, haja vista que são relatados de forma espontânea pelas empresas, mesmo assim, representam uma amostragem a ser considerada, em que incidentes causados por Scan e DoS representam 84,40% do total.

Figura 1 – Incidentes Notificados ao CERT.br – janeiro a maio de 2023



Fonte: CERT.br, 2023

Os fatores contribuintes para as falhas humanas são extensos: fatores de trabalho (interrupções constantes, instruções ausentes ou falta de clareza, equipamentos inadequados, alta carga horária), fatores individuais (nível baixo de habilidade e competência, alto índice de estresse). Portanto, compreender a interação complexa desses fatores e adotar abordagens holísticas para mitigar riscos é essencial para melhorar a segurança e o desempenho em ambientes de trabalho.

Conforme Da Silva & Costa (2009), a discussão acerca do fator humano como elemento fundamental para a formulação de um novo conceito de Segurança da Informação mostra-se essencial. Isso ocorre porque os princípios de disponibilidade, integridade e confidencialidade da informação se não estiverem vinculados ao fator humano, que é indispensável para sua efetiva implementação, terão uma contribuição limitada para assegurar a eficácia do sistema.

Dentro desse cenário, Fonseca (2009) argumenta que a informação enfrenta uma variedade de ameaças, que podem surgir tanto de forma física, lógica ou humana. Para proteger seus sistemas e ambientes de informações contra acessos não autorizados, as organizações investem significativamente em tecnologias avançadas. No entanto, ressalta que negligenciar o fator humano pode comprometer todos esses esforços de segurança.

Embora as tecnologias avançadas sejam essenciais para proteger sistemas e dados, o principal fator para o sucesso ou fracasso de estratégias para a segurança da informação é o fator humano, sua importância e complexidade é indiscutível, e a próxima seção trará um outro olhar para essa problemática

2.2. O mito do elo mais fraco na Segurança da Informação

É senso comum que o fator humano representa um enorme desafio na segurança da informação, entretanto, as organizações podem adotar medidas de mitigação para esse tipo de risco, reduzindo as vulnerabilidades resultantes de erros ou comportamentos inseguros.

Conforme Garratech (2023)

> Investir em ferramentas e sistemas especializados é importante para se construir uma estratégia de segurança de dados efetiva dentro de uma empresa, mas se engana quem pensa que esse é o principal pilar na prevenção de ataques cibernéticos ou danos por acidente. Na verdade, o principal fator não se encontra em uma máquina ou um software específico, muito menos no mundo digital, ele é sim de carne e osso, repleto de emoções e complexidades; o principal fator é o humano.

Quando se reconhece a relevância do elemento humano na segurança da informação e a necessidade de um tratamento diferenciado para torná-lo efetivo, torna-se mais fácil buscar soluções para elevá-lo à categoria de barreira defensiva, nesse sentido, a palavra de ordem é investir em conhecimento com a implementação de programas de conscientização, treinamentos continuados em uma linguagem acessível, apresentar clareza nas políticas de segurança da informação, propiciar controles de acesso adequados e estabelecer uma cultura de segurança com ênfase na responsabilidade compartilhada indistintamente por todos que fazem parte de uma organização.

2.2.1 Conscientização e treinamento

Segundo o CERT (2013) as mitigações baseadas em treinamento e conscientização podem ser resumidas brevemente como: aumentar a conscientização sobre ameaças internas e ameaças internas não intencionais e a motivação para ter cuidado com elas, reconhecer "*phishing"* e outros vetores de ameaças de mídias sociais, incutir disciplina no processo para incentivar o cumprimento de políticas e diretrizes, treinar continuamente para manter o nível adequado de conhecimento e habilidades, promover treinamentos sobre percepção de risco e preconceitos cognitivos que afetam as decisões.

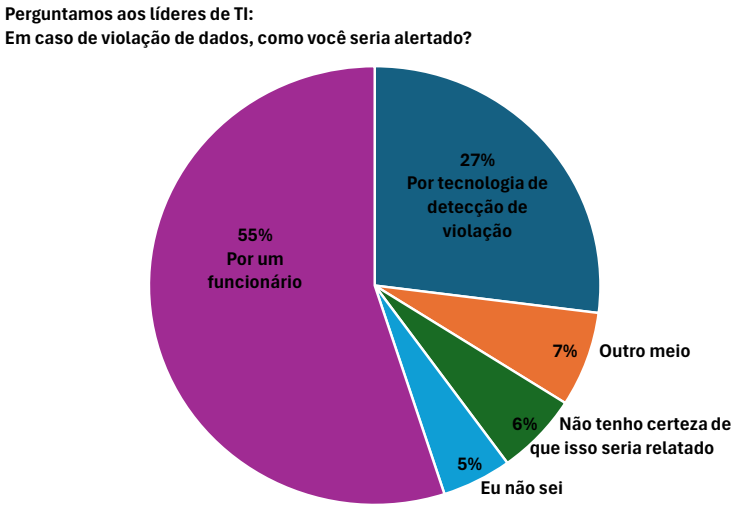
Programas de conscientização e treinamento adequados podem fortalecer o fator humano fazendo com que se torne efetivamente uma barreira contra ameaças cibernéticas, a partir do momento em que as pessoas estão bem informadas, elas se tornam conscientes dos riscos e passam a adotar comportamentos seguros, tais como: a utilização de senhas fortes, a identificação de ataques de engenharia social, "*phishing*", a adoção de medidas de segurança física e digital adequadas, entre outras ações. A conscientização e o treinamento adequados podem fortalecer o fator humano como uma barreira efetiva contra ameaças cibernéticas, para tanto é preciso investir na educação digital, capacitando profissionais a reconhecerem sinais de possíveis riscos e a adotar melhores práticas de segurança.

O controle 7.3 da norma ISO/IEC 27001 (2022) aborda a conscientização, afirmando que todas as pessoas que desempenham funções em uma organização devem estar cientes da política de segurança da informação, qual a sua contribuição para a eficácia do Sistema de Gestão da Segurança da Informação (SGSI), os benefícios que o melhor desempenho da segurança da informação pode trazer, bem como as implicações que não conformidades são capazes de acarretar.

Uma boa prática é a criação de uma cultura de segurança contemplando desde o alto escalão até o nível operacional, é preciso compreender que a segurança da informação é responsabilidade de todos, não somente de uma equipe específica. O sistema de incentivo e recompensa para comportamentos seguros costuma alavancar o engajamento da equipe nessa jornada de conscientização.

O relatório *Insider Data Breach Survey Report* (EGRESS, 2021) traz um levantamento sobre o nível de confiabilidade da equipe perante as lideranças, foram entrevistadas empresas do Reino Unido e Estados Unidos e o resultado é demonstrado na Figura 2.

Figura 2 – Alerta de violação de dados



Fonte: Egress, 2021

A pergunta feita às lideranças da área de Tecnologia da Informação (TI) foi: “Em um incidente de violação de dados, como você seria alertado? ”, mais de 50% responderam por um empregado contra somente 27% por um meio tecnológico de detecção. As outras opções de resposta foram: de outra forma (7%), eu não estou confiante de que serei informado (6%) e eu não sei (5%).

Essas lideranças demonstram que com equipes conscientes e bem treinadas, o fator humano pode ser uma barreira muito mais eficiente do que dispositivos de detecção de ameaças, desempenhando um papel de destaque na detecção e relatos de incidentes de segurança.

A capacidade de estar ciente dos sinais de atividade suspeita ou violações de segurança, possibilita um relato imediato para que as medidas cabíveis possam ser tomadas para mitigar os riscos, ajudando a identificação e resolução de problemas de segurança de forma mais rápida e eficaz.

Nesse sentido, a técnica de gamificação tem se mostrado uma excelente ferramenta para tornar o aprendizado sobre segurança da informação mais cativante e interativo, como no caso de criação de um ambiente de competição saudável entre equipes, com o intuito de identificar ameaças simuladas.

Conforme mencionado por Zichermann & Cunningham (2011), a gamificação pode ser facilmente aplicada a qualquer problema que possa ser resolvido, influenciando a motivação e o comportamento humano.

À medida que as pessoas adquirem maior consciência sobre a importância da segurança da informação e a relevância de seu papel nesse processo, a barreira de proteção se solidifica e o nível de segurança atinge um patamar mais elevado.

2.2.2. Comunicação e transparência

A comunicação é um processo de extrema relevância nas interações estabelecidas entre indivíduos diariamente. No âmbito empresarial, a comunicação evoluiu para se tornar uma ferramenta essencial na definição da cultura organizacional, requerendo abordagens inteligentes e transparentes a fim de gerar resultados positivos.

É uma boa prática o estabelecimento de canais de comunicação abertos para que os funcionários consigam relatar incidentes de segurança sem a preocupação com represálias.

De acordo com Neiva Santos de Oliveira (2018), a empresa deve focar em princípios como transparência, empatia, comprometimento, pensamento crítico e profissionalismo, especialmente por lidar diariamente com uma variedade de indivíduos. É essencial buscar atender a todos com respeito, reconhecendo sempre suas contribuições e lembrando que trabalham não apenas em benefício da empresa, mas também de si mesmos e de suas famílias.

Já quando o foco é a implementação de sistemas e procedimentos de segurança, é preciso contemplar as seguintes questões:

- Qual é o nível de experiência do usuário? Medidas muito complicadas, que possam dificultar as tarefas diárias, têm grande chance de serem ignoradas.

- Como é o comportamento digital da equipe? Existem ferramentas como análise de comportamento de usuários (UBA) ou análise de comportamento de entidade do usuário (UEBA) que utilizam algoritmos e "*machine learning*", dessa forma podem ajudar a identificar atividades suspeitas baseado em padrões comportamentais.

- As políticas de acesso e privacidade estão bem definidas? O ideal é que haja clareza nessas definições, para que sejam de fácil entendimento, e os usuários compreendam que o seu acesso se restringe apenas às informações e recursos necessários para realizar as suas funções.

Segundo Freire et al. (2017), "As organizações devem estar sempre preocupadas em propiciar um ambiente seguro não só tecnologicamente, mas também funcionalmente. Cada indivíduo deve ter conhecimento suficiente sobre SI para poder implantá-la no dia a dia."

Um olhar voltado para a perspectiva de motivação e valorização dos recursos humanos é algo que as organizações devem almejar sempre, assim sendo, a forma de transmitir as demandas necessárias para diferentes indivíduos precisa abranger além da transparência, requer valores como empatia e compromisso.

3. Metodologia

Este trabalho foi elaborado baseando-se no método hipotético-dedutivo, utilizando métodos de pesquisas bibliográficas em livros, artigos científicos, dissertações e publicações.

De acordo com Marconi & Lakatos (2021) o método constitui o conjunto de atividades sistemáticas e racionais que, com maior segurança e eficiência, viabiliza a obtenção do objetivo, delineando o percurso a ser seguido, identificando equívocos e subsidiando as escolhas do pesquisador.

No decorrer deste estudo, abordou-se inicialmente o fator humano na segurança da informação, seguido pelos desafios que enfrenta ao receber o rótulo de "elo mais fraco", e de que maneira a conscientização e treinamento possibilitam o questionamento desse "título". Finalmente, abordou-se a questão de comunicação e transparência.

Objetivando a sua fundamentação, foram realizadas entrevistas individuais estruturadas em duas organizações com diferentes escopos, os sujeitos foram dois gestores que possuem envolvimento com a questão de incidentes de segurança. O formato das entrevistas propiciou o acompanhamento das respostas, abrindo a possibilidade de inclusão de perguntas relacionadas não inclusas no roteiro.

Segundo Severino (2013) as entrevistas estruturadas são feitas com direcionamento preestabelecido, semelhante a um questionário, porém, com caráter mais pessoal. Esse aspecto possibilita categorizar mais facilmente as respostas.

Nas entrevistas, o objetivo primordial consistiu em compreender o perfil do gestor que estava sendo entrevistado, avaliando seu entendimento acerca dos incidentes que impactaram a empresa e a maneira pela qual as preocupações referentes ao fator humano receberam abordagem.

Interrogativas foram dirigidas sobre incidentes de segurança que haviam ocorrido previamente e sobre como o gestor se mantém atualizado em relação a tópicos relacionados à TI e segurança da informação. Adicionalmente, também se investigou o perfil da companhia no que tange a problemas de natureza humana.

Explorou-se também o valor da informação para a empresa e os riscos que a acompanham, a intenção foi entender como as empresas estão lidando com essa questão. Por último, indagou-se sobre as ferramentas e técnicas de defesa implementadas na empresa, bem como os motivos por trás dos investimentos atuais e futuros na gestão da segurança da informação.

4. Resultados e Discussões

O levantamento e análise dos dados baseou-se nas informações obtidas por meio de entrevistas, feitas em duas etapas: a primeira no mês de agosto de 2023 em duas empresas situadas na Região Metropolitana de Campinas, e a segunda etapa no mês de novembro de 2023.

Na primeira etapa, uma empresa é familiar de médio porte, do ramo de autopeças, chamaremos aqui de Empresa 1, quem concedeu a entrevista ocupa o cargo de Diretor Técnico; a segunda é uma empresa de grande porte voltada para a área farmacêutica, denominaremos como Empresa 2, o entrevistado ocupa o cargo de Gerente de Segurança da Informação.

Na continuidade do processo de entrevistas, a atenção foi direcionada a duas empresas atuantes no setor de tecnologia da informação. Identificaremos essas empresas como Empresa 3 e Empresa 4, sendo que os entrevistados ocupam os cargos de Gerente de SOC e Gerente de TI, respectivamente.

O propósito central de cada etapa reside na elaboração de um quadro comparativo entre as práticas adotadas por cada uma das empresas. Tal análise visa não somente destacar as abordagens específicas em relação à segurança da informação, mas também permitir uma avaliação comparativa mais abrangente, que possibilite relacionar as estratégias referentes ao fator humano em segurança da informação entre empresas especializadas em tecnologia da informação e empresas de outros setores.

4.1. Roteiro das Entrevistas

O roteiro é composto por 8 questões que procuram obter um conteúdo que possibilite traçar um perfil do gestor, da empresa e a tratativa de questões referentes ao fator humano na segurança da informação, as questões propostas encontram-se no Apêndice A.

Optou-se pela análise do conteúdo em detrimento de uma transcrição das respostas, mantendo-se o anonimato das empresas e dos entrevistados, já que o objetivo é tão somente ilustrar o comportamento das empresas e dos indivíduos quando se trata de fator humano na segurança da informação.

4.2. Análise comparativa das empresas com base nas entrevistas da etapa 1

A intenção da formulação desse quadro comparativo é refletir sobre o comportamento diante de questões referentes ao fator humano na segurança da informação, por parte de uma empresa de grande porte com uma área de TI bem constituída, e no contraponto, uma empresa de médio porte que não possui internamente uma área de TI. A Tabela 1 apresenta de que maneira estão estruturadas para atendimento dessa demanda tão emergente.

No que tange à questão referente aos incidentes mais recentes e/ou significativos, no caso da Empresa 1 o site da empresa sofreu um ataque de negação de serviço (*DoS - Denial of Service*) e ficou uma manhã toda fora do ar. Houve uma falha na configuração do *Firewall*.

A Empresa 2 tem sofrido diversos ataques no último semestre de fontes externas e internas, porém com toda governança de segurança da informação implantada, em conjunto com as ferramentas configuradas, todos os eventos foram identificados e controlados antes da efetivação concreta de um incidente.

Tabela 1 - Aspectos da tratativa do fator humano na segurança da informação nas empresas da etapa 1

Tópicos abordados	Empresa 1	Empresa 2
Equipe específica para tratar incidentes de segurança	Não possui equipe específica, existe um DPO (encarregado de dados) e uma empresa terceirizada de TI.	Sim, uma equipe BlueTeam trabalha para tratar incidentes críticos de segurança.
Sistemática quando ocorre um incidente de segurança	É informado imediatamente ao DPO e à assessoria de TI terceirizada, para uma avaliação da gravidade e possíveis medidas de mitigação.	Por meio de monitoração em tempo real, após o evento ser conhecido, o plano de resposta à incidentes de segurança da informação é invocado.
Treinamento e Conscientização	Existe uma cartilha de conscientização com explicações sobre tratamento de dados, código de conduta e principais ameaças em linguagem acessível, é fornecida durante a integração de funcionários, foi entregue a todos os funcionários durante o processo de adequação à LGPD. Os treinamentos são semestrais e as campanhas de conscientização são mensais.	A empresa possui um processo contínuo de treinamento e conscientização em segurança da informação e proteção de dados pessoais, mantendo contínua reciclagem de todo o pessoal da empresa que lida com dados e informações.
Valor da informação e riscos	Mantém uma Política de Segurança da Informação, possui identificação e avaliação de ativos de informação, controles de acesso, gestão de riscos e oportunidades, backup e recuperação de dados.	A empresa possui um conjunto de políticas de segurança da informação, geral e por tema, com revisão anual e publicada para as partes interessadas de acordo com a função na empresa.
Ferramentas e Técnicas de Defesa	Firewall, antivírus, política de senhas, política de backup, treinamentos e conscientização.	Ativos de segurança, como firewalls, IPS/IDS, WAFs (Web Application Firewall), EDRs (Endpoint Detection and Response).
Investimento em soluções de cibersegurança	Não há cota específica para essa finalidade.	Determinado em planejamento para ano seguinte, dependendo do resultado financeiro da empresa.

Fonte: Autores |(2023)

4.3. Análise comparativa das empresas com base nas entrevistas da etapa 2

O propósito implícito à elaboração deste segundo conjunto de comparações é analisar o comportamento de duas empresas do setor específico de Tecnologia da Informação diante de questões relacionadas ao fator humano na segurança da informação e avaliar suas estruturas para atender a essa demanda, conforme retrata a Tabela 2.

Tabela 2 - Aspectos da tratativa do fator humano na segurança da informação nas empresas da etapa 2

Tópicos Abordados	Empresa 3	Empresa 4
Equipe específica para tratar incidentes de segurança	Sim, existe uma equipe interna na empresa que trata os incidentes de segurança da informação.	Não existe uma equipe interna, mas uma empresa externa faz a monitoração de todo o ambiente e cuida do tratamento dos incidentes de segurança da informação.
Sistemática quando ocorre um incidente de segurança	Processo definido pela equipe de segurança cibernética.	Política e processo interno alinhado com a empresa que presta o serviço de segurança da informação.
Treinamento e Conscientização	Contratada uma empresa externa que aplica treinamento a cada 6 meses.	Treinamento realizado somente para novos empregados.
Valor da informação e riscos	Política de privacidade, os riscos são monitorados pela equipe de segurança cibernética.	Política de classificação da informação e monitoração pela equipe interna.
Ferramentas e Técnicas de Defesa	Firewall de borda, WAF para aplicações.	Firewall de borda e soluções de EDR e IPS/IDS.
Investimento em soluções de cibersegurança	Baseado em contratos fechados com clientes, venda de produtos e serviços.	Sem informação.

Fonte: Autores (2023)

4.4. Análise comparativa geral das duas etapas de entrevistas

Finalizando a análise, a Tabela 3 sintetiza os aspectos gerais em cada um dos tópicos nas duas etapas de entrevistas.

Tabela 3 - Aspectos gerais da tratativa do fator humano na segurança da informação

Tópicos Abordados	Aspectos Gerais
Equipe específica para tratar incidentes de segurança	Dentre as quatro empresas entrevistadas, duas optaram pela terceirização dessa tratativa.
Sistemática quando ocorre um incidente de segurança	Todas possuem um plano de resposta a incidentes.
Treinamento e Conscientização	Existe em todas, variando a periodicidade e o público-alvo.
Valor da informação e riscos	Todas possuem políticas de segurança da informação, políticas de privacidade e monitoramento dos riscos.
Ferramentas e Técnicas de Defesa	Todas possuem ferramentas e técnicas de defesa com variações de acordo com o porte de cada empresa.
Investimento em soluções de cibersegurança	Com base nesse aspecto, pode-se concluir que somente duas das empresas entrevistadas possuem uma abordagem clara em relação a esse tipo de investimento.

Fonte: Autores (2023)

Cabe destacar que a pesquisa não oferece resultados conclusivos; ela se baseia em uma amostra e pode não refletir com precisão a situação em diferentes áreas ou com diferentes grupos de entrevistados.

5. Considerações finais

A segurança da informação é um processo contínuo de aprendizado e melhoria, requer um acompanhamento constante e ajustes conforme a necessidade do momento. O ideal é todo esse processo ser submetido a uma democratização do conhecimento,

difundindo a conscientização da equipe sobre o seu papel de ferramenta de contra-ataque às violações no tratamento dos dados.

Ao adotar uma abordagem mais abrangente e centrada nas pessoas, é possível aprimorar consideravelmente a postura de segurança da organização e reduzir os riscos relacionados ao fator humano na segurança da informação.

Uma cultura organizacional que valoriza a segurança da informação pode incentivar os funcionários a adotarem comportamentos seguros e agirem como defensores da segurança. Cada vez que a segurança da informação é uma prioridade em todos os níveis da organização, os funcionários se sentem responsáveis por proteger os dados e os recursos da empresa, tornando-se uma efetiva barreira contra ameaças internas e externas.

Fica claro pela coleta de dados e respectivas análises que as ações relacionadas a segurança da informação nas empresas avaliadas possuem diferenças significativas na abordagem em proporcionar aos funcionários conhecimento adequado para tratar, durante as suas atividades rotineiras, o manuseio de ativos de informação de forma a não produzir riscos ao negócio.

Quando as pessoas estão engajadas e têm voz ativa na implementação e revisão das medidas de segurança, conseguem colaborar com suas concepções e conhecimentos para fortalecer a segurança da informação, tais como: a identificação de lacunas ou vulnerabilidades, sugestões de melhorias e a adoção de boas práticas no uso de sistemas e dados.

Portanto, embora o fator humano possa ser considerado uma vulnerabilidade na segurança da informação, quando adequadamente educado, treinado e envolvido, pode se tornar uma sólida ferramenta de defesa para proteger as informações e os sistemas de uma organização.

Referencial Bibliográfico

Camillo, Mark; Hess, Sebastian. American International Group. AIG. Human Cyber Risk – The first line of defence. Disponível em: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-human-factor.pdf . Acesso em 02 jun. 2022.

Cert. Unintentional Insider Threats: A Foundational Study Produced for Department of Homeland Security Federal Infrastructure Protection Bureau, 2013. Disponível em: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf . Acesso em 25 ago. 2023.

Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil. Estatísticas dos Incidentes Reportados ao CERT.br. São Paulo: CERT.br, 2023. Disponível em: https://stats.cert.br/incidentes/ . Acesso em 29 jun. 2023.

Da Silva, Maicon Herverton Lino Ferreira; Costa, Veridiana Alves de Sousa Ferreira; Pernambuco, Unidade Acadêmica de Serra Talhada. O fator humano como pilar da Segurança da Informação: uma proposta alternativa. Disponível em: http://www.eventosufrpe.com.br/jepex2009/cd/resumos/r0052-3.pdf . Acesso em 23 ago.2023.

Egress Software Technologies. Insider Data Breach Survey Report, 2021. Disponível em: https://www.egress.com/blog/what-is-human-layer-security/2021-insider-breach-survey. Acesso em 26 abr. 2022.

Egress software technologies. Egress CISO Guide: Preventing Human Error on Email, 2023. Disponível em: https://www.egress.com/media/lq0bj5bj/egress_ciso_guide_preventing_human_ error.pdf . Acesso em 13 mar. 2023.

Fonseca, Paula Fernanda. Gestão de Segurança da Informação: o fator humano. Pontifícia Universidade Católica do Paraná. Curitiba, 2009. Disponível em: https://www.cursosavante.com.br/cursos/curso533/conteudo7486.pdf. Acesso em 23 ago. 2023.

Fontes, Edison Luiz Gonçalves. Segurança da informação. Saraiva Educação SA, 2017.

Freire, R. F. P.; Silva, H. C. C.; Queiroz, R. G.; Batista, A. A. M.. O fator humano como uma vulnerabilidade em segurança da informação. Revista Brasileira de Administração Científica, v.8, n.3, p.146-157, 2017. DOI: https://www.sustenere.co/index.php/rbadm/article/view/SPC2179-684X.2017.003.0012 . Acesso em 18 jul.2023.

Garratech. A importância do fator humano na segurança da informação, 2023. Disponível em: A importância do fator humano na segurança da informação. Disponível em http://www.garratech.com.br. Acesso em: 20 mar. 2023.

Health and safety executive. Introduction to human factors, 2022. HSE. Disponível em: http://www.hse.gov.uk . Acesso em: 3 dez. 2022.

ITForum. Fator humano: o principal componente da segurança da informação , 2018. Disponível em: Fator humano: o principal componente da segurança da IT Forum. Acesso em: 30 jan. 2023.

International Standard. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks, 2022.

International Standard. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems. —Requirements, 2022.

Marconi, Marina de Andrade; Lakatos, Eva Maria. Fundamentos de Metodologia 1 - 9. ed. - São Paulo : Atlas 2021. p.83.

Minto, Lalo Watanabe. Teoria do Capital Humano. HISTEDBR – Grupo de Estudos e Pesquisas ¨História, Sociedade e Educação no Brasil¨. Faculdade de Educação da Unicamp, 2021. Disponível em: https://www.histedbr.fe.unicamp.br/navegando/glossario/teoria-do-capital-humano. Acesso em 14 jan.2023.

Neiva Santos de Oliveira, F. (2018). Comunicação das Organizações: Um olhar sobre a importância da Comunicação Interna. Media & Jornalismo, 18(33), 61-74. https://doi.org/10.14195/2183-5462_33_4. Acesso em 17 de julho de 2023.

Severino, A. J. Metodologia do Trabalho Científico [livro eletrônico]1. ed. São Paulo: Cortez, 2013. p.97.

Steves, Michelle; Greene, Kristen; Theofanos, Mary. National Institute of Standards and Technology. NIST. A Phish Scale: Rating Human Phishing Message Detection Difficulty, 2019. Disponível em: https://csrc.nist.gov/publications/detail/conference-paper/2019/02/24/rating-human-phishing-message-detection-difficulty. Acesso em 23 maio 2023.

Verizon. Data Breach Investigations Report (DBIR), 2021. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em 02 fev. 2023.

Zichermann, G.; Cunningham, C. Gamification by design: Implementing game mechanics in web and mobile apps. " O'Reilly Media, Inc.", 2011. Disponível em: https://books.google.com.br/books/about/Gamification_by_Design.html?id=Hw9X1miVMMwC&redir_esc=y. Acesso em: 18 ago. 2023.

APÊNDICE A - Questionário utilizado na pesquisa

1. A empresa possui uma equipe específica para tratar incidentes de segurança? Em caso afirmativo, quantas pessoas estão envolvidas?

2. Qual a sua função na empresa e há quanto tempo atua com assuntos relacionados a incidentes de segurança?

3. Que sistemática é adotada quando ocorre um incidente de segurança? Poderia relatar o mais recente ou mais significativo?

4. Como os funcionários se mantêm informados e atualizados sobre assuntos ligados à segurança da informação?

5. A empresa possui programas cíclicos de treinamento e conscientização? Quais?

6. De que forma a empresa lida com o valor da informação e o risco inerente a ela?

7. Quais as ferramentas e técnicas de defesa implantadas na empresa?

8. Há um orçamento específico para investimentos em gestão da segurança da informação?