CENTRO UNIVERSITÁRIO UNICARIOCA
MESTRADO PROFISSIONAL EM NOVAS TECNOLOGIAS DIGITAIS NA EDUCAÇÃO

George João de Almeida Chaves

USO DE METODOLOGIAS ATIVAS DE APRENDIZAGEM NO DESENVOLVIMENTO DE CULTURA EM CIBERSEGURANÇA EM AMBIENTES CORPORATIVOS

Rio de Janeiro
2021

George João de Almeida Chaves

USO DE METODOLOGIAS ATIVAS DE APRENDIZAGEM NO DESENVOLVIMENTO DE CULTURA EM CIBERSEGURANÇA EM AMBIENTES CORPORATIVOS

Dissertação apresentada ao Programa de Pós-Graduação em Novas Tecnologias Digitais na Educação do Centro Universitário UniCarioca como parte dos requisitos necessários para a obtenção do Título de Mestre em Novas Tecnologias Digitais na Educação.

Orientador: Prof. Dr. Alessandro Jatobá

Co-orientadora: Prof. Dra. Rosa Valim

Rio de Janeiro

2021

George João de Almeida Chaves

USO DE METODOLOGIAS ATIVAS DE APRENDIZAGEM NO DESENVOLVIMENTO DE CULTURA EM CIBERSEGURANÇA EM AMBIENTES CORPORATIVOS

Dissertação apresentada ao Programa de Pós-Graduação em Novas Tecnologias Digitais na Educação do Centro Universitário UniCarioca como parte dos requisitos necessários para a obtenção do Título de Mestre em Novas Tecnologias Digitais na Educação.

O Presidente da Banca abaixo assinado atesta que os membros da banca participaram de forma remota desta defesa de dissertação.

Examinado por:

Prof. Dr. Sc. – Alessandro Jatobá, Presidente da Comissão Examinadora (UniCarioca)

Prof. Dr. Sc. – Paulo Victor Rodrigues de Carvalho (UniCarioca)

Prof. Dr. Sc. – Hugo Cesar Bellas (Fiocruz)

Profa. Me. Sc. – Josilene Marrone Coelho de Barros (SENAC/RJ)

Rio de Janeiro

2021

C512u Chaves, George João de Almeida
Uso de metodologias ativas de aprendizagem no desenvolvimento de cultura em cibersegurança em ambientes corporativos / George João de Almeida Chaves – Rio de Janeiro, 2021.
103 f.

Orientadores: Alessandro Jatobá e Rosa Lídice de Moraes Valim.
Dissertação (Mestrado Profissional em Novas Tecnologias Digitais na Educação) - Centro Universitário UniCarioca, Rio de Janeiro, 2021.

1. Segurança da informação. 2. Educação corporativa. 3. Privacidade de dados. 4. Indicadores de competência. 5. Metodologia ativa de aprendizagem. . I. Jatobá, Alessandro, prof. orient. II. Valim, Rosa Lídice de Moraes, prof. coorient. III. Título.

CDD 370.153

Dedico este trabalho à minha mãe Gilda de Almeida Chaves, minha grande inspiração na Educação, ao meu pai José Pereira chaves, meu maior incentivador; à minha companheira Gisele Soares dos Santos e à minha filha, Giovana Soares dos Santos, meu maior motivo de alegria.

AGRADECIMENTOS

Agradeço imensamente a todos aqueles que direta, ou indiretamente, contribuíram de alguma forma com o desenvolvimento deste trabalho e que, foram de grande valia para meu meu aprendizado durante todo o período do Mestrado. É impossível mencionar nomes, sem cometer alguma injustiça, pois todos, sem exceção foram fontes de conhecimento e inspiração durante algum momento.

No entanto, não posso deixar de citar os Coordenadores do curso, Professor Antônio Carlos Mól e a Professora Ana Paula Legey, em meus agradecimentos, seja pela construção da proposta do curso, seja pelo apoio ao aluno durante toda a jornada. Agradeço também ao Professor e orientador, Alessandro Jatobá, por ter me orientado durante o desenvolvimento dessa pesquisa. Também não pode deixar de citar todos os professores do MPNTDE, que trouxeram muitos insights e provocações durante todo o Mestrado.

Aos meus colegas de turma, aos colegas de trabalho e a todos que em algum momento sentaram comigo para discutir de que forma poderíamos contribuir para melhorar a Educação no país de alguma forma, o meu muito obrigado!

RESUMO

Devido a grande digitalização dos processos nas organizações, é notório o crescimento de crimes cibernéticos e incidentes de segurança, especialmente na última década. Um dos maiores vetores de ataque utilizados pelos criminosos é a Engenharia Social, que explora aspectos da vulnerabilidade humana e induz as pessoas a realizarem ações que potencialmente colocam em risco os ativos de informação da organização. Atuando como Consultor em Projetos de Gestão de Riscos e Segurança da Informação e, sendo responsável por programas de treinamento em algumas organizações brasileiras, pude identificar pontos de melhoria na metodologia que as empresas vêm utilizando para capacitar ou conscientizar os colaboradores. A presente pesquisa apresenta um modelo de ensino baseado em técnicas que utilizam metodologias ativas de aprendizagem para o desenvolvimento da cultura em cibersegurança nas pessoas. O experimento foi aplicado em cerca de 200 colaboradores de uma grande organização de telecomunicações internacionalmente conhecida e se mostrou positivo, motivando e engajando os participantes durante as atividades realizadas e resultou em números que diretamente se correlacionam a adoção de um melhor comportamento dos colaboradores frente a uma ameaça de segurança da informação. Conclui-se, portanto, que o uso das metodologias ativas de aprendizagem em programas de treinamento de segurança da informação em ambientes corporativos, pode contribuir para a redução da probabilidade de um incidente ocorrer ou reduzir os impactos causados por uma ameaça digital que explora uma vulnerabilidade tecnológica, organizacional ou humana.

Palavras Chave: segurança da informação; educação corporativa; privacidade de dados; indicadores de competência; metodologia ativa de aprendizagem

ABSTRACT

Due to the great digitalization of processes in organizations, the growth of cyber crimes and security incidents is notorious, especially in the last decade. One of the biggest attack vectors used by criminals is Social Engineering, which explores aspects of human vulnerability and induces people to take actions that potentially put the organization's information assets at risk. Acting as a Consultant in Risk Management and Information Security Projects and, being responsible for training programs in some Brazilian companies, I was able to identify points of improvement in the methodology that companies have been using to train or raise awareness among employees. This research presents a learning model based on techniques that use active learning methodologies, in particular, Hybrid Teaching, Case Studies and Inverted Classroom. The experiment was applied to around 200 employees of a large internationally known telecommunications company and proved to be positive, motivating and engaging participants during the activities carried out and resulted in numbers that directly correlate to the adoption of better employee behavior in the face of a information security threat. It is concluded, therefore, that the use of active learning methodologies in information security training programs in corporate environments, can contribute to reduce the probability of an incident to occur or reduce the impacts caused by a digital threat that exploits a vulnerability technological, organizational or human.

Key words: information security; corporative education; data privacy; competence indicators; active learning methodologies

LISTA DE ILUSTRAÇÕES

Figura 01 – Atividade prática pautada na resolução de problemas 13
Figura 02 - Tríade de Segurança da Informação 22
Figura 03 – Exemplo de Engenharia Social 26
Figura 04 – Engenharia social através de phishing 27
Figura 05 – Forma de comunicação à vítima em infecções por Ransomware . 28
Figura 06 – E-mail enviado pelo criminoso extorquindo a vítima 28
Figura 07 – Ação de conscientização em cibersegurança 30
Figura 08 – Caminho metodológico da pesquisa 35
Figura 09 – Programa de treinamento 38
Figura 10 – Ambiente de ensino 40
Figura 11 – Resultado de e-mail phishing 41
Figura 12 – Processo de Gestão de Riscos conforme ISO 31000 43
Figura 13 – Atividade colaborativa de Gestão de Riscos 44
Figura 14 – Consolidado da atividade de Gestão de Riscos 44
Figura 15 – Dashboard gerado a partir de avalições de reação 45
Figura 16 – Incidentes de segurança reportados nos últimos 12 meses 49
Figura 17 – Uso de Engenharia social como vetor de ataque cibernético 49
Figura 18 - Formatos de ações de treinamento e conscientização 50
Figura 19 – Percepção do comportamento dos colaboradores 52
Figura 20 – Atividade Hands-On de Gestão de Riscos 53
Figura 21 – Atividade gamificada usando o Kahoot! 54
Figura 22 – Ranking da atividade gamificada usado o Kahoot! 55
Figura 23 – Atividade baseada na metodologia PBL 55
Figura 24 – Atividade baseada em Sala de Aula Invertida 56
Figura 25 – Atividade baseada em Estudo de Caso 57
Figura 26 – Atividade de cocriação com uso do Microsoft Teams 58
Figura 27 – Avaliação da experiência do colaborador em um treinamento 59
Figura 28 – Pesquisa sobre a relevância do tema para os participantes 60
Figura 29 – Resultado de pesquisa de satisfação após um dos Workshops ... 61
Figura 30 – Modelo de avaliação de indicadores de eficácia do programa 62
Figura 31 – Indicadores históricos de simulações de e-mail phishing 62
Figura 32 – Indicadores atualizados de e-mail phishing 63
Figura 34 – Evolução histórica comparativa de indicadores 64

LISTA DE TABELAS

Tabela 01 – Ameaças digitais 24
Tabela 02 – Perguntas do questionário..... 36
Tabela 03 – Resultados de simulação de e-mail phishing 46
Tabela 04 – Formas de comunicação de segurança aos colaboradores 48
Tabela 05 – Público-alvo de treinamentos em Cibersegurança 50
Tabela 06 - Resposta aberta da Avaliação de Reação 60
Tabela 07 – Comparativo de indicadores de comportamento de usuários 63

LISTA DE ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas
AVA - Ambiente Virtual de Aprendizagem
CISO - Chief Information Security Officer
EaD - Educação a Distância
ISO - International Organization for Standardization
NBR - Norma Brasileira
OCDE - Organização para a Cooperação e o Desenvolvimento Econômico
OTA - Online Trust Alliance
PBL - Problem Based Learning
SD - Sequência Didática
SGSI - Sistema de Gestão de Segurança da Informação
SI - Segurança da Informação
SPAM - Sending and Posting Advertisement in Mass
TI - Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Inquietação 12
1.2 Caracterização do problema 14
1.3 Propostas de solução para o problema 16
1.4 Objetivo geral 18
1.5 Objetivos específicos 18

2 FUNDAMENTAÇÃO TEÓRICA 20
2.1 Ameaças Digitais 20
2.2 Engenharia Social 25
2.3 Cultura em Cibersegurança 29
2.4 Metodologias ativas de aprendizagem 30

3 MÉTODO 34
3.1 Metodologia 34
3.2 Levantamento exploratório 35
3.3 Mapeamento do ambiente 37
3.4 Criação do programa de treinamento 37
3.5 Criação de indicadores de eficácia do treinamento 40
3.6 Execução do programa de treinamento 42
3.7 Avaliação de Reação 45
3.8 Aferição da eficácia do programa de treinamento 46
3.9 Consolidação e análise dos resultados 47

4 RESULTADOS E DISCUSSÕES 48
4.1 Resultados do levantamento exploratório 48
4.2 Uso de metodologias ativas de aprendizagem 52
4.3 Avaliação de reação 58
4.4 Comparativo de indicadores 60

5. CONCLUSÃO 64

REFERÊNCIAS 66

APÊNDICES 70
A. Gráficos do Questionário online 71
B. Sequência Didática 79

1 INTRODUÇÃO

> “Ninguém nasce feito, é experimentando-nos no mundo que nós nos fazemos.” (FREIRE, 1921-1997).

1.1 Inquietação

Na área de educação, atuo na iniciativa privada há 8 anos. Já fui professor de Informática para o Ensino Fundamental (6º e 7º anos), professor de Curso Técnico em Informática e Química, professor de cursos de Pós-Graduação, instrutor em treinamentos corporativos e, além de docente, atuei em Colégios e Universidades, exercendo a função de Coordenador de Curso e Especialista de Produtos Educacionais. Durante toda minha jornada como Educador até aqui, quer seja na Educação Formal ou Educação Corporativa, sempre foi notório que os mais de 1 mil alunos em que participei de sua formação, demonstravam maior interesse quando sentiam que aquele conhecimento fazia sentido para eles. O engajamento se dava de maneira muito mais fluída quando eles participavam ativamente do processo de construção da aprendizagem. Além disso, percebi que nem sempre uma metodologia que era usada em um grupo, funcionava da mesma forma em outro grupo. Por isso, a possibilidade do uso das tecnologias educacionais para construção do saber, aliada às metodologias ativas de aprendizagem foi algo em que percebi ter feito toda a diferença em promover maior engajamento dos participantes, seja qual for o curso ou faixa etária.

Já em minha vivência como profissional de tecnologia e segurança da informação, fui responsável por tratar diversos incidentes de segurança que geraram impactos às organizações. Minha percepção na identificação das origens desses incidentes é que o fator humano estava habitualmente presente como uma das causas. Seja pelo desconhecimento técnico do colaborador ou por ter sido usado como parte de uma estratégia mais elaborada de ataque cibernético, as pessoas trouxeram riscos ou potencializaram impactos para a organização, gerando consequências negativas para ela, como interrupção dos serviços, retrabalho, prejuízo financeiro, danos à reputação ou desconfiança do mercado.



Figura 01 – Atividade prática pautada na resolução de problemas

Mais recentemente, ocupando posições em Consultorias de Segurança da Informação e, sendo responsável por criar programas de treinamento em organizações brasileiras, pude identificar pontos de melhoria na metodologia que as empresas vêm utilizando para capacitar ou conscientizar os colaboradores. Os problemas identificados a partir desta observação, estão descritos abaixo:

- O colaborador não se sente responsável pela segurança da informação e proteção de dados, acreditando que isso é uma tarefa específica do setor de Tecnologia da Informação ou da área de Segurança da organização;
- Os programas de conscientização em segurança das empresas são pontuais, muitas vezes acontecendo após a organização ter sido vítima de grave incidente de segurança. Não há intenção pela continuidade do programa, limitando-se a propósitos específicos e sem considerar o uso de métricas para avaliações da eficácia destes programas;
- Os treinamentos não são customizados para a realidade da organização, fazendo com que os participantes tenham uma percepção de que os

conteúdos ministrados estão distantes de sua realidade e não se sentem engajados na realização das atividades propostas.

Boa parte dos incidentes de segurança ocorridos nas organizações poderia ser evitado se o colaborador adotasse um comportamento alinhado às boas práticas de uso dos dispositivos computacionais. Mas, para que seja desenvolvido o senso de pertencimento do colaborador e que ele se sinta parte integrante da proteção de informações da organização passando a adotar uma postura mais alinhada com as boas práticas, é necessário que ele seja motivado a participar ativamente de treinamentos e programas de conscientização oferecidos pelas suas empresas.

Essa pesquisa, portanto, considera o uso de metodologias ativas de aprendizagem como opção ao modelo tradicional adotado pelas organizações, inserindo o colaborador no papel de principal agente de construção do conhecimento. Assim, atitudes como oportunizar a escuta aos colaboradores, valorizar suas opiniões, exercitar a empatia, responder aos questionamentos, encorajá-los, dentre outras, serão favorecedoras da motivação (BERBEL, 2011) e da criação de um ambiente favorável à aprendizagem.

1.2 Caracterização do problema

A todo momento os processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças digitais de toda natureza, que buscam identificar um ponto fraco ou uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2001, p. 18).

Uma definição abrangente para a segurança da informação é dada por Sêmola (2003, p.44):

> [...] uma prática adotada para tornar um ambiente seguro [...], de caráter interdisciplinar, composta de um conjunto de metodologias e aplicações que visam estabelecer: controles de segurança [...] dos elementos constituintes de uma rede de comunicação e/ou que manipulem a informação; e procedimentos para garantir a continuidade de negócios na ocorrência de incidentes.

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos, físicos e humanos. A camada física é o

ambiente onde está instalado fisicamente os equipamentos como computadores, notebooks, servidores, equipamentos de conectividade, estando estabelecidos fisicamente no perímetro da organização ou nas casas das pessoas, caso esteja sendo considerado o trabalho de home office. Para Adachi (2004), "a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física".

A camada lógica é caracterizada pelo uso de programas de computador responsáveis pela funcionalidade dos equipamentos, pela realização de transações em base de dados organizacionais, proteção das comunicações e arquivos e criptografia. Segundo Adachi (2004), é nessa camada que estão as "regras, normas, protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas".

Já a camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de Tecnologia da Informação – TI. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; se são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (ADACHI, 2004).

Das três camadas, esta é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual (SCHNEIER, 2001).

De acordo com (Furnell & Thomson, 2009), um dos grandes problemas e ameaças verificados na implementação de práticas e procedimentos na segurança da informação são os colaboradores. Por este fato, torna-se necessário promover dentro da organização uma cultura de segurança e assegurar que as boas práticas são uma componente natural do comportamento dos usuários, uma vez que eles podem provocar vulnerabilidades e eventuais danos nos ativos de informação.

Desta forma, é de fundamental importância que as organizações busquem encontrar meios de tornar o aprendizado em temas relacionados a segurança da informação no ambiente corporativo mais interessante e lúdico para seus colaboradores.

1.3 Propostas de solução para o problema

A adoção de metodologias ativas de aprendizagem combinadas ao uso de ferramentas digitais de aprendizagem seria uma estratégia eficaz no sentido de promover uma maior conscientização em Cibersegurança no universo corporativo?

No trabalho “Gamificação como solução de treinamento em Cibersegurança na Prefeitura Municipal de Esteio / RS – MOREIRA, Cassio dos Santos - AMTEC, 2019”, o autor implementou um Ambiente Virtual de Aprendizagem – AVA com técnicas de Gamificação como solução para o aumento do nível de maturidade dos colaboradores em geral, quer seja minimizando os riscos, quer seja aumentando o nível de percepção de ameaças dos usuários. Os principais problemas relatados no cenário foram: senhas fracas dos usuários e sem alterações regulares, ameaças persistentes de phishing, ataques de ransomware, e senhas anotadas em quadros e perto das estações de trabalho. O autor do estudo também relata que a própria Prefeitura de Esteio foi vítima de um ataque por ransomware, indisponibilizando 100% dos arquivos de trabalho armazenados em um servidor.

A plataforma implementava visava engajar os participantes a cumprir diferentes missões, que foram desde a execução de módulos de treinamento, não cair em e-mails phishing, reportar problemas, responder questionários, dentre outras diversas atividades. Para cada ação bem executada, o colaborador adquiria pontos e aparecia em um ranking semanal, que era exibido por todos os participantes.

O autor conclui, através de questionários e levantamentos realizados antes e depois de seu experimento, que o nível de maturidade em segurança da informação aumentou, apresentando alguns indicadores coletados:

- O número de reports à área de segurança aumentou em 260% após a jornada de treinamento, evidenciando uma postura mais proativa dos colaboradores frente às ameaças de segurança;
- Os usuários passaram a relatar incidência de SPAM - "Sending and Posting Advertisement in Mass", de forma que o responsável pela Segurança pudesse melhorar os filtros de e-mail;
- A percepção dos riscos também aumentou. Na pesquisa feita antes do treinamento, apenas 10,6% dos colaboradores informou que não aceitaria um Pendrive de terceiros devido ao risco de infecção. Após o treinamento, esse número aumentou para mais de 84%.

Além disso, o autor destaca que um dos principais atrativos revelados pelos colaboradores e que os fizeram ficar mais engajados com as atividades foi o fato da aprendizagem ter sido divertida.

No trabalho “Campanha de Conscientização em Segurança da Informação: Um Estudo de Caso, SANTOS, Rodrigues Costa - aedb.br, 2017”, o autor propõe uma campanha de conscientização em uma empresa do setor elétrico, utilizando diversos métodos audiovisuais e segmentando o público-alvo em 3 categorias: Estratégico, Tático e Operacional. O público estratégico compreendeu o presidente, os diretores e demais alto executivos da companhia. O público tático foi formado pelos chefes de departamento e divisão, além dos coordenadores de equipe e líderes de projeto e o público operacional compreendeu todos os funcionários da empresa não gerentes, técnicos, estagiários, incluindo os prestadores de serviço da companhia. O autor justificou a adoção dessa estratégia de forma a “maximizar o nível de assimilação das ações de conscientização, pois, dependendo do público, há diferença na forma com que cada um está exposto às informações sensíveis da companhia”.

O autor fez uma pesquisa para avaliar quais formatos de ação melhor contribuíram para o entendimento e fixação dos temas propostos. A ordem de preferência dos participantes foi:

1. Palestras
2. Vídeos com os colaboradores
3. Jogo virtual
4. Dicas no jornal diário
5. Cartilha de Segurança
6. Cinema com pipoca temático
7. Vitrine com ideias inovadoras para Segurança da Informação

No trabalho “Information Systems Security and Users Behavior”, PIMENTA, Alexandre Manuel Santareno – Journal of Information Systems and Technology Management, 2016”, aborda-se os aspectos relacionados a comportamento do usuário em ambiente corporativo através de pesquisa com 780 respondentes e o autor observou algumas atitudes negativas reveladas pelos usuários, como:

- A maioria já foi infetada por vírus

- Optam por senhas fáceis de memorizar, em detrimento das de construção robusta
- Utilizam a Internet na organização para fins pessoais
- Ligam dispositivos de armazenamento externo de outras pessoas aos computadores de trabalho
- Não bloqueiam o seu computador quando se ausentam

O trabalho “Segurança da Informação com ênfase na conscientização de usuários de rede, de Breustedt, BRUNO, Ricardo – Centro Universitário de Brasília, 2017”, destinou-se a estudar uma proposta para tornar o sistema de segurança da informação de um órgão público mais seguro, com ênfase na conscientização de usuários de rede.

O trabalho “Segurança da Informação VS Engenharia Social – Como se proteger para não ser mais uma vítima, ALVES, Cassio Bastos – Centro Universitário do Distrito Federal, 2010” teve como objetivo principal abordar a engenharia social no que se refere aos seus métodos, técnicas e meios utilizados pelo engenheiro social para enganar a vítima e comprometer assim a segurança da informação pessoal ou em ambientes corporativos.

1.4 Objetivo geral

Propor uma metodologia de ensino que visa desenvolver maior consciência em segurança cibernética no universo corporativo, com o objetivo de reduzir a probabilidade de ataques que exploram técnicas de Engenharia Social.

1.5 Objetivos específicos

- Aumentar o nível de engajamento dos colaboradores em programas de conscientização em segurança da informação nas organizações;
- Realizar levantamento do modelo de ensino-aprendizagem dos programas de treinamento e conscientização de organizações

brasileiras que possuem similaridade com a organização objeto de estudo;

- Criar indicadores para acompanhamento da eficácia do programa de treinamento e conscientização desenvolvido nesta pesquisa;
- Analisar as reações dos participantes dessa pesquisa, durante e após as atividades aplicadas;
- Avaliar comparativamente os resultados obtidos dessa metodologia com a metodologia tradicional utilizada pela própria organização;

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão apresentadas as concepções, conceitos e teorias que nortearam o desenvolvimento desta pesquisa.

2.1 Ameaças digitais

Com a globalização e as novas necessidades dos seres humanos, os avanços tecnológicos vêm diminuindo as distâncias, facilitando os processos e as atividades. As relações entre as pessoas tornam-se mais fáceis com o uso da internet, unindo culturas e possibilitando o intercâmbio de informações. A sociedade evoluiu, e com ela a disseminação do computador e da Internet. A rede mundial de computadores tem sido utilizada para os mais diversos fins, seja para buscar conhecimento, realizar negócios comerciais, conectar pessoas, utilizar as redes sociais e de relacionamentos, dentre outros. O advento de tecnologias como computação em nuvem, a utilização maciça de smartphones pelas pessoas e o uso de diversos aplicativos e plataformas digitais para fins pessoais ou profissionais, tem aumentando de forma significativa na última década. Paralelamente, os sistemas de informação também adquiriram grande importância para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável [BRASIL, 2007].

Ao mesmo tempo em que os avanços tecnológicos trouxeram muitos benefícios, surgiram novas demandas e as organizações tiveram que passar por transformações, de forma a resguardar os seus processos de negócio dos crimes digitais, aqueles praticados por meio da internet. O relatório Cyber Incident & Breach Trends Report 2018 divulgado pela Online Trust Alliance (OTA), traz dados contundentes sobre ataques cibernéticos. Em 2018, os danos causados pelos cibercriminosos totalizaram US$ 45 bilhões e cerca de 2 milhões de incidentes de segurança foram reportados. O relatório da OTA é baseado em estatísticas, dados e informações de várias empresas e organizações de segurança cibernética, incluindo o FBI e o Cybersecurity Ventures, dentre outras.

O relatório aponta que cerca de 95% das violações poderiam ter sido evitadas. Esse número indica que as pessoas e as empresas não se preocuparam tanto com a segurança de dados e informações quanto deveriam ou as organizações não

adotaram estratégias adequadas para a proteção dos dados. Os impactos relacionados a interrupção de sistemas, fraude ou vazamentos de dados podem gerar consequências financeiras ou danos à Figura corporativa das empresas.

Portanto, o papel da segurança da informação nas organizações é fundamental e a proteção a informações privilegiadas é essencial. A maioria das definições de Segurança da Informação (Brostoff, 2004; Morris e Thompson, 1979; Sieberg, 2005; Smith, 2002; Wikipedia, 2020) pode ser sumarizada como a proteção contra o uso ou acesso não-autorizado à informação, bem como a proteção contra a negação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas.

Na sociedade da informação (Gouveia, 2004), vale destacar os seguintes fenômenos:

- Aumento das ameaças e das vulnerabilidades tecnológicas;
- Expressiva convergência tecnológica;
- Aumento significativo de sistemas, redes de informação e sua interconexão;
- Aumento substantivo de acesso à Internet e das redes sociais;
- Aumento de velocidade e cobertura de internet;
- Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças.

A Segurança da Informação se aplica a todos os aspectos de proteção da informação ou dados, em qualquer forma. Segundo Ramos (2006, p.16), “segurança é estar livre de perigos e incertezas”. Sêmola (2003, p. 40) define que “segurança é implementar controles que reduzam o risco a níveis adequados, viáveis e administráveis”.

O nível de proteção deve, em qualquer situação, corresponder ao valor dessa informação e aos prejuízos que poderiam decorrer do uso impróprio dela. A proteção de dados nas organizações se dá através de três pilares fundamentais, que se complementam: Tecnologia, Processo e Pessoas (SOLMS, 2008). Tais pilares são comumente chamados de “Tríade de Segurança da Informação”.



Figura 02 - Tríade de Segurança da Informação

O pilar de Tecnologia se refere às soluções de segurança que as organizações adotam para tornar seus processos mais seguros. Essas soluções atuam nas mais diversas camadas da organização e visam proteger os ativos de informação. Nesse pilar estão as ferramentas de segurança como antivírus, firewall, soluções contra vazamento de informações, sistemas de cofre de senhas, ferramentas de auditoria, sistemas de detecção de intrusos, dentre outros.

O pilar de Processos se refere às políticas, normativas e procedimentos de segurança presentes na organização, que devem ser aprovados por membros da diretoria, ser de conhecimento de todos os colaboradores e seus princípios devem ser praticados pelas pessoas responsáveis. Neste pilar, estão os procedimentos de backup, criação e exclusão de credenciais de acesso, contratação de funcionários, procedimento para expurgo de arquivos e sanitização de discos de armazenamento, dentre outros.

Já o pilar de Pessoas se refere a programas de treinamento e conscientização que são executados com os colaboradores da empresa, visando aumentar suas percepções contra riscos cibernéticos e minimizar a amplitude de ataques. Neste pilar estão todas as atividades que as organizações fazem visando o desenvolvimento do colaborador em questões de segurança: Palestras, Workshops, Pílulas de conhecimento, Treinamentos e Simulações.

Apesar de uma melhor distribuição de recursos de proteção de ativos de informação nos três pilares, ainda é notório que a maior parte dos investimentos das organizações é direcionado à tecnologia e, em segundo lugar, processos. O pilar de pessoas habitualmente é tratado com certo descaso pelas organizações, direcionando menor investimento ou ações muito pontuais focadas apenas no time de segurança. Um contrassenso, haja visto que a maior parte dos incidentes de segurança da

informação nas empresas é oriundo de ataques que exploram técnicas de Engenharia Social.

A tríade da segurança da informação se baseia nos princípios da Confidencialidade, Integridade e Disponibilidade. Para cada um desses princípios, é de fundamental importância que a organização adote medidas técnicas e organizacionais para a sua proteção.

Ferreira (2003, p. 2) conceitua cada um dos aspectos:

> Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas. Integridade: salvaguarda da exatidão da informação e dos métodos de processamento. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Os principais componentes de segurança da informação são:

- **Ameaça**: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT NBR ISO/IEC 27002:2013, p.3).
- **Ativo**: Qualquer coisa que tenha valor para a organização (ABNT NBR ISO/IEC 27002:2013, p.1).
- **Risco**: Efeito da incerteza nos objetivos (ABNT ISO GUIA 73, 2013, p. 1).
- **Vulnerabilidade**: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças (ABNT NBR ISO/IEC 27002:2013, p.3).

As ameaças digitais tecnológicas são classificadas como malwares, que são softwares maliciosos “que se destinam a se infiltrar ilicitamente no sistema de um computador e danificar ou roubar informações confidenciais ou não” (VIEIRA, 2011). Eles podem estar inseridos em programas de computadores falsos, mídias removíveis, anexos de e-mails, páginas de web, entre outros. Nesse caso a importância da conscientização de usuários de rede cresce, por se tratar do agente crítico para que o ataque possa ser iniciado. Aderindo à regra usual de não abrir um anexo de e-mail que vem de uma fonte desconhecida é uma das melhores maneiras de combater o código malicioso. (HARRIS, 2013, p. 1197, TRADUÇÃO NOSSA).

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, em 2019, classificou e conceituou os malwares conforme demonstrado no quadro a seguir:

Tipo de malware	Descrição
Vírus	Programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.
Worm	Programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.
Botnet	Programa que dispõe de mecanismos de comunicação com o invasor que permite que ele seja controlado remotamente.
Spyware	Programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.
Backdoor	Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.
Trojan	Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.
Rootkit	Conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
Ransomware	Programa que criptografa os arquivos da vítima indisponibilizando o acesso a arquivos e sistemas, exigindo um pagamento em resgate para que o acesso volte ao normal

Tabela 01 – Ameaças digitais

2.2 Engenharia Social

A engenharia social é “o ato de obter acesso não autorizado a um sistema ou informações sensíveis, como senhas, através do uso de confiança e construção de relacionamento com aqueles que têm acesso a essas informações” (CHITREY; SINGH; SINGH, 2012 apud KUMAR; CHAUDHARY; KUMAR, 2015). Segundo Relatório de Ameaças da Symantec de 2019, mais de 80% dos incidentes de segurança reportados pelas organizações tiveram indícios de uso de técnicas de Engenharia Social.

O termo engenharia social passou a ficar mundialmente conhecido a partir da década de 1990, através de um famoso hacker chamado Kevin Mitnick. Esse termo

designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas, explorando a confiança das pessoas para ludibriá-las. Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. (SILVA, E., 2008).

Existem diversas interpretações dadas ao termo “Engenharia Social”. A que norteou essa pesquisa foi a seguinte:

> 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). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos. (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

As vulnerabilidades do aspecto humano são potencialmente exploradas em ataques de Engenharia Social. Destaca-se abaixo algumas características das pessoas que as tornam suscetíveis a serem exploradas através de técnicas de Engenharia Social (JUNIOR, 2016):

- Vontade de se tornar útil: O ser humano procura ser Cortez ou ajudar os outros quando necessário.
- Buscar amizades: Os humanos costumam se sentir bem ao serem elogiados, de maneira que muitas vezes ficam abertos para fornecer informações.
- Prorrogar responsabilidades: Muitas vezes o ser humano considera não ser o único responsável pelo conjunto de responsabilidades ou atividades.
- Persuasão: É caracterizada pela capacidade de convencer, buscando assim a respostas desejadas para alcançar o objetivo. Isso acontece porque o ser humano possui características que o tornam vulneráveis a manipulação.

Além disso, outra grande vulnerabilidade dentro da empresa é o próprio funcionário insatisfeito, desmotivado e desvalorizado. Todo o investimento em

tecnologia, treinamentos e conscientização, pode ser jogado fora se a companhia não cuidar e valorizar seus funcionários. (PRESCOTT, 2007).

Em se tratando do universo de ameaças digitais, os ataques de engenharia social podem ser divididos em dois grupos (PEIXOTO, 2006):

- Ataques diretos: são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas e até mesmo pessoalmente. Este exige do engenheiro social, um planejamento antecipado e bem detalhado, além de um segundo plano para caso o primeiro não dê certo, além de muita criatividade e articulação para que o plano seja bem sucedido.
- Ataques indiretos: Caracterizam-se pela utilização de softwares ou ferramentas para invadir como, por exemplo, vírus, Cavalos de Troia (trojan) ou através de sites e e-mails falsos para assim obter informações desejadas.

A Figura 03 demonstra, de forma ilustrativa, como os atacantes conseguem obter informações sobre um ambiente computacional, com o objetivo de direcionar um ataque a uma organização específica.

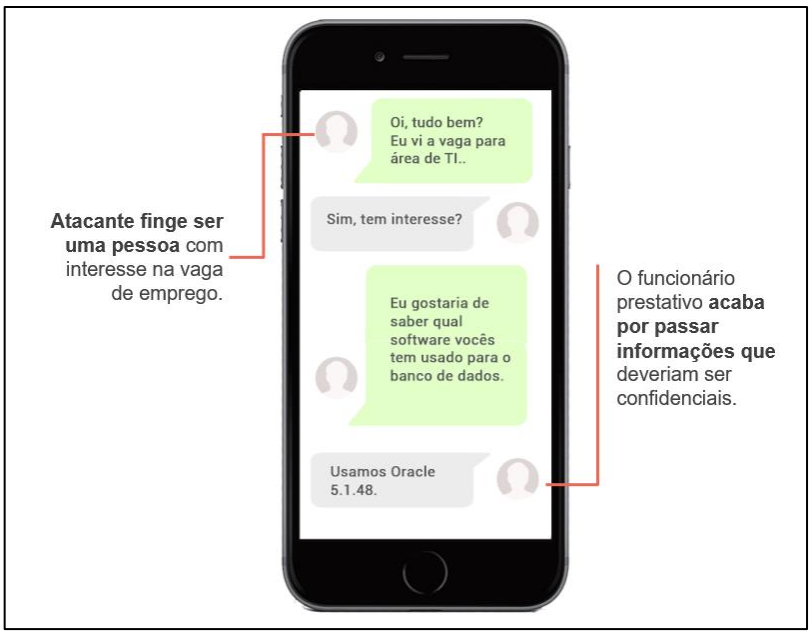


Figura 03 – Exemplo de Engenharia Social

A vertente de ataques indiretos cresceu exponencialmente na última década, muito por conta da possibilidade de expressivos ganhos financeiros dos atacantes, especialmente motivados por ataques do tipo “Ransomwares”.

O principal vetor de ataque do tipo Ransomware, envolve a utilização de e-mails phishing, que se trata de um falso e-mail com o objetivo de ludibriar o destinatário, seja por uma oferta exclusiva, a necessidade de instalação de algum componente no Sistema Operacional para continuar usando algum serviço, ou trazendo alguma informação confidencial, a qual a vítima só terá acesso se executar um clique no e-mail. Todos os links e arquivos anexados em e-mail, entretanto, apenas direcionam a instalação de agentes maliciosos, que visam causar algum dano nos sistemas computacionais da organização.

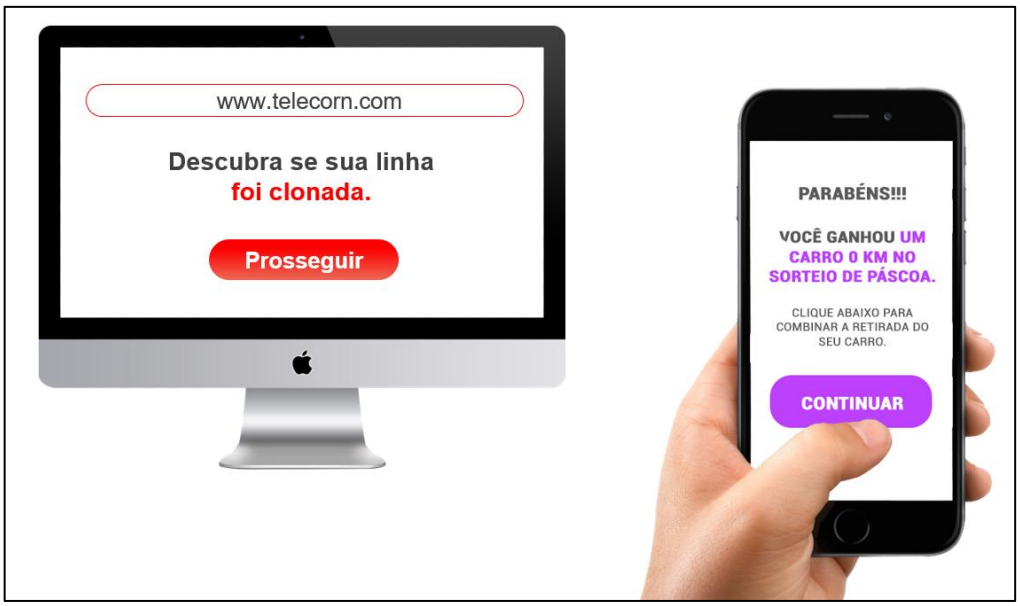


Figura 04 – Engenharia social através de phishing

Em caso de infecção por Ransomware, a organização pode ter seus arquivos inacessíveis e seus sistemas completamente inutilizáveis, em que o atacante, criptografia os arquivos, impossibilitando sua aberta, e exige pagamento em criptomoedas, para liberar o acesso.



Figura 05 – Forma de comunicação à vítima em infecções por Ransomware

Os ataques do tipo Ransomwares tem gerado grande preocupação das organizações, haja visto que gera um impacto imediato em suas operações em caso de infecção.

De: "Smartden" <smartden@protonmail.com>
Enviada: 2019/06/24 12:18:03
Para: DH
Assunto: Re: 1CB5A86425091865

Hello!
Don't worry, we can help you to restore your servers to initial state.

If you want to be sure that we can decrypt your data,
you can send us up to 3 small encrypted files for free test decryption!
After decryption process we can help you to improve security of your it-infrastructure.

You have to pay in Bitcoin cryptocurrency.
Price of decryption tool and your decryption key { 1CB5A86425091865}
is: 0.6 BTC
If you pay within 48 hours we will make a discount
to: 0.5 BTC
Our BTC Wallet: 1JAyw6EYMRhrTbXLjKAFSfmSTkqSkYqUzh
If you want to fix the price please start the dialog!

========== HOW TO BUY BITCOIN ==========
You can easily buy BTC in your country on http://localbitcoins.net
1. Make registration
2. Find BTC seller in your country. They speak on your language, so they can help you.
3. Buy BTC from seller

Figura 06 – Fragmento de e-mail enviado pelo criminoso extorquindo a vítima

2.3 Cultura em Cibersegurança

Na reunião da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) ocorrida em março de 2009, foi realçado o tema Cultura de Segurança como vetor estratégico das Nações, e os seguintes aspectos foram colocados em evidência:

- Cada parte envolvida tem um importante papel para assegurar a segurança em função de suas competências, e devem ser sensibilizados sobre os riscos associados à segurança de sistemas e redes de informação;
- As questões de segurança devem ser objeto de preocupação e responsabilidade de todos os atores, seja governamental, empresarial, e de outros (pesquisa e terceiro setor)

Aliado aos mecanismos de segurança implementados pela organização para a proteção de seus ativos, é fundamental que os colaboradores façam uso de boas práticas em segurança. De acordo com (Kruger & Kearney, 2008) e (Albrechtsen, 2007), os usuários devem, além dos mecanismos de segurança definidos, adotar as seguintes medidas de segurança no seu posto de trabalho:

- Aplicar as atualizações de segurança recomendadas
- Utilizar senhas robustas e diferentes em cada aplicação
- Procurar transferir informações de forma encriptada, sempre que possível
- Não compartilhar ou divulgar as suas senhas com os outros
- Ser responsável e cuidadoso na utilização da Internet e do correio eletrônico
- Informar no caso de incidentes com vírus, roubos ou perdas de informação
- Estar ciente que todos os atos praticados têm consequências
- Bloquear o computador quando se ausentar
- Não utilizar software ilegal ou de compartilhamento de arquivos.



Figura 07 – Ação de conscientização em cibersegurança em ambiente corporativo

A questão predominante é que, apesar das organizações adotarem procedimentos de segurança na proteção de seus ativos, é preciso contar com os colaboradores para que a proteção seja efetiva. Segundo (Workman, Bommer, & Straub, 2008), a principal ameaça à segurança é a falta de consciencialização dos usuários para esta questão, uma vez que existem medidas de segurança disponíveis que podem ser aplicadas, mas estes ignoram-nas, deixando que sejam provocados ataques e violações à segurança dos SI nas organizações.

2.4 Metodologias ativas de aprendizagem

É possível constatar que um aprendiz de um treinamento corporativo é diferente de um aluno da educação formal. Enquanto o primeiro grupo precisa dimensionar o tempo entre as atividades propostas por um instrutor com as rotinas inerentes à sua função nas organizações, o segundo dedica-se um pouco mais às atividades propostas pelo professor. Por isso, a utilização de técnicas relacionadas a metodologias ativas de aprendizagem é fundamental para que os estudantes de um treinamento corporativo estejam engajados nas atividades propostas. Isso pode ser conseguido se o colaborador se sente parte integrante do processo de ensino-aprendizagem.

A linha de pensamento de (SIEMENS, 2014) considera um contexto em que o aluno deve ser incentivado a buscar seu próprio conhecimento, ser responsável por construir seu aprendizado e se desenvolver em um cenário educacional moderno. Já para Vygotsky (2008), o aprendiz é um ser ativo, real, concreto, em permanente transformação e que interage com o meio que o cerca. Este sujeito é formado dentro de um ambiente cultural definido historicamente, sendo então um produto das ações sociais deste meio.

O processo de aprendizagem pode ser entendido como um ciclo que ocorre a partir do objetivo de se produzir algum conteúdo, onde haja interação entre a nova informação e o conhecimento anterior. Neste sentido a existência de um contexto é fundamental, pois a partir dele será possível transformar a informação em conhecimento.

As práticas em um ambiente de aprendizagem devem buscar o envolvimento dos participantes nas atividades propostas, estimulando a interação permanentemente e destacando a importância que a presença e a colaboração do dos outros participantes são imprescindíveis para a construção do conhecimento, assumindo que “às vezes, cumprem o papel dele” (SCHÖN, 2000, p. 40). Nesse processo, valoriza-se a experiência pessoal, que transforma a aprendizagem em uma atividade satisfatória, que favorece as competências sociais, o pensamento crítico e fortalece o respeito mútuo.

O advento das tecnologias educacionais favorece a aplicação das metodologias ativas de aprendizagem, uma vez que o professor passa a possuir uma série de recursos tecnológicos para implementar as técnicas possíveis em que o aprendiz passa a fazer parte essencialmente da construção de seu conhecimento. Para John Dewey, que utilizava o método ativo de aprendizagem no século passado, o ensino deveria proporcionar a formação de cidadãos com competências e habilidades adequadas à realidade. Tal processo de ensino-aprendizagem deveria ocorrer apoiado em metodologias do tipo “aprender fazendo” ou “learning by doing”, também conhecida como “hands-on” (DEWEY, 1944).

Há diversas técnicas de ensino-aprendizagem baseadas em metodologias ativas de aprendizagem e que são objeto desta pesquisa. Um dos métodos utilizados, por exemplo, trata-se da Aprendizagem baseada em Problemas (Problem Based Learning – PBL), (Da Silva Batista (2019). Nesse método, são utilizados problemas

como meio para ensinar e aprender, o aprendizado passa a utilizar o aluno como protagonista do conhecimento, deixando se ser ator passivo, para ser agente ativo de seu aprendizado. O professor assume então o papel de orientador ou mediador nos grupos de trabalho e a relação entre aprendiz-professor torna-se muito mais intensa do que em atividades puramente expositivas. Essa metodologia favorece também a interação entre as pessoas, uma vez todos estão unidos em prol de um objetivo, que é o de propor soluções para um problema apresentado.

Há diversas outras técnicas de metodologias ativas de aprendizagem, sendo que todas elas, em geral, buscam colocar o aluno como protagonista de seu processo de aprendizagem e visam promover um engajamento maior nas atividades propostas. As características das metodologias usadas nesta pesquisa estão descritas abaixo:

- **Ensino Híbrido**: O Ensino Híbrido é um modelo de educação que também entra na categoria de exemplos de metodologias ativas. Ele se caracteriza por mesclar dois modos de ensino. O online, que se trata do modelo de ensino em que o aluno possui controle sobre algum elemento do seu estudo na escola ou fora dela, como o tempo, modo, ritmo ou o local e o offline ou presencial, que é o modelo de ensino que é necessariamente realizado em algum espaço físico unindo todos os participantes. Nesse sentido, a ideia é que para o Ensino Híbrido, os modos online e offline devem se complementar, proporcionando diferentes formas de ensinar e aprender.
- **Estudo de caso**: Essa opção de metodologia ativa começa com o professor apresentando um exemplo de situação real que os estudantes devem resolver. O estudo de caso ajuda os alunos a aprender a solucionar cenários complexos e adquirir conhecimento em questões práticas, tornando o processo de ensino-aprendizagem mais interativo e significativo
- **Gamificação**: Trata-se da utilização de elementos de jogos em situações relacionadas à educação. Essa metodologia geralmente é utilizada para gerar maior engajamento dos estudantes, motivando suas ações e promovendo a aprendizagem ou a resolução de problemas de forma criativa. Nela, o professor precisa “gamificar” os aspectos normais de determinada matéria, associando com o mundo dos jogos para engajar mais os participantes.

- **Sala de aula invertida**: Originária do termo em inglês Flipped classroom, propõe uma inversão nas aulas tradicionais. Assim, os alunos também devem ler o conteúdo em casa, para que o encontro em sala de aula seja dedicado a discussões e resolução da matéria estudada. Além disso, a sala de aula invertida também ajuda a promover maior dinamismo no ensino, uma vez que reduz a quantidade de aulas expositivas e teóricas feitas somente pelo professor.
- **Mão na massa – Hands On**: O método de mão na massa é uma excelente ideia para despertar a autonomia, criatividade, senso crítico, proatividade e outras qualidades que podem ser essenciais para os estudantes. O fato de fazer com que o participante produza algo, já faz com que ele se empenhe mais em sua construção de saber e consequentemente tenha uma melhoria quanto à fixação dos conhecimentos.

3 MÉTODO

Nesta seção será apresentada a metodologia de pesquisa, o perfil dos participantes, os meios e procedimentos adotados.

3.1 Metodologia

A metodologia adotada nesta pesquisa é de abordagem qualitativa, com a coleta de dados quantitativos ao longo do seu desenvolvimento. A pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social (GOLDENBERG, 1997, p. 34).

Nesta pesquisa assumiu-se o enfoque qualitativo, visto que o pesquisador manteve contato direto com o ambiente, os participantes e o objeto de estudo em questão, realizando um trabalho de campo intensivo, onde foram analisados o engajamento e o aproveitamento dos participantes frente às atividades propostas. Além disso, foi feito comparativo entre indicadores de comportamento dos colaboradores antes e após a aplicação do estudo de caso.

O método foi dividido em 10 etapas:

- Etapa 1: Delineamento da pesquisa
- Etapa 2: Levantamento da fundamentação teórica
- Etapa 3: Levantamento exploratório
- Etapa 4: Mapeamento do ambiente
- Etapa 5: Criação do Programa de treinamento (Ebook e Sequência Didática)
- Etapa 6: Criação de indicadores de eficácia do programa
- Etapa 7: Execução do programa de treinamento
- Etapa 8: Avaliação de reação
- Etapa 9: Aferição da eficácia do programa de treinamento
- Etapa 10: Consolidação e análise dos resultados

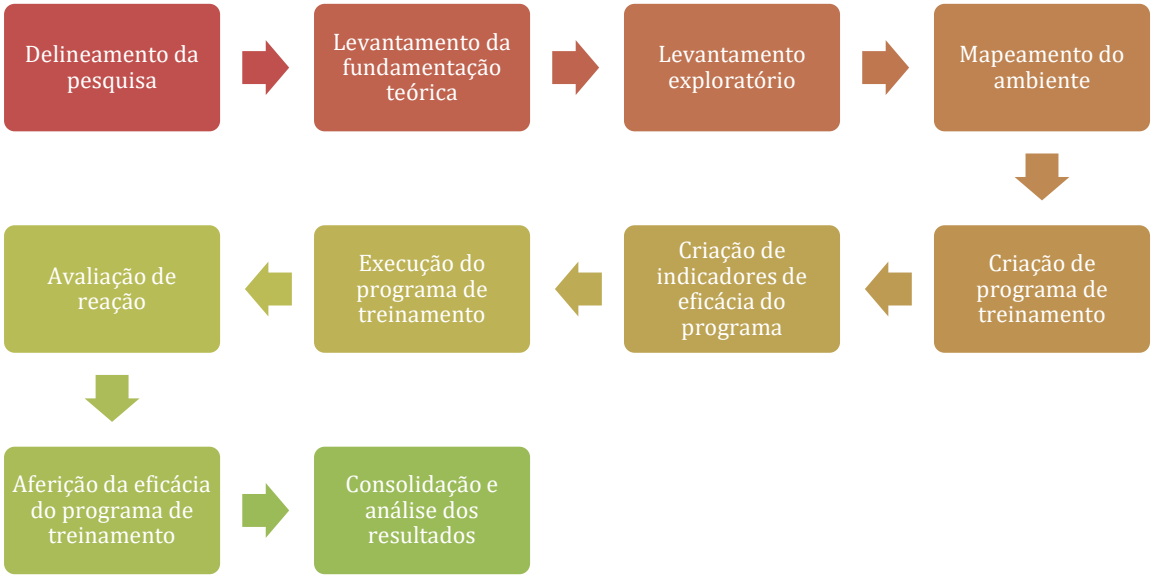


Figura 08 - Caminho metodológico da pesquisa

3.2 Levantamento exploratório

Esta etapa teve como objetivo fazer um levantamento qualitativo da maneira como as organizações brasileiras desenvolvem programas de treinamento e conscientização em segurança da informação e de que forma mensuram os resultados de suas ações. Este levantamento exploratório da pesquisa, baseou-se em um formulário de perguntas e respostas, onde foram investigadas características relacionadas ao formato, carga horária, principais motivadores das ações e resultados de seus programas. Foi aplicado um questionário online denominado “Ações de conscientização em Cibersegurança em ambiente corporativo” para um grupo de 28 líderes de Segurança Digital em suas empresas estabelecidas em território brasileiro, assumindo a função de Gerente de Segurança da Informação, Gerente de Riscos e Compliance, Gerente Executivo de Tecnologia e Segurança da Informação, Diretor de Segurança da Informação (Chief Information Security Officer - CISO), dentre outros cargos correlatos.

O ramo de atuação das empresas entrevistadas foi: Comércio e Varejo (6 empresas), Transporte, Comunicação e Serviços Públicos (4), Indústria (3), Serviços

(3), Utilities (3), Educação (2) Agronegócio, Alimentos e Bebidas (2), Tecnologia da Informação (2), Saúde (1), Construção e Engenharia (1) e Finanças (1).

O questionário aplicado foi composto por 15 perguntas fechadas, relacionadas aplicação das atividades de treinamento e conscientização em segurança da informação dos colaboradores e terceirizados da empresa As respostas do questionário foram analisadas utilizando estatística simples por frequência absoluta.

Perguntas do questionário "Ações de conscientização em Cibersegurança em ambiente corporativo"	
01	Qual o segmento de atuação de sua empresa?
02	A sua empresa possui um Sistema de Gestão de Segurança da Informação (SGSI)?
03	Qual a quantidade de colaboradores que estão dedicados exclusivamente a atividade de Segurança da Informação?
04	Qual o faturamento anual da organização
05	Qual o Budget de Segurança da Informação para 2020?
06	Como os colaboradores tomam conhecimento das Políticas e Normativas de Segurança da Informação da organização?
07	Na fase de ambientação de novos colaboradores, a organização inclui um Onboarding de Segurança da Informação?
08	Quantos incidentes de segurança da informação a sua empresa foi vítima nos últimos 12 meses?
09	As vulnerabilidades do aspecto humano (engenharia social) são exploradas pelos atacantes nos ataques cibernéticos que sua organização sofreu nos últimos 12 meses?
10	Como são feitos os treinamentos e as campanhas de conscientização em segurança da informação para os colaboradores?
11	Quais são os motivadores principais para que a organização realize treinamentos e campanhas de conscientização para seus colaboradores?
12	De que forma a organização conscientiza seus colaboradores quanto aos riscos de segurança?
13	Qual a carga horária média anual de treinamento que a organização oferece anualmente aos colaboradores?
14	A organização utiliza metodologias ativas em seus programas de treinamento e conscientização (Sala de aula invertida, Aprendizagem baseada em problemas, Ensino Híbrido, Gamificação e Hands-On)?
15	Após as ações de treinamento e conscientização em segurança realizadas pela organização, qual a sua percepção quanto ao comportamento dos colaboradores?
16	Há uma clara percepção de valor da alta direção quanto aos programas de treinamento e conscientização em segurança da informação?

Tabela 02 – Perguntas do questionário

Os resultados deste levantamento serão apresentados no capítulo 4 desta dissertação. Vale ressaltar que estes dados subsidiaram a necessidade de criação de indicadores para avaliar a eficácia do programa de conscientização utilizando metodologias ativas de aprendizagem proposto nessa pesquisa.

3.3 Mapeamento do ambiente

A organização que serviu de base nesse estudo é uma companhia multinacional do ramo de telecomunicações, estabelecida no Brasil e que oferta serviços de telefonia e internet fixa e móvel, já em pesquisa avançada para a implantação do 5G em todo o território nacional. A organização possui mais de 8 mil colaboradores e prestadores de serviço. Há um staff de 34 colaboradores que gerenciam as operações de segurança da informação em toda a empresa.

A organização realiza treinamentos regulares para seus colaboradores, sendo a área de Recursos Humanos, responsável por gerenciar as atividades dos treinamentos. O tema “Segurança da Informação” também é abordado nessas ações. Os assuntos dos treinamentos dessa vertente são definidos pela área de Cyber Security, que indica quais são aqueles mais importantes serem tratados para a capacitação dos colaboradores.

Durante a pesquisa, foi identificado que, apesar da organização realizar treinamentos regulares, os temas não conversam entre si e não possuem indicadores que permitem o acompanhamento de sua eficácia. Os treinamentos para os colaboradores de forma geral são sempre de curta duração (2 horas), independente do conteúdo explorado, o que promove a falta de aprofundamento em temas importantes. Também foi identificado que os cursos acontecem sem considerar o conhecimento prévio dos participantes. Não há interação e não há participação efetiva dos colaboradores, que apenas acompanham a passagem de slides pelo instrutor. De forma geral os cursos também não promovem uma imersão considerando o ambiente de trabalho dos colaboradores. Do contrário, trazem os assuntos de forma genérica, e, muitas vezes, considerando segmentos diferentes da organização. Todos os treinamentos ficam armazenados em repositório virtual da organização, em que os colaboradores podem ter acesso a qualquer momento.

3.4 Criação do programa de treinamento

Esta etapa da pesquisa teve como objetivo o desenvolvimento de um programa de treinamento integrado às metodologias ativas de aprendizagem e que possibilitasse o uso de recursos e ferramentas digitais, com o objetivo de criar um ambiente de colaboração e interação social no processo de ensino-aprendizagem durante as atividades propostas. A partir do mapeamento do ambiente, foi definido que o modelo de aprendizagem seria híbrido, sendo a maior parte considerando educação a distância e os colaboradores utilizando seus dispositivos móveis e notebooks como principais meio para acesso a materiais de estudo.

O programa de treinamento em segurança da informação foi criado em formato de Workshops de 24 horas totais, em sessões de 3 horas de duração. Os encontros aconteceram 2 vezes por semana, durante o horário de expediente dos colaboradores. A dinâmica dos encontros foi construída de maneira a propiciar interação e colaboração dos participantes em diversos momentos de cada dia de atividade, seja através de Estudos de Caso, Desafios, Práticas e aplicação de Sala de Aula Invertida.

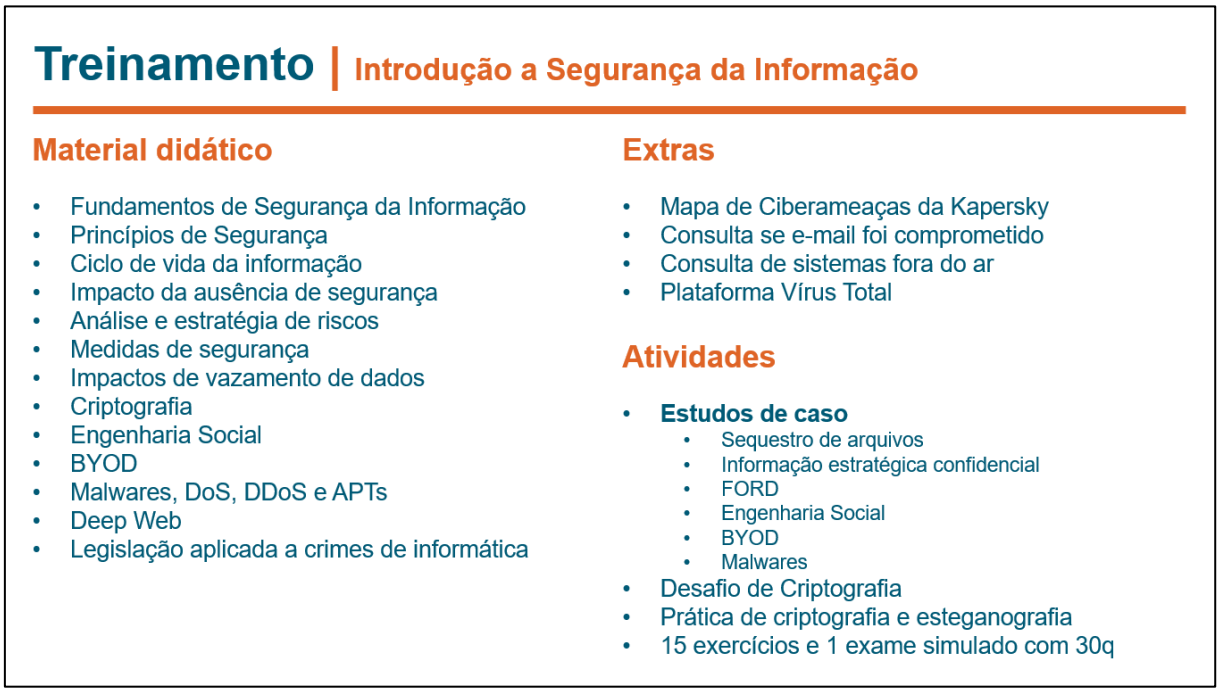


Figura 09 – Programa de treinamento

As tecnologias utilizadas para a realização desse programa de treinamento e suas principais características estão descritas a seguir.

- **Cisco Webex[1]:** é uma plataforma de videoconferências e reuniões a distância. O recurso, que pode ser acessado via desktop e celulares, dispensa download de programas para entrar em reuniões, basta acessar um link enviado por e-mail. Além disso, é compatível com navegadores como o Chrome, Internet Explorer, Firefox e Safari. A versão paga permite até 200 participantes simultâneos
- **Mentimeter[2]:** é uma plataforma online para criação e compartilhamento de apresentações de slides com interatividade. O serviço, disponível em planos gratuitos e pagos, possibilita que profissionais de diversas áreas, como instrutores e professores, criem apresentações complexas. A ferramenta oferece recursos interativos, como nuvem de palavras e questionários, que podem ser compartilhadas via Internet com seu público.
- **Kahoot[3]:** é uma plataforma de aprendizado baseada em jogos, usada como tecnologia educacional em escolas e outras instituições de ensino. Seus jogos de aprendizado, "Kahoots", são testes de múltipla escolha que permitem a geração de usuários e podem ser acessados por meio de um navegador da Web ou do aplicativo Kahoot.
- **OnlineQuizCreator[4]:** é uma plataforma que permite criar rapidamente seus próprios quizzes. Eles são divertidos de jogar, têm diversos recursos, opções de estilo e dados estatísticos que podem ser utilizados durante sessões de aprendizagem.
- **Microsoft Teams[5]:** plataforma desenvolvida para a colaboração de equipes. O conceito inicial do aplicativo foi desenhado para colaboração de equipes corporativas, mas ultimamente tem sido utilizado também para fins educacionais.
- **Microsoft Power BI[6]:** é um serviço de análise de negócios da Microsoft que tem o objetivo de fornecer visualizações interativas e recursos de business intelligence

[1] https://www.webex.com/pt/
[2] https://www.mentimeter.com/
[3] https://kahoot.it/
[4] https://www.onlinequizcreator.com/
[5] https://www.microsoft.com/pt-br/microsoft-teams/
[6] https://powerbi.microsoft.com/pt-br/

com uma interface simples para que os usuários finais criem os seus próprios relatórios e dashboards.



Figura 10 – Ambiente de ensino

A escolha das ferramentas tecnológicas considerou como requisitos: a disponibilidade de versões gratuitas, versões amigáveis a dispositivos de diferentes tamanhos e resoluções e às plataformas e ferramentas já homologadas pela organização que foi objeto desta pesquisa.

3.5 Criação de indicadores de eficácia do treinamento

Conforme já descrito no tópico 3.3 – Mapeamento de ambiente, a organização objeto desse estudo já realizava treinamentos regulares em segurança da informação para seus colaboradores e os avalia através de “Avaliações de Reação”, em que os colaboradores podem informar sua satisfação das atividades sob os mais variados aspectos, pontuando os instrutores, o conteúdo e o formato dos treinamentos.

Apesar de servir como um instrumento útil para avaliar a qualidade dos treinamentos, a Avaliação de Reação não mede a eficácia do programa, que relacionado ao tema desta pesquisa, está intrinsicamente relacionada à adoção de um comportamento mais adequado pelos colaboradores ao utilizar os diversos meios computacionais para realização de suas atividades, sem colocar a organização em

risco. Esse comportamento mais adequado está relacionado às Boas Práticas que os colaboradores devem adotar conforme mencionado no tópico 2.3 – Cultura em Cibersegurança.

Por outro lado, durante o mapeamento do ambiente, foi identificado que ela realiza testes recorrentes de e-mail phishing para todos os colaboradores e terceirizados que possuem e-mail corporativo da instituição. Esses testes são disparados pela área de Cyber Security, sempre com uma temática diferente, quer seja, um e-mail que pareça institucional, outro que pareça uma promoção de um restaurante de renome, outro relacionado a informação de dados cadastrais para ter direito a um desconto em período da Black Friday, dentre outros.

A Figura 11 representa o resultado de um e-mail phishing para quase 4 mil colaboradores. O procedimento esperado por eles seria encaminhar o e-mail para uma Lista de Distribuição específica para tratar o tema. No entanto, apenas 4,5% das pessoas fizeram o procedimento esperado. Praticamente 1 em cada 3 pessoas que visualizaram o e-mail fizeram um procedimento indevido, que foi clicar no link indicado no e-mail. Destes, quase 300 colaboradores ainda informaram seus dados pessoais no website destino do link. São mais de 1 mil pessoas que colocariam a organização em risco, caso o destino do link fosse algum programa malicioso, podendo causar algum tipo de interrupção nos serviços da companhia.

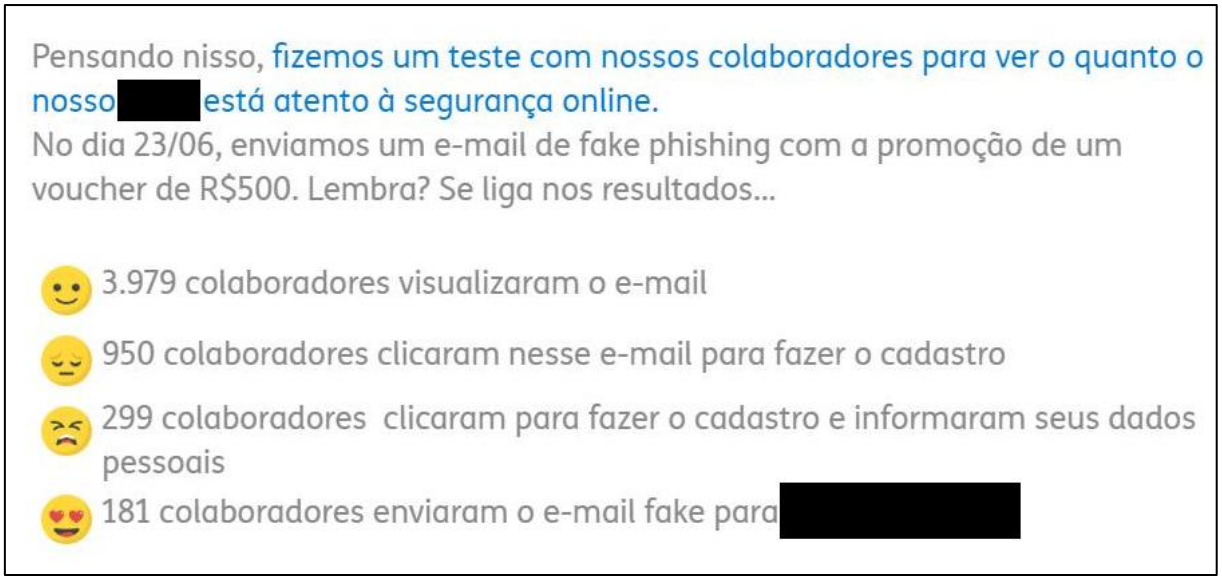


Figura 11 – Resultado de e-mail phishing

A organização não faz correlação destes testes simulados de e-mail phishing com as ações de treinamento e conscientização, tornando-se assim, ações apartadas, apesar de serem gerenciadas pelas mesmas áreas envolvidas.

Como a organização mantém um histórico do resultado do comportamento dos colaboradores nas simulações de e-mail phishing, este pesquisador considerou esse indicador como uma métrica adequada para avaliar a eficácia do programa de treinamento e conscientização que foi implementado na organização. Foi definido que o comparativo será da média histórica comportamental que a organização já possui com os resultados de indicadores após as ações do programa de treinamento.

3.6 Execução do programa de treinamento

O programa de treinamento foi composto pela produção de um ebook e uma Sequência Didática (SD) e foi direcionado para colaboradores da área de Operações de Network de uma grande companhia de telecomunicações, com presença mundial. Ao todo, foram impactados 195 participantes, sendo colaboradores diretos ou terceirizados, situados em todo o território nacional.

Durante todo o programa de treinamento e conscientização em segurança da informação, buscou-se executar as atividades de forma dinâmica, interativa e solicitando a participação dos colaboradores, tangibilizando os conteúdos ministrados e práticas aplicadas, aos desafios reais do dia a dia dos colaboradores. As atividades levavam tinham os seguintes objetivos:

- Despertar interesse dos colaboradores, engajando-os na realização das atividades propostas;
- Discutir sobre os desafios reais da organização trazidos por eles;
- Fazer com que eles se motivassem a buscar conhecimento prévio por conta própria, visando a aplicação da sala de aula invertida;
- Permitir análises cocriadas e estimular debates sobre o tema.

Como exemplo da abordagem adotada, pode-se comparar o ensino de Gestão de Riscos tradicional com o método utilizado nessa pesquisa. Normalmente um curso de Gestão de Riscos aborda essencialmente o que está descrito nas Normas de Risco internacionalmente conhecidas. Como exemplo, cito a ABNT NBR ISO 31000, que apresenta princípios e diretrizes para a Gestão de Riscos de forma geral e a ABNT NBR ISO 27005, que traz diretrizes para a Gestão de Riscos Cibernéticos, um dos temas dos Workshops ministrados neste programa de treinamento.

A Figura 12 faz parte do processo de Gestão de Riscos de Segurança da Informação, alinhado com as normas citadas. Na abordagem tradicional, essa ilustração é utilizada pelo instrutor para explicar todo o ciclo de vida do risco da organização, eventualmente citando exemplos. No entanto, ao trazer uma abordagem puramente teórica, torna-se mais difícil para o participante reconhecer os riscos em sua organização. A teoria não o ajuda significativamente a compreender de que forma os riscos podem ser gerenciados.

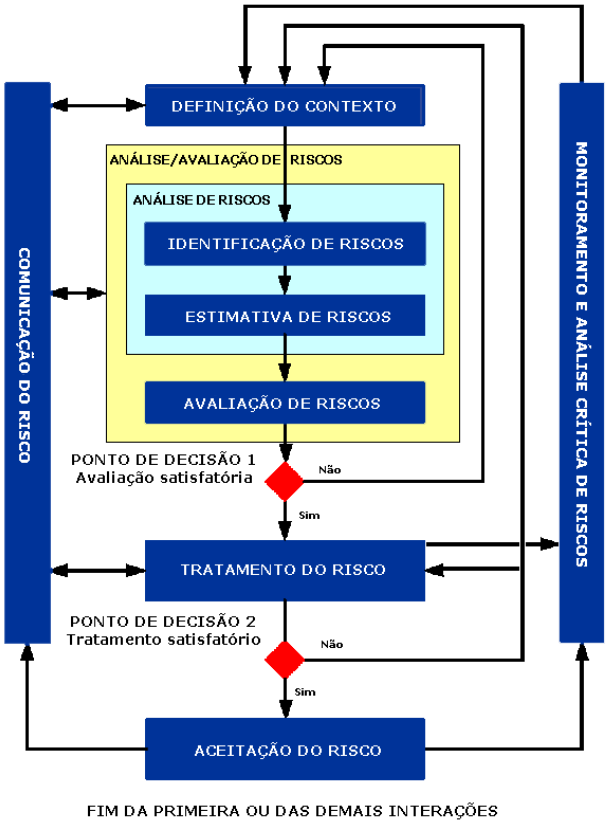


Figura 12 – Processo de Gestão de Riscos conforme ISO 31000

Já na abordagem proposta nesta pesquisa, a ilustração anterior foi enviada aos participantes previamente ao encontro onde estariam discutindo os riscos da organização. Foi solicitado que eles fizessem a leitura de algumas páginas que envolviam o processo de Gestão de Riscos e quando estiveram presentes no encontro, a atividade ocorreu de maneira totalmente prática, com eles executando toda a sequência de avaliação de riscos considerando o seu ambiente diário de trabalho.



Risco Identificado	Fator Consequência	Fator Exposição ao Risco	Fator Probabilidade	Grau de Criticidade	Medida Preventiva para evitar Risco	Investimento
Falta de energia elétrica no Datacenter	Grave	Uma vez por semana ou ao mês, ocasionalmente.	Coincidência se acontecer	Correção imediata – risco tem que ser reduzido	Instalar um Gerador de energia elétrica	R$ 100.000,00
Interrução no link de internet	Grave	Haramente possivel, sabe-se que ocorre, mas não com frequência	Coincidência se acontecer	Risco deve ser monitorado	Instalar link redundante	R$ 10.000,00
Infecção por ransomware	Grave	Uma vez ao ano ou ao mês, irregularmente.	Coincidência se acontecer	Correção urgente – requer atenção	Adquirir ferramenta de proteção avançada	R$ 250.000,00
Exclusão de arquivos por funcionário desligado	Moderado	Remotamente possível, não sabe se já ocorreu	Completamente possível - 50% de chance	Risco deve ser monitorado	Adotar política de backup eficiente	R$ 6.000,00
Acesso indevido ao sistema tarifário	Severo - Prejuízos	Haramente possivel, sabe-se que ocorre, mas não com frequência	Espera-se que aconteça.	Correção imediata – risco tem que ser reduzido	Revisar acessos de sistemas críticos	R$ 80.000,00

Figura 13 – Atividade colaborativa de Gestão de Riscos

Essa atividade de Avaliação de Riscos foi executada no Microsoft Teams, permitindo a participação simultânea de dezenas de colaboradores.

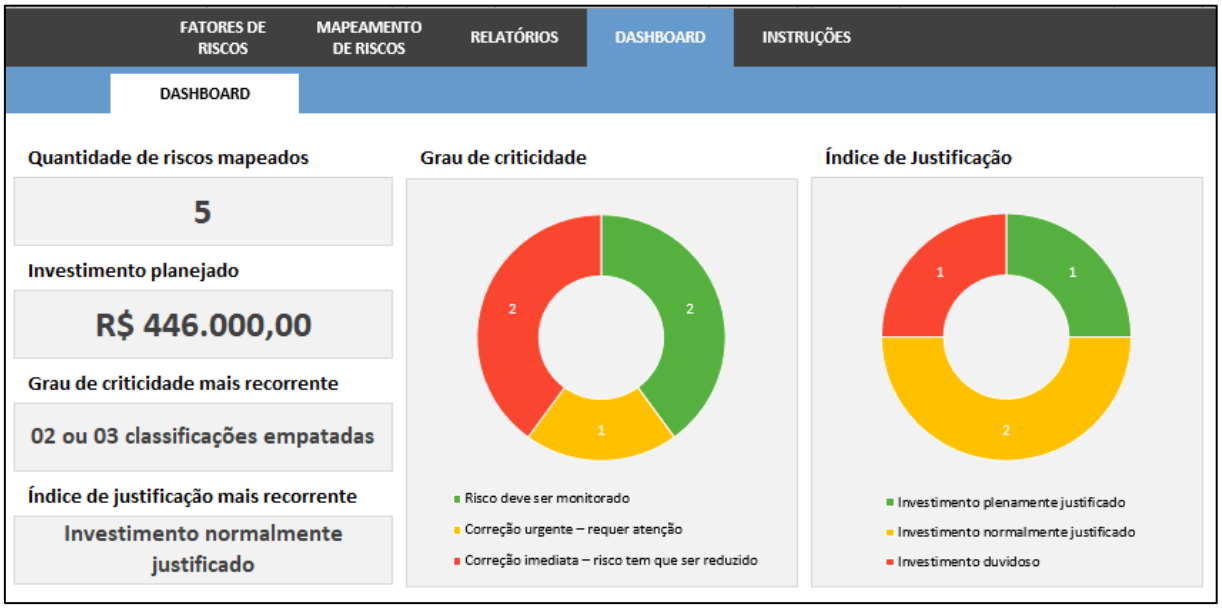


Figura 14 – Consolidado da atividade de Gestão de Riscos

3.7 Avaliação de Reação

Para o acompanhamento do programa de treinamento e conscientização em cibersegurança, foram criados indicadores educacionais que mediam a performance das atividades como um todo. Esses indicadores foram coletados através de Avaliações de Reação em que os participantes respondiam através de Questionários pelo Microsoft Forms sempre quando o treinamento alcançava 50% e ao seu término.

Os questionários tinham respostas fechadas e abertas e, quando respondidos pelos participantes, alimentavam visões gerenciais que podiam ser acompanhadas pelos Gerentes e Executivos através de Dashboards do Power BI.

Através da Avaliação de Reação, os participantes podiam compartilhar suas impressões quanto ao conteúdo, ao formato dos treinamentos, à dinâmica do instrutor, a importância daquele tema para seu dia a dia no trabalho e se ele se sentia mais preparado para lidar com as ameaças cibernéticas.

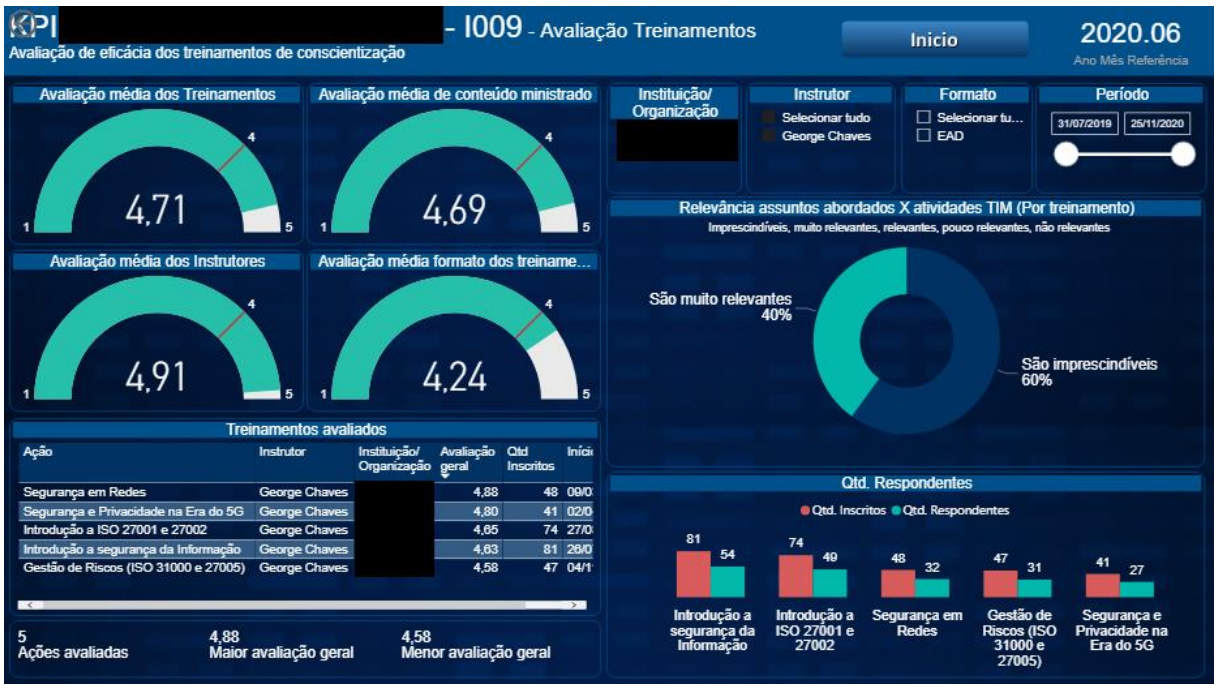


Figura 15 – Dashboard gerado a partir de avalições de reação

3.8 Aferição da eficácia do programa de treinamento

Conforme descrito no tópico 3.5 – Criação de indicadores de eficácia do treinamento, a principal métrica utilizada para avaliar a eficácia do programa de treinamento proposto nesta pesquisa foi o resultado das ações dos colaboradores através das simulações de e-mail phishing executadas pela organização.

Antes do início do programa de treinamento e conscientização proposto nesta pesquisa, o comportamento dos colaboradores frente ao e-mail falso que a organização disparou foram coletados com a área de Cyber Security. Ao todo, a organização já tinha enviado 4 e-mails phishing. Os resultados de cada um deles encontra-se na tabela a seguir.

Ação adotada pelo colaborador	**Simulações**			
	1	**2**	**3**	**4**
Não fez nada	1456	1698	2.549	2976
Clicou no link	1143	1092	950	191
Clicou no link e inseriu dados pessoais	150	50	299	378
Relatou o e-mail phishing (AÇÃO ESPERADA)	189	307	181	577
TOTAL DA AMOSTRA	**2.938**	**3.147**	**3.979**	**4.122**

Tabela 03 – Resultados de simulação de e-mail phishing antes do experimento

A tabela mostra que a organização vem impactando cada vez mais colaboradores com suas simulações de e-mail phishing. O comportamento esperado do colaborador nessas situações é relatar o e-mail à uma Lista de Distribuição específica para tratar casos como esse. A média desse comportamento considerando as quatro simulações é de 9%. Já os colaboradores que não adotam o procedimento esperando, mas por outro lado não realizam nenhuma ação que coloque a organização em risco, tem uma tendência de alta, sendo a última simulação atingindo 72% dos colaboradores. Considerando as 4 simulações, foram registradas 4.253 ações indevidas dos colaboradores, o que representa uma média de 16% de comportamento que colocaria a organização em risco. No entanto, o número de colaboradores que tomaram ações indevidas, vem reduzindo com a continuidade das simulações da organização, indo de 44%, 37% 32% e, finalmente, 13% na última simulação registrada antes do início do programa de treinamento proposto.

O objetivo do programa de treinamento e conscientização em segurança da informação proposto nesta pesquisa é tornar os colaboradores mais conscientes frente aos riscos cibernéticos e fazê-los adotar uma postura mais proativa frente às ameaças à segurança. Assim, o resultado de novas simulações de e-mail phishing foi registrado e comparado entre os colaboradores que não participaram do treinamento com aqueles que estiveram presentes nas atividades realizadas.

3.6 Consolidação e análise dos resultados

A última etapa desta pesquisa envolve a consolidação e análise dos resultados gerados pela pesquisa, originadas pelas várias atividades associadas, sendo (1) Levantamento exploratório, onde se objetivou compreender melhor o problema e direcionar adequadamente o desenvolvimento deste trabalho; (2) Avaliação de Reação, consolidando as respostas dos participantes das atividades desenvolvidas durante todo o plano de treinamento e conscientização em cibersegurança e (3) Comparativo de indicadores de comportamento, avaliando se as ações propostas contribuíram para um comportamento mais alinhado às boas práticas pelos colaboradores participantes do treinamento.

4 RESULTADOS E DISCUSSÕES

Esta seção tem por objetivo apresentar os resultados da pesquisa, desde o seu levantamento exploratório até a experimentação do objeto tecnológico.

4.1 Resultados do levantamento exploratório

Conforme descrito no tópico 3.2 – Levantamento exploratório, inicialmente esta pesquisa contou com a aplicação de um questionário composto de 15 perguntas, denominado “Ações de conscientização em Cibersegurança em ambiente corporativo” para um grupo de 28 líderes de Segurança Digital em suas empresas estabelecidas em território brasileiro.

Das organizações entrevistadas, a maioria (89%) já possui um Sistema de Gestão de Segurança da Informação – SGSI em seu ambiente organizacional. Isso significa que ações de treinamento e conscientização em segurança da informação já fazem parte de seu Planejamento Estratégico de Cibersegurança. A maioria das empresas (60%) declarou que possui de 5 a 20 colaboradores dedicados às atividades de segurança na organização.

A pesquisa também buscou identificar as estratégias de comunicação das políticas, normas e procedimentos de segurança da informação para os colaboradores da organização. A maioria das organizações informou que as normativas estão disponíveis na Intranet para qualquer colaborador, sendo o correio eletrônico também muito utilizado para essa divulgação, especialmente em procedimentos de Onboarding de novos colaboradores.

Como os colaboradores tomam conhecimento das Políticas e Normativas de Segurança da Informação da organização?	
Elas são divulgadas na Intranet	24
São enviadas por e-mail	16
Através de treinamento	10
São entregues em formato papel ao colaborador	8
Não há políticas e normas de SI na organização	0

Tabela 04 – Formas de comunicação de segurança aos colaboradores

Todos os 28 entrevistados informaram que a empresa foi vítima de algum incidente de segurança da informação nos últimos 12 meses. Considerando o escopo da pesquisa, 19 responderam que a organização foi vítima de 6 a 50 incidentes de segurança, que provocaram ou não prejuízo financeiro ou reputacional a ela.

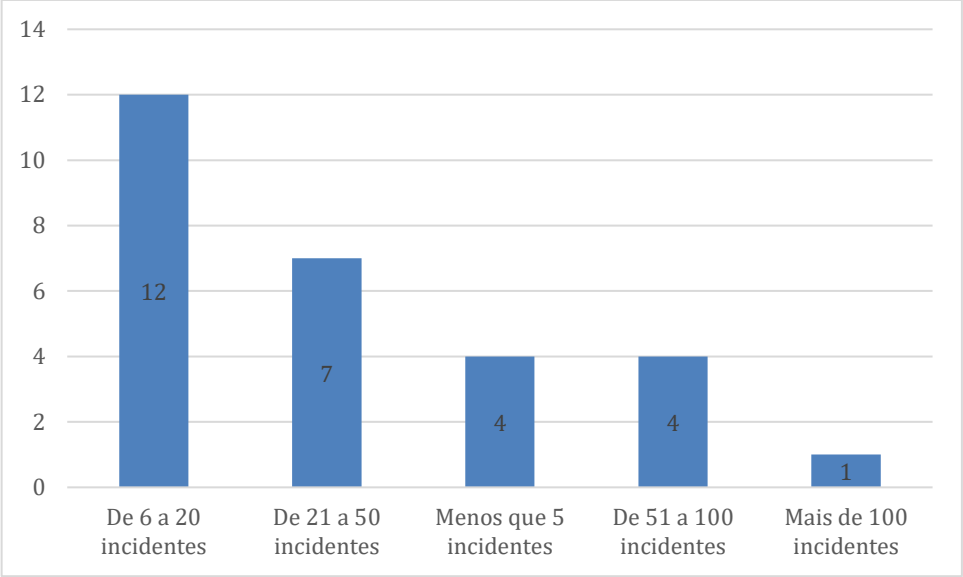


Figura 16 – Incidentes de segurança reportados nos últimos 12 meses

Para identificar a correlação do uso de técnicas de Engenharia Social no universo de incidentes de segurança da informação relatados pelos entrevistados, as respostas foram analisadas estatisticamente, por se tratar de uma pergunta composta exclusivamente de questão objetiva, utilizando opções de resposta em formato Likert, onde os participantes, uma vez questionados, especificam seu nível de concordância com uma afirmação.

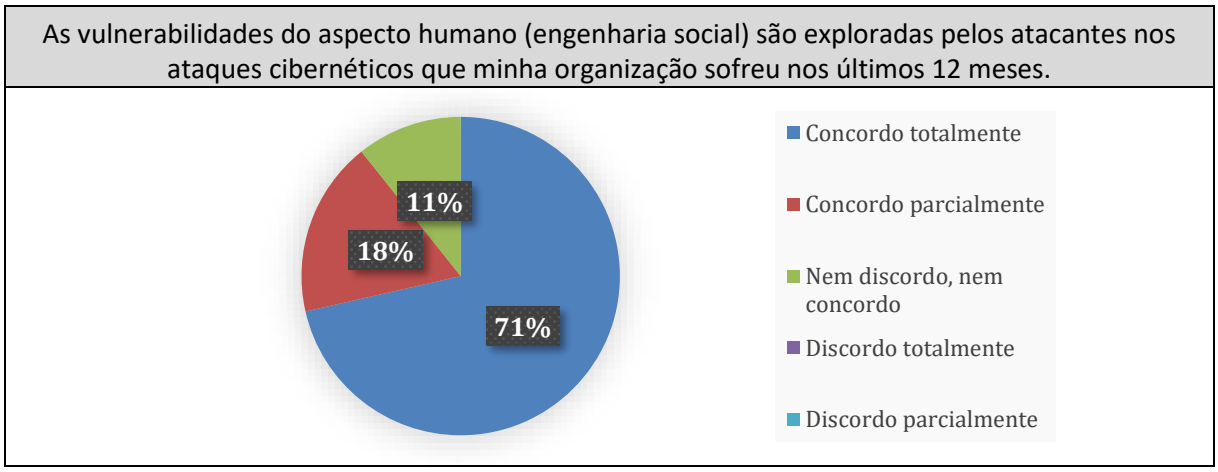


Figura 17 - Uso de Engenharia social como vetor de ataque cibernético

Observa-se com as respostas obtidas, que os entrevistados reconhecem que a Engenharia Social é uma ameaça que precisa ser combatida pela sua organização.

Com relação aos treinamentos e campanhas de conscientização, a maioria dos respondentes afirmou que os treinamentos são realizados apenas para profissionais de segurança e boa parte respondeu que os treinamentos foram realizados uma única vez. Quatro respondentes informaram que a organização nunca realizou treinamento focado em Segurança da Informação.

Como são feitos os treinamentos e as campanhas de conscientização em segurança da informação para os colaboradores? Marque a alternativa que melhor se aplica	
Os treinamentos são feitos apenas para os profissionais de segurança	12
Os colaboradores em geral fizeram treinamento de introdução a SI uma única vez	7
Fazemos treinamentos regulares em segurança da informação	5
A organização nunca realizou treinamentos focados em segurança da informação	4
TOTAL	**28**

Tabela 05 – Público-alvo de treinamentos em cibersegurança

A pesquisa visou identificar também de que forma as organizações conscientizam seus colaboradores frente às ameaças de segurança. A maior parte respondeu que a organização executa as atividades através de meios tradicionais (Palestras e cursos de capacitação). Apenas dois respondentes informaram que a organização realiza simulações para avaliar o comportamento dos colaboradores e apenas um respondente informou que a organização realiza treinamentos imersivos.

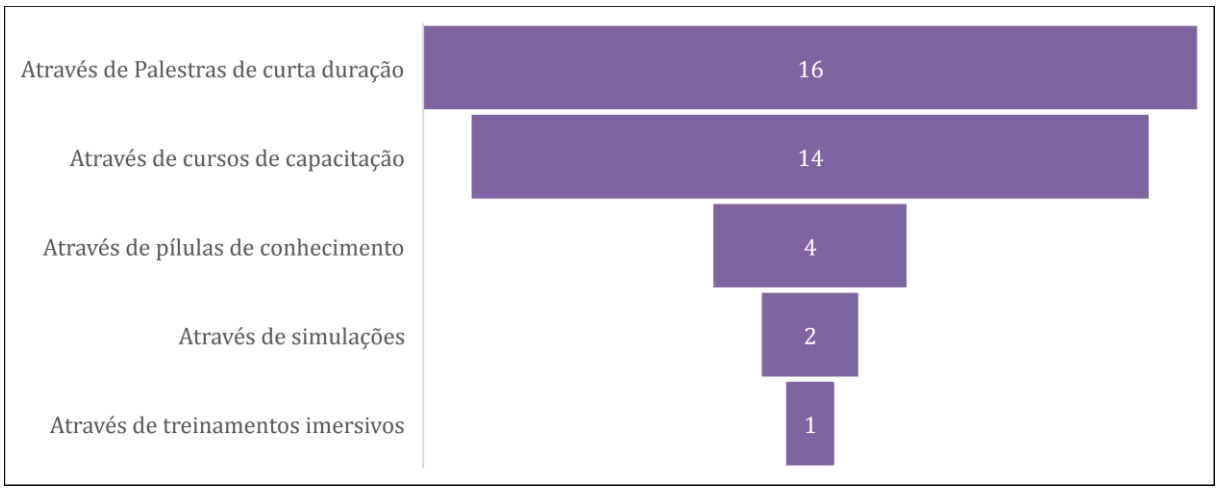


Figura 18 - Formatos de ações de treinamento e conscientização

A maioria dos respondentes (78%) informou que suas organizações oferecem menos de 8 horas anuais de treinamento em segurança da informação. Considerando que um colaborador em regime CLT e que trabalha 8 horas por dia x 5 dias por semana x 52 semanas por ano, ele exercerá sua atividade por 2.080 horas trabalhadas por ano. A carga horária de 8 horas de treinamento anual informada pelos respondentes representa 0,38% do tempo do colaborador em suas atividades laborais.

Complementando a pergunta anterior, foi questionado aos participantes se eles consideram que a alta direção tem uma clara percepção de valor quanto aos programas de treinamento e conscientização em segurança da informação. Apenas 1 respondente informou que "Concorda totalmente". A maioria absoluta (16 respondentes ou 57%) respondeu que "Discorda totalmente" ou "Discorda parcialmente").

A pesquisa também objetivou identificar a algumas das técnicas de metodologia ativa de aprendizagem eram utilizadas pela organização nos programas de treinamento e conscientização. Apenas 6 respondentes disseram que usam pelo menos uma das técnicas, que no formulário estava descrito: Sala de aula invertida, Aprendizagem baseada em problemas, Ensino Híbrido, Gamificação e Hands-On.

Por fim, os entrevistados foram perguntados sobre sua percepção geral quanto ao comportamento dos colaboradores após suas ações de treinamento e conscientização. A maioria dos entrevistados (67%) informou que eles adotaram um comportamento mais alinhado às boas práticas. No entanto, uma parcela significativa (28%) informou que não sentiu diferença após o programa de conscientização adotado.

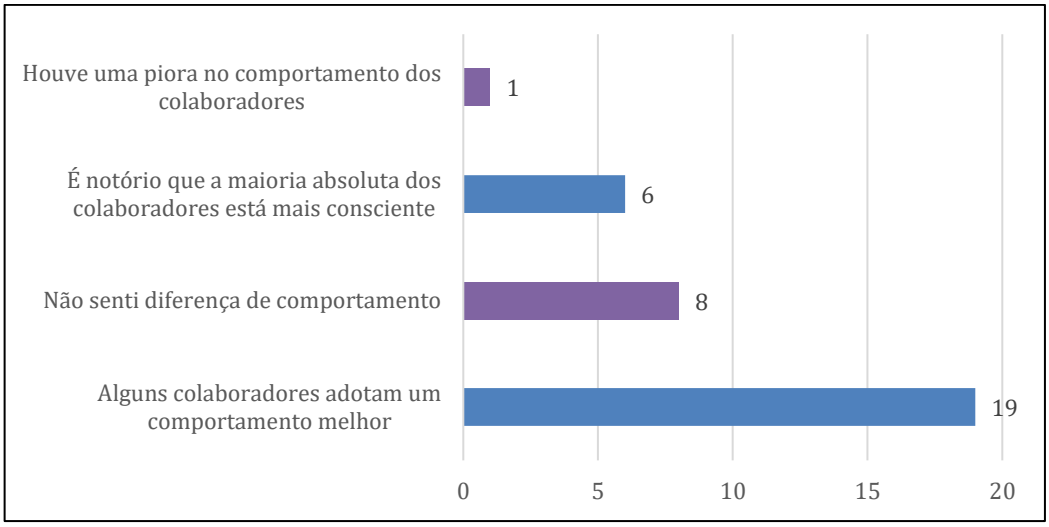


Figura 19 – Percepção do comportamento dos colaboradores

O resultado completo do Levantamento exploratório está no Apêndice deste documento.

4.2 Uso de metodologias ativas de aprendizagem

Como descrito na introdução deste trabalho, o tema “segurança da informação” é considerado por muitos, como um assunto de difícil absorção, seja por onerar as funcionalidades de um sistema, comprometendo sua performance, seja porque o usuário não assimila que o tema pode colocar em risco não só a segurança dos sistemas corporativos, como também a sua segurança digital pessoal.

Durante os Workshops ministrados pelo autor, procurou-se fazer uso de metodologias ativas de aprendizagem para obter engajamento e comprometimento dos colaboradores durantes as atividades previstas.

Um fator considerado de risco foi que os Workshops foram ministrados durante o horário de expediente da organização, competindo com as atividades laborais dos participantes. Alguns deles apontaram essa dificuldade em conciliar as atividades do dia a dia com a necessidade de ficarem imersos nos treinamentos. As considerações dos participantes acerca desse fato estão descritas no próximo tópico: Avaliação de Reação.

Para exemplificar o uso das metodologias ativas de aprendizagem e abordagem estritamente prática, o autor demonstra, através de exemplos, como foi a dinâmica durante o processo de ensino-aprendizagem desse programa de treinamento.

Atividade: Riscos corporativos

- Objetivo: Engajar os participantes
- Metodologia ativa associada: Hands-on
- Ferramentas utilizadas: Cisco Webex e Mentimeter

No primeiro encontro do curso de Gestão de Riscos, o instrutor convidou os colaboradores a participar de uma dinâmica interativa em que eles pudessem apontar

quais os maiores riscos de segurança em sua visão, pontuando-as de 0 a 10, onde 0 representava a menor criticidade e 10, a maior.

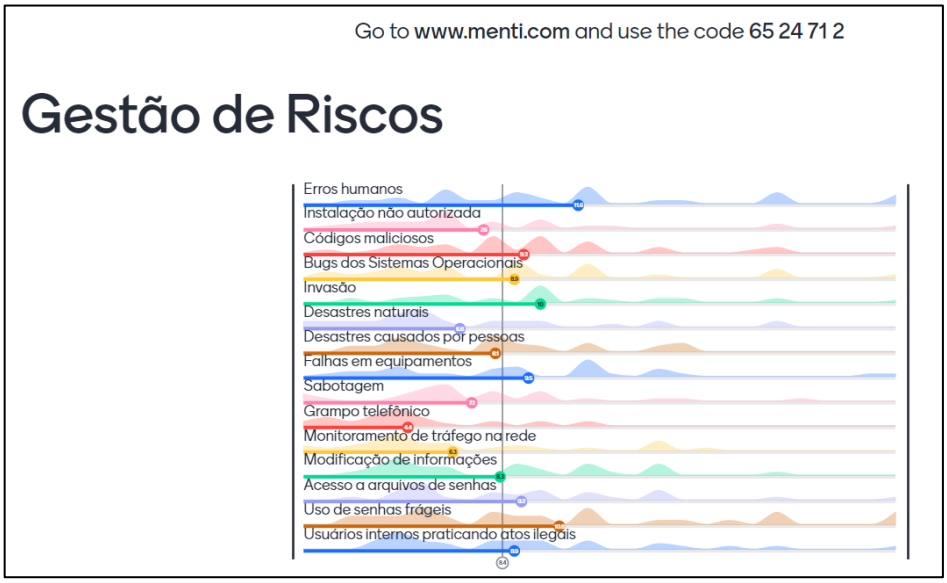


Figura 20 – Atividade Hands-On de Gestão de Riscos

A atividade teve amplo engajamento e promover discussões, a partir do momento em que identificamos aqueles riscos que estavam acima da média. O maior risco apontados por eles mesmos foi o de “Erros humanos”, o que, de certa forma, funcionou para inserir neles um senso de responsabilidade em suas atividades do dia a dia.

Atividade: Quiz de Segurança em Redes

- Objetivo: Aferir o conhecimento dos participantes através de perguntas simplificadas
- Metodologia ativa associada: Gamificação
- Ferramentas utilizadas: Cisco Webex e Kahoot!

Durante uma sessão do Workshop de “Segurança em Redes”, os participantes foram convidados a participar de um QUIZ que aferisse o conhecimento deles nos conteúdos e práticas ministrados até aquele momento. A atividade foi divertida e contou com 46 participantes que estavam online em diversos estados do Brasil.

Destaco a fala de um dos participantes após a ação: “Hoje a gente brincou como sempre, mas aprendeu como nunca”.

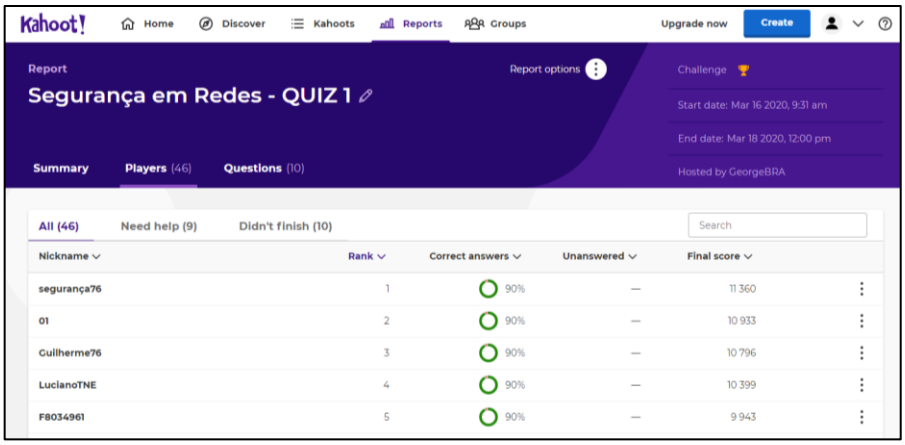


Figura 21 – Atividade gamificada usando o Kahoot!



Figura 22 – Ranking da atividade gamificada usado o Kahoot!

Atividade: Identificação de ativos críticos na organização

- Objetivo: Obter o conhecimento prévio dos participantes
- Metodologia ativa associada: Aprendizagem baseada em problemas (PBL)
- Ferramentas utilizadas: Cisco Webex e Mentimeter

Durante um encontro do Workshop de Segurança da Informação, foi solicitado aos participantes que indicassem quais eram os ativos mais críticos da organização. Enquanto eles descreviam os ativos, todos os participantes acompanhavam e faziam suas considerações

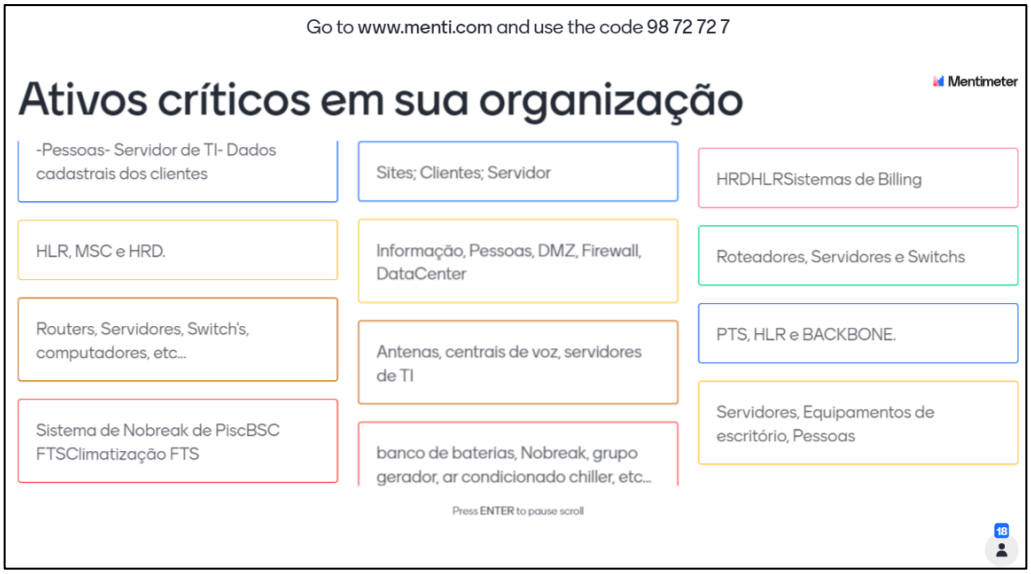


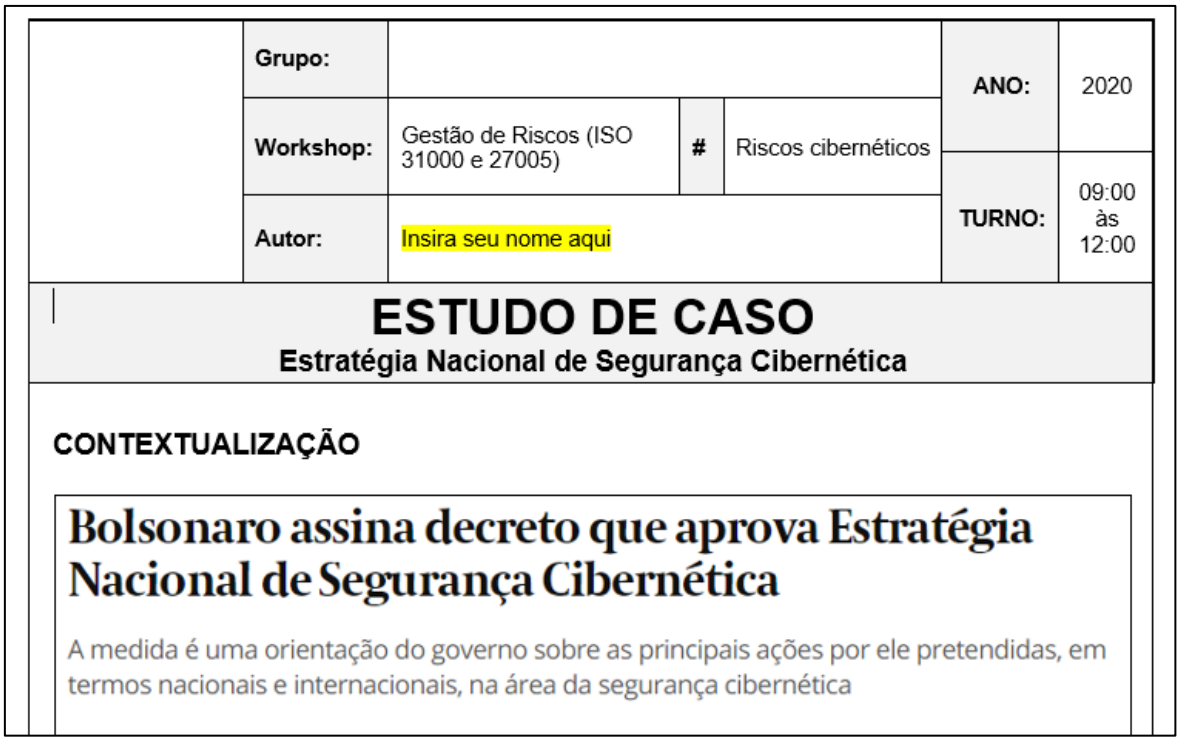
Figura 23 – Atividade baseada na metodologia PBL

A atividade se mostrou interessante, pois na medida em que os colaboradores lançavam um novo ativo que eles consideravam crítico, outros respondentes questionavam a sua criticidade. Essa discussão serviu de base para que o instrutor pudesse inserir um novo elemento no processo de Gestão de Riscos: de que é preciso saber calcular a criticidade de um ativo antes de definir quais controles serão implementados para sua segurança.

Atividade: Estratégia Nacional de Segurança Cibernética

- Objetivo: Discutir a visão do Brasil quanto aos riscos cibernéticos que podem colocar em risco a nossa soberania
- Metodologia ativa associada: Sala de Aula Invertida
- Ferramentas utilizadas: Cisco Webex

Ao término de um encontro do Workshop de Gestão de Riscos, os participantes foram convidados a fazer a leitura do decreto Nº 10.222, que aprovava a Estratégia de Nacional de Segurança Cobernética (E-ciber).



	Grupo:			**ANO:**	2020
	Workshop:	Gestão de Riscos (ISO 31000 e 27005)	**#** Riscos cibernéticos		
	Autor:	Insira seu nome aqui		**TURNO:**	09:00 às 12:00

ESTUDO DE CASO

Estratégia Nacional de Segurança Cibernética

CONTEXTUALIZAÇÃO

Bolsonaro assina decreto que aprova Estratégia Nacional de Segurança Cibernética

A medida é uma orientação do governo sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética

Figura 24 – Atividade baseada em Sala de Aula Invertida

No encontro posterior, o instrutor trouxe algumas questões à tona e pôde fomentar um debate interessante com os participantes, através de suas avaliações individualizadas e repletas de repertório.

Atividade: Matrix tecnológica: esforço x impacto

- Objetivo: Discutir a relevância das novas tecnologias frente aos desafios reais da organização
- Metodologia ativa associada: Estudo de caso
- Ferramentas utilizadas: Cisco Webex e Mentimeter

Durante um encontro do Workshop de “Riscos cibernéticos na era do 5G” foi pedido que os participantes fizessem um Estudo de Caso baseando-se nas tecnologias disponíveis atualmente, que causariam grande impacto em sua organização, especialmente levando em consideração as questões relacionadas a segurança da informação e privacidade de dados. Após a execução do estudo de

caso, os participantes deveriam lançar as repostas no Mentimeter, permitindo que todos os colaboradores pudessem ver e discutir sobre o tema.

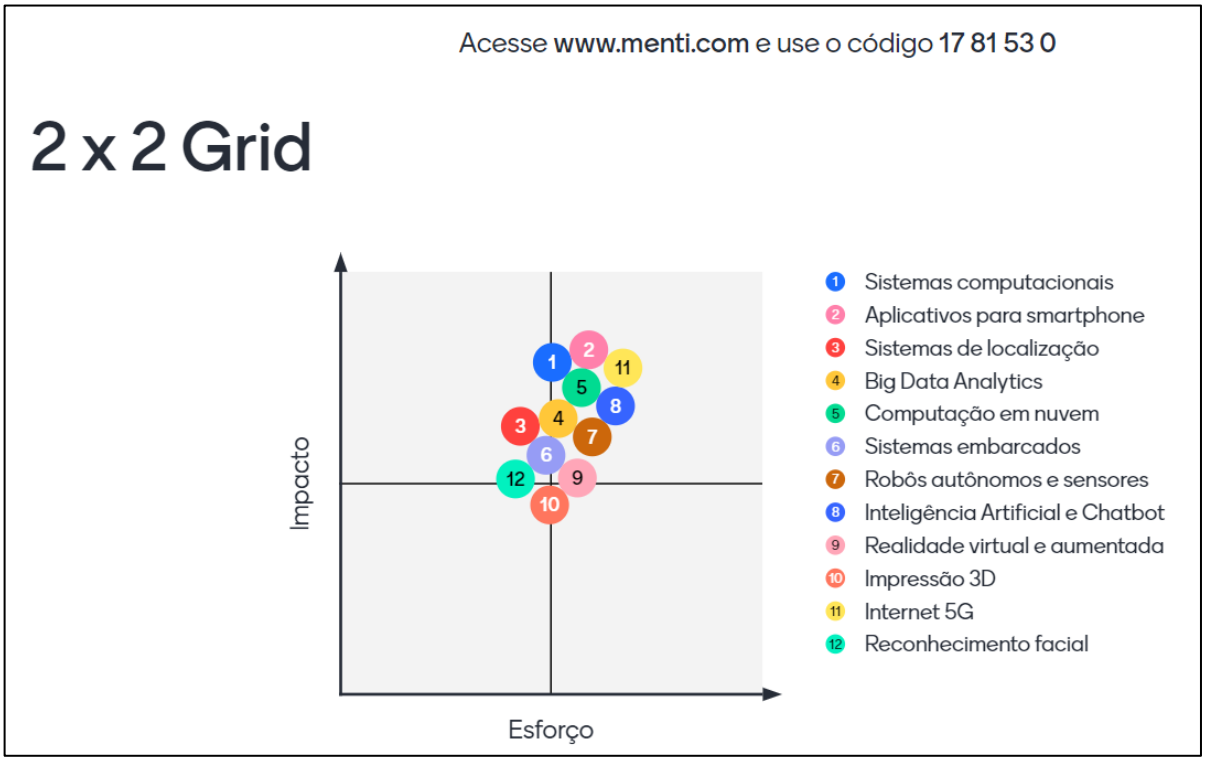


Figura 25 – Atividade baseada em Estudo de Caso

Atividade: Relação Riscos x Benefícios com o 5G

- Objetivo: Avaliar os benefícios do uso de uma tecnologia em contrapartida da visão de riscos
- Metodologia ativa associada: Dinâmica de grupo
- Ferramentas utilizadas: Microsoft Teams

Em uma das atividades do Workshop de “Segurança e Privacidade na era do 5G”, os participantes foram separados em grupo e tiveram que colocar na balança quais eram os riscos e os benefícios do uso das tecnologias estudadas em um segmento de negócio especificado no viés de segurança da informação.



Figura 26 – Atividade de cocriação com uso do Microsoft Teams

A atividade foi realizada inteiramente no Power Point do Microsoft Teams e os participantes puderam discutir diretamente através de mensagens na apresentação. Ao término da atividade, os colaboradores apresentaram suas visões e fizeram muitos elogios sobre a dinâmica da atividade, que transcorreu com uma intensa troca de ideias.

4.3 Avaliação de reação

Nesta seção serão apresentados os resultados após a execução do programa de treinamento e conscientização em cibersegurança com o uso de metodologias ativas de aprendizagem. Conforme descrito no método, esta etapa foi realizada em dois momentos distintos em cada Workshop, utilizando como procedimento de coleta de dados, um questionário.



Figura 27 – Avaliação da experiência do colaborador em um treinamento

Com relação à pergunta sobre a relevância dos temas discutidos para o dia a dia do colaborador na organização, todos os respondentes assinalaram que os assuntos são relevantes ou muito relevantes.

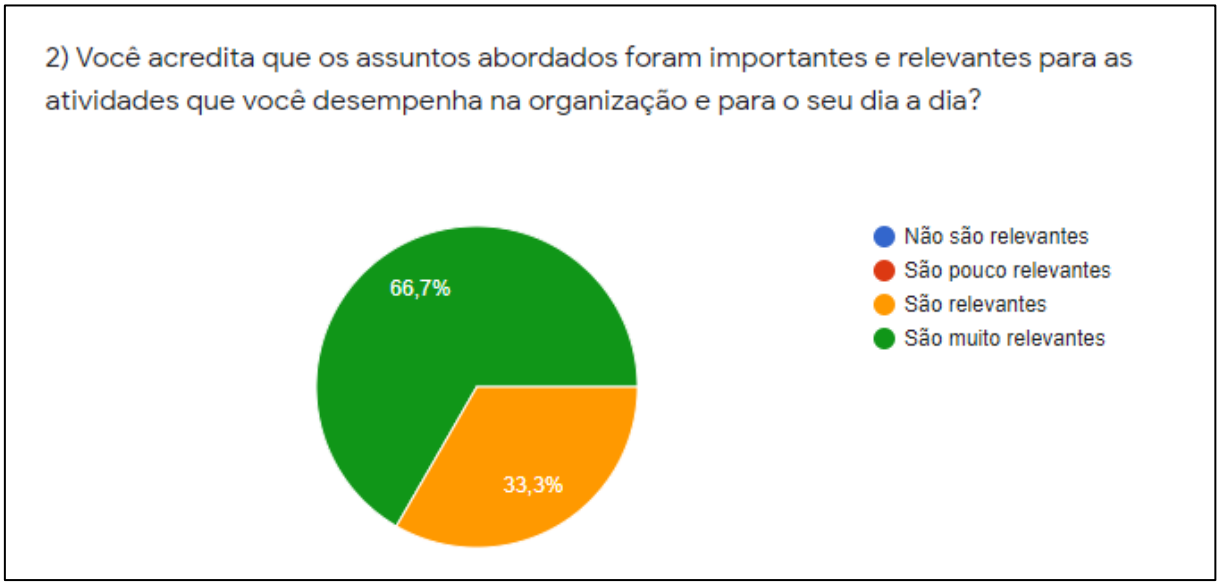


Figura 28 – Pesquisa sobre a relevância do tema para os participantes

Foi pedido que os participantes dessem uma resposta aberta sobre os treinamentos. A tabela abaixo apresenta algumas das respostas dos colaboradores.

Eu simplesmente achei sensacional. Uma ideia incrível. Instrutor e conteúdo maravilhosos.
Ótimo treinamento, agregou bastante no conhecimento sobre segurança da informação
Treinamento muito bom, instrutor tem uma didática excelente e o conteúdo foi muito interessante, grato pela empresa ter promovido esse treinamento.
Foi ótimo... obtive conhecimento que nunca tive acesso...adorei...que tenham mais treinamentos ótimos como esse.
Excelente iniciativa, me surpreendeu. Gostei e espero que na medida do possível termos mais oportunidades de aprendizagem como esta. Alguns conteúdos valem além do profissional, nos ajuda na vida e este conteúdo será cada vez mais importe para todos nós na sociedade, agradeço a todos envolvidos.

As avaliações de reação serviram para identificar pontos de melhoria na condução dos Workshops programados



Figura 29 – Resultado de pesquisa de satisfação após um dos Workshops

De forma geral, o feedback dos participantes foi bastante positivo. O único ponto de atenção gerado pelos feedbacks foi que os participantes relataram que foi difícil conciliar as atividades do dia a dia com o tempo necessário de dedicação ao treinamento.

4.4 Comparativo de indicadores

No tópico 3.5 – Indicador de eficácia do treinamento, foi descrito que o principal indicador para medir a eficácia do programa de treinamento proposto nesta pesquisa

seria o número relacionado ao comportamento dos colaboradores frente a simulações de e-mail phishing disparadas pela área de Cyber Security da organização.

Para facilitar a compreensão do método utilizado para a comparação dos indicadores, a Figura a seguir ilustra os momentos em que as duas simulações de e-mail phishing foram utilizadas na organização. O resultado das simulações 5 e 6 estão separados entre os colaboradores que não participaram das ações do programa de treinamento e conscientização e aqueles que realizaram as atividades.

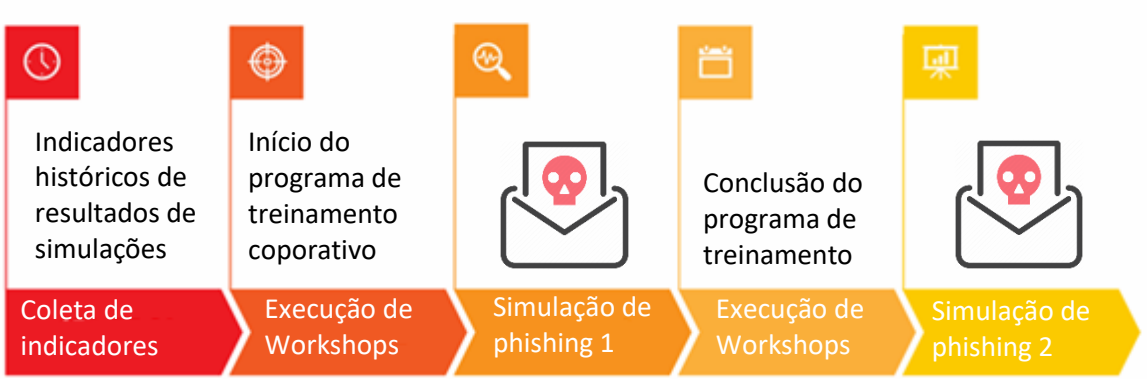


Figura 30 – Modelo de avaliação de indicadores de eficácia do programa

Com relação aos indicadores históricos predecessores ao programa de treinamento, a Figura a seguir apresenta uma discreta evolução de maturidade em segurança da informação dos colaboradores, baseada no comportamento esperado deles em situações de e-mail phishing. Da primeira à quarta simulação, os indicadores variaram entre 6% e 14% entre aqueles que encaminhavam o e-mail suspeito ao e-mail associado. Esses indicadores apresentam os números totais dos colaboradores testados de todas as áreas da organização.

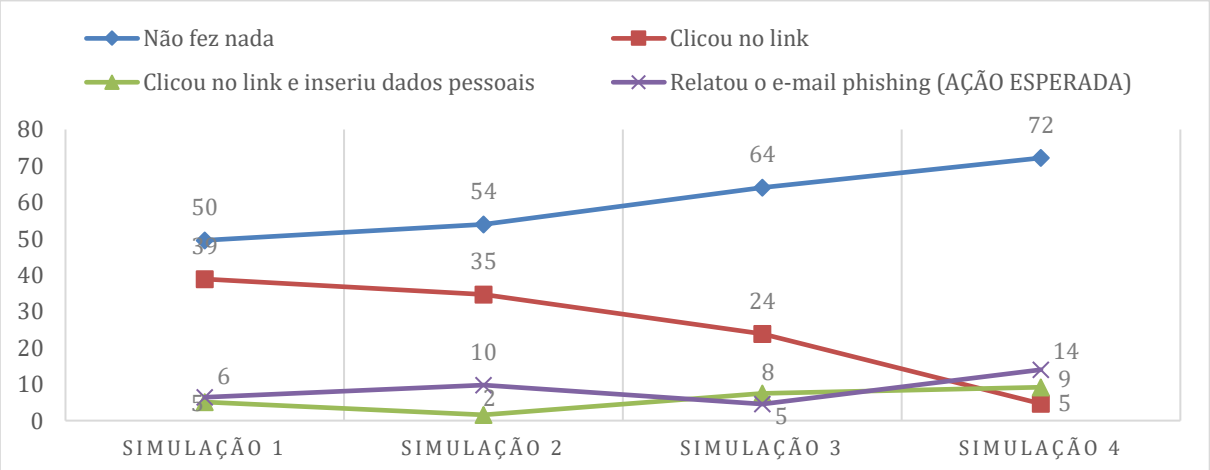


Figura 31 – Indicadores históricos de simulações de e-mail phishing

Os números da Figura a seguir apresentam os resultados das simulações 5 e 6 de e-mail phishing, essas já realizadas após o início e o término das ações de conscientização, respectivamente. Para efeito de comparação, os 195 participantes dos treinamentos não estão compondo o resultado ilustrado abaixo.

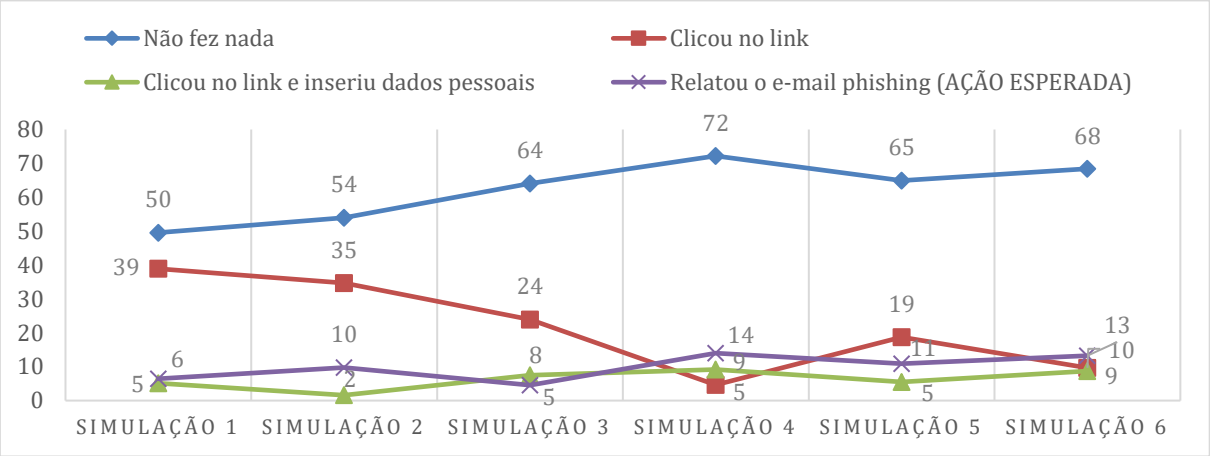


Figura 32 - Indicadores atualizados de e-mail phishing

Como pode ser identificado, não houve alterações significativas de comportamento dos colaboradores considerando as simulações 4, 5 e 6 de e-mail phishing. O número de colaboradores que coloca em risco a organização se mantém acima de 20% após o resultado da sexta simulação. Já o número de colaboradores que não toma as medidas necessárias em situações como essa, continua alto.

A tabela a seguir, por outro lado, apresenta os resultados das simulações 5 e 6 de e-mail phishing exclusivamente dos colaboradores participantes do treinamento. Observa-se uma queda acentuada do número de colaboradores que adotam uma medida potencialmente insegura frente a uma ameaça oriunda de um e-mail e nota-se um aumento expressivo de colaboradores que realizam o procedimento adequado, encaminhando o e-mail à Lista de distribuição corporativa para que seja averiguado.

	Simulação 5		Simulação 6	
	Participantes gerais	Participantes do treinamento	Participantes gerais	Participantes do treinamento
Não fez nada	65%	28%	68%	22%
Clicou no link	19%	3%	10%	3%
Clicou no link e inseriu dados pessoais	5%	1%	9%	0%
Relatou o e-mail phishing (AÇÃO ESPERADA)	**11%**	**68%**	**13%**	**75%**
TOTAL DA AMOSTRA		129		195

Tabela 07 – Comparativo de indicadores de comportamento de usuários

Ao fazer um recorte dos indicadores históricos dos colaboradores participantes do programa de treinamento e conscientização em segurança, observa-se uma mudança de tendência entre as simulações 4 e 5 de e-mail phishing, que se mantém após a coleta de resultados da simulação 6

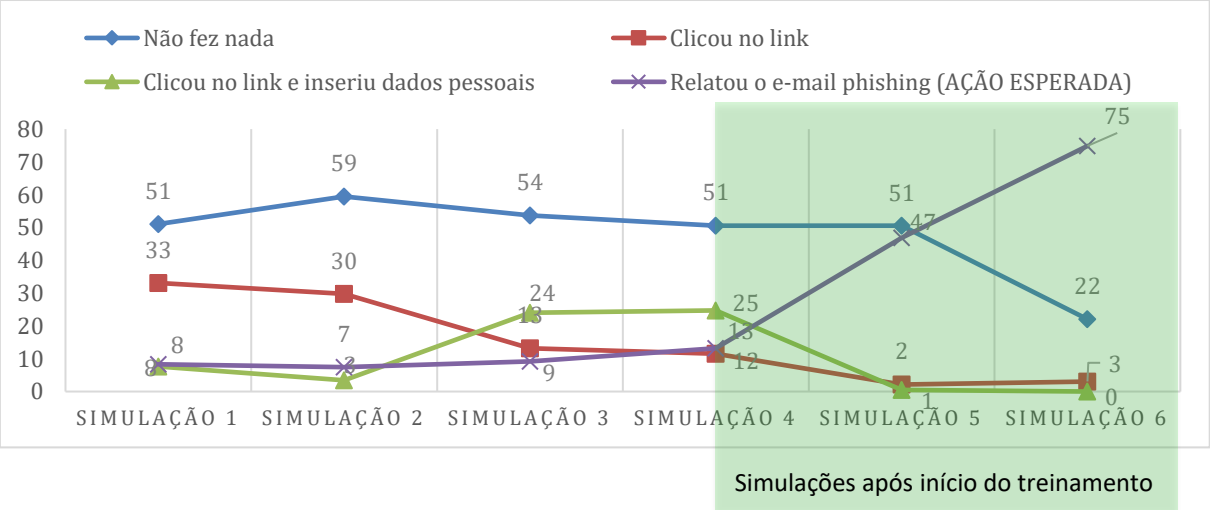


Figura 34 – Evolução histórica comparativa de indicadores

O destaque em verde da Figura acima demonstra que os colaboradores passaram a adotar um comportamento mais alinhado às boas práticas em cibersegurança em ambiente corporativo, além de adotarem uma postura mais proativa frente a ameaças digitais.

5. CONCLUSÃO

Esta pesquisa permitiu identificar os possíveis benefícios do uso de metodologias ativas de aprendizagem em programas de treinamento e conscientização em segurança da informação em ambiente corporativo.

Os dados obtidos por meio do questionário aplicado na pesquisa exploratória indicaram que as organizações brasileiras em geral, utilizam meios tradicionais de aprendizagem para tentar desenvolver nos colaboradores uma cultura cibernética alinhada às boas práticas, em uma tentativa de fazer com que os colaboradores passem a adotar um comportamento mais adequado e que minimize as ameaças digitais que expõem a organização em risco.

Durante a pesquisa, foi identificado resultados positivos em programas de conscientização que utilizaram algum tipo de metodologia ativa de aprendizagem, onde os autores perceberam grande engajamento dos colaboradores durante as atividades propostas, identificando também uma melhoria significativa no comportamento dos colaboradores após as ações.

No experimento aplicado em uma grande empresa do ramo de telecomunicações para cerca de 200 colaboradores de todo o país, em que as técnicas de metodologia ativa de aprendizagem foram aplicadas durante todo o programa de treinamento e conscientização em Cibersegurança, quer seja a Sala de Aula Invertida, Estudos de Caso, Gamificação, Ensino híbrido e Aprendizagem baseada em problemas, foi também percebido grande engajamento dos participantes nas atividades propostas e percepção de valor dos colaboradores, o que ficou evidenciando nas Avaliações de Reação submetidas a eles.

A organização em que o experimento fora aplicado já vinha executando um plano de treinamento em segurança a algum tempo e os resultados dessas ações já vinham contribuindo, de certa forma com um comportamento mais alinhados às boas práticas dos colaboradores, o que ficou evidenciando com os resultados de simulações de e-mail phishing disparadas periodicamente para os funcionários, em que, esperava-se que eles não colocassem a organização em risco tomando uma ação indevida.

No entanto, ao comparar os indicadores comportamentais dos colaboradores que não fizeram parte desse experimento com aqueles que fizeram, foi percebido claramente uma mudança mais expressiva de comportamento do segundo grupo. A ação esperada dos colaboradores ao receber um e-mail suspeito representou apenas 12% do universo testado no grupo que não participou do programa de treinamento proposto nessa pesquisa, enquanto a média daqueles que participaram do programa de treinamento, superou a marca de 71%. Esses números evidenciam claramente que os colaboradores que participaram do treinamento que considerou as metodologias ativas de aprendizagem estavam mais preparados para identificar uma ameaça e reportar ao setor responsável.

Em relação às perspectivas futuras, após os resultados desta pesquisa, compreendem-se que novos indicadores de eficácia do programa podem ser experimentados, a partir da correlação de simulações de outras técnicas de Engenharia Social e incidentes de segurança. Esse trabalho de acompanhamento de indicadores é de fundamental importância para a percepção de que os colaboradores estão adotando um comportamento mais alinhado às boas práticas de Cibersegurança e trazendo menos riscos às organizações.

Pretende-se também que os resultados sejam utilizados por outros pesquisadores como referência no aprofundamento a respeito do tema, alimentando uma esfera maior que objetiva o aperfeiçoamento das práticas educacionais nesta metodologia

REFERÊNCIAS

ABNT NBR ISO/IEC 27001. **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**, 2ª Edição, 2013.

ABNT NBR ISO/IEC 27002. **Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**, 2ª Edição, 2013.

ALECRIM, Cecília. **Desenvolvimento humano e aprendizagem**. 2010. Disponível em:<http://lms.ead1.com.br/webfolio/Mod2020/mod_desenvolvimento_humano_e_aprendizagem_v1_fgf.pdf>. Acesso em: 01 nov. 2019.

ALVES, Cássio Bastos. **Segurança da Informação vs. Engenharia Social : Como se proteger para não ser mais uma vítima**. Disponível em: <https://adm-portal.appspot.com.storage.googleapis.com/_assets/modules/academicos/academico_3641.pdf>. Acesso em: 15 nov. 2018

ARAS, Vladmir. **Crimes de Informática: uma nova criminalidade**. Revista Eletrônica Jus Navigandi. Publicado em 01 out 2001. Disponível em: Acesso em: 09 nov 2018.

BREUSTEDT, Ricardo Bruno. **Segurança da Informação com ênfase na conscientização de usuários de rede**. Disponível em: < https://repositorio.uniceub.br/jspui/bitstream/235/12408/1/51600438.pdf>. Acesso em: 14 abr. 2020

CERT.br- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Resposta e Tratamento de Incidentes de Segurança no Brasil- Cartilha de Segurança para Internet**. Disponível em: < http://www.cert.br/sobre/>. Acesso em: 12 jun. 2019

COLARES, Rodrigo Guimarães. **Cybercrimes: os crimes na era da informática, 2002**. In: Jus Navigandi, Teresina, ano 6, n. 59, out. 2002. Disponível em: http://jus2.uol.com.br/doutrina. Acesso em: 06 nov 2018.

Cyber Incident & Breach Trends Report 2018. Disponível em: < https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf>. Acesso em: 18 jun. 2020

FOUCAULT, Michel. **Vigiar e punir**. Petrópolis: Vozes, 1995.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

GHEDIN, Evandro. **Teorias psicopedagógicas do ensino.** Boa Vista: UERR Editora, 2012.

GOLEMAN, D. **Inteligência emocional: a teoria revolucionária que redefine o que é ser inteligente**. Rio de Janeiro: Objetiva, 1995.

GOUVEIA, Luis Borges. **O conceito de rede no digital face aos media sociais**. Revista do Reseau Mediterraneen de Centres d´estudes et de formation - MULTIMED, 2004

HISTÓRIA e desenvolvimento do computador. Disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/ >. Acesso em: 01 nov. 2019.

LE COADIC, Y. **A Ciência da Informação**. 2. ed. Brasília: Briquet de Lemos, 2004.

LEVY, Pierre. **A Inteligência Coletiva: por uma antropologia do ciberespaço**. São Paulo, Edições Loyola, 2007

MARCACINI, Augusto Tavares Rosa. **Aspectos Fundamentais do Marco Civil da Internet**. São Paulo: 2016.

MARCIANO, João Luiz Pereira. **Segurança da Informação – uma abordagem social**. Disponível em: < https://repositorio.unb.br/bitstream/10482/1943/1/Jo%c3%a3o%20Luiz%20Pereira%20Marciano.pdf>. Acesso em: 14 abr. 2019

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.

MOREIRA, Cássio dos Santos. **Gamificação como solução de treinamento em Cibersegurança na Prefeitura Municipal de Esteio/RS**. Disponível em: < http://raam.alcidesmaya.com.br/index.php/projetos/article/view/63/61>. Acesso em: 02 jan. 2020

NETTO, Abner da Silva. **Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas**. Disponível em: < https://www.scielo.br/scielo.php?pid=S1807-17752007000300007&script=sci_arttext link>. Acesso em: 14 abr. 2019

PIMENTA, Alexandre Manuel Santareno. **A segurança dos sistemas de informação e o comportamento dos usuários**. Disponível em: < https://www.scielo.br/scielo.php?pid=s1807-17752016000300533&script=sci_arttext>. Acesso em: 16 abr. 2019

RIGON, Evandro Alencar. **Modelo de avaliação da maturidade em segurança da informação**. Disponível em: < https://repositorio.ufsc.br/bitstream/handle/123456789/184549/Modelo_Avaliacao_Maturidade_Seguranca_Informacao_Rigon.pdf?sequence=-1&isAllowed=y>. Acesso em: 14 abr. 2019

SANTOS, Rodrigo Costa dos. **Campanha de Conscientização em Segurança da Informação: Um Estudo de Caso**. Disponível em: <https://www.aedb.br/seget/arquivos/artigos16/382440.pdf>. Acesso em: 01 dez. 2019

SILVA, Denise Ranghetti Pilar da. **Segurança da informação: uma reflexão sobre o componente humano**. Disponível em: < http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410>. Acesso em: 14 abr. 2019

SOLMS, R. V. **Information security governance**. South Africa, Springer, 2008.

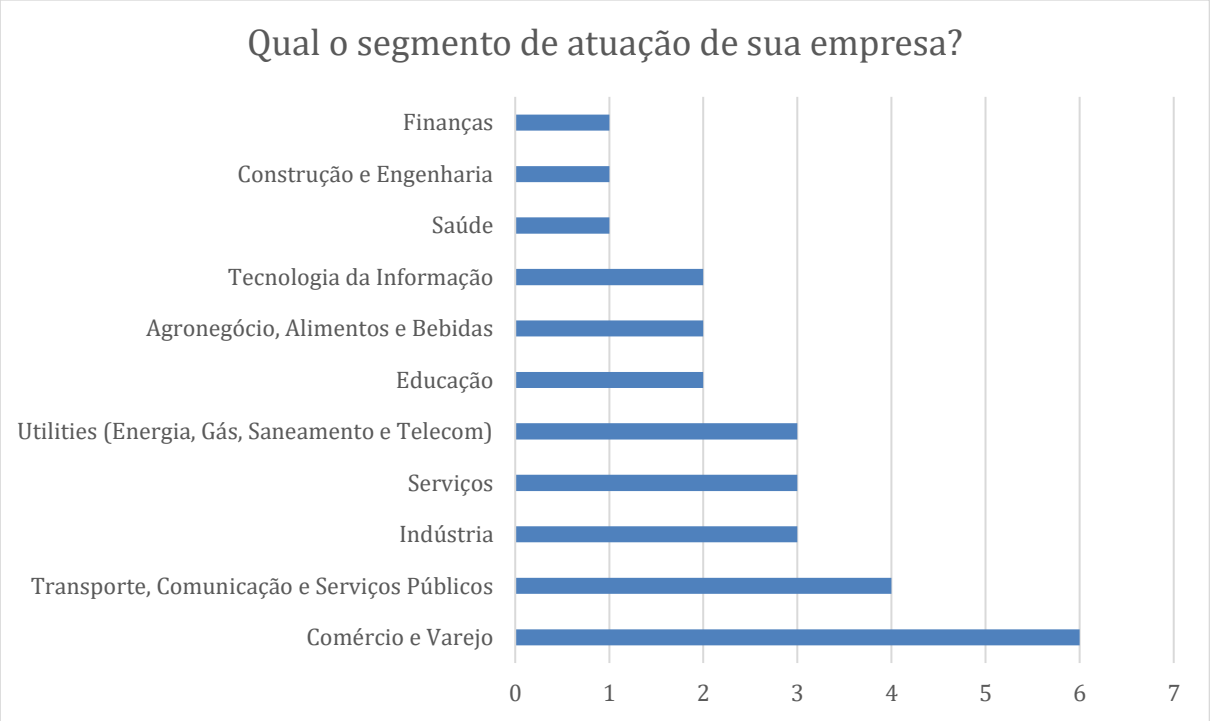
SUTHERLAND, Jeff. **Scrum a Arte de fazer o dobro do trabalho na metade do tempo**. ed. Leya, 2016

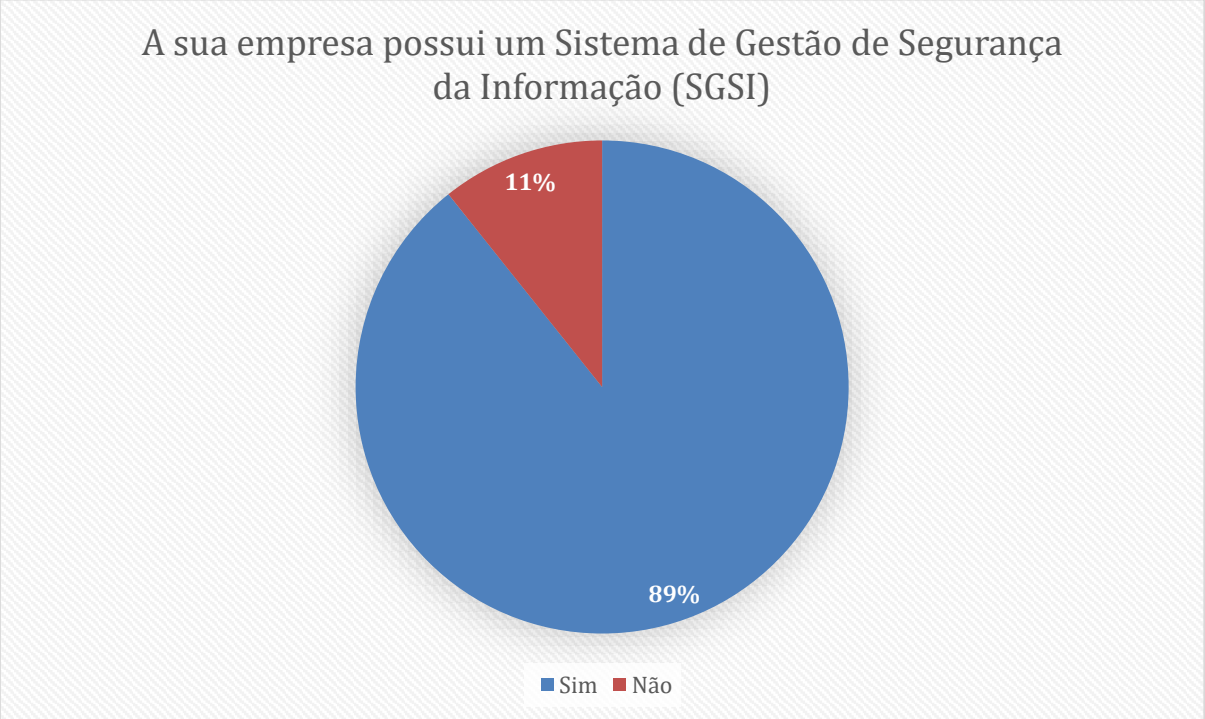
Symantec Internet Security Threat Report. Disponível em: < https://docs.broadcom.com/doc/istr-24-executive-summary-en>. Acesso em: 18 jun. 2020

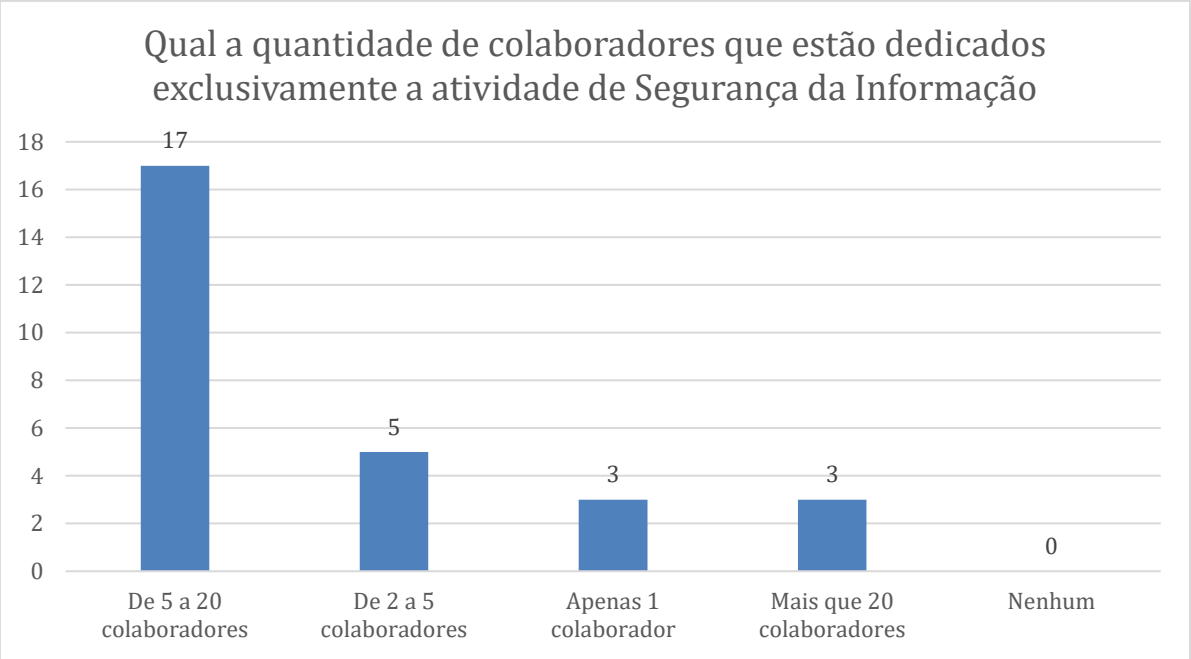
YGOTSKY, L. S. **A formação social da mente**. São Paulo: Martins Fontes, 1999.

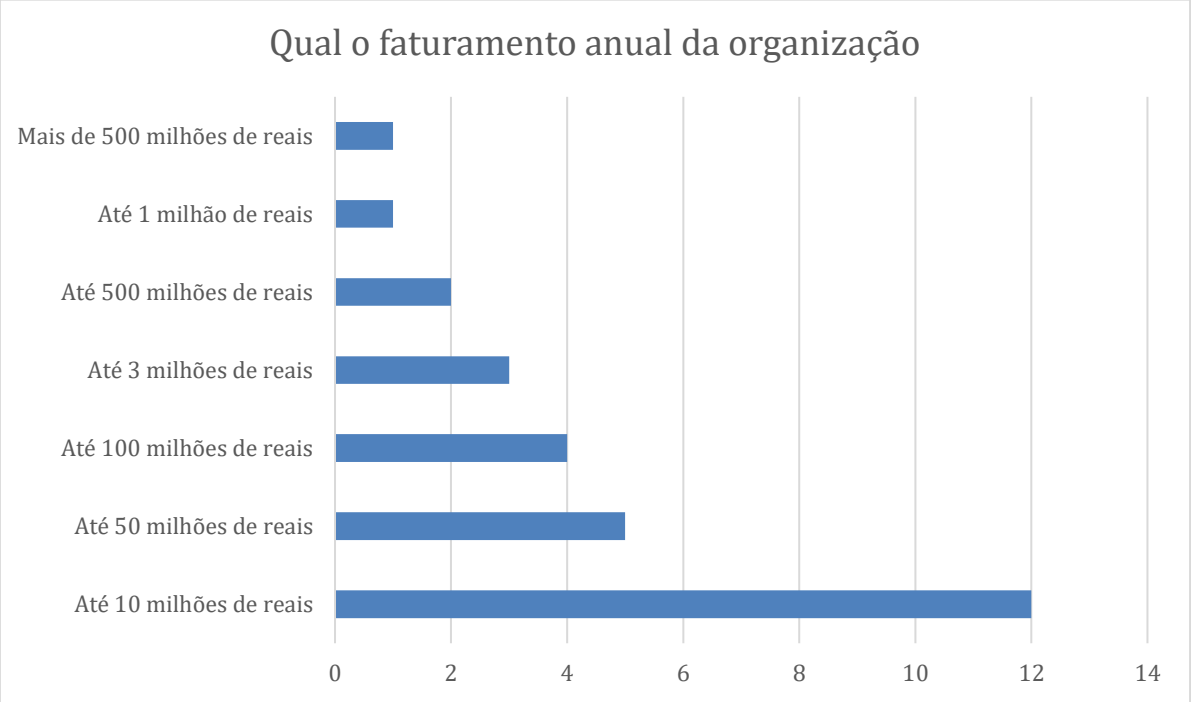
APÊNDICES

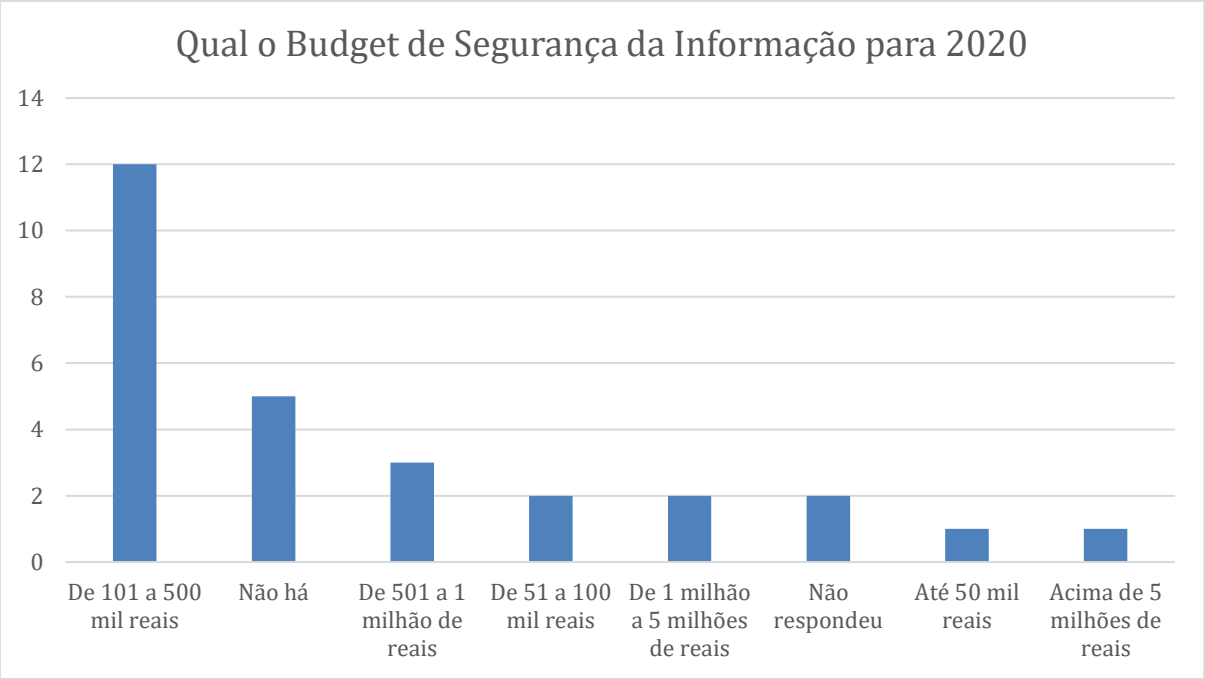
A. Gráficos do Questionário online denominado “Ações de conscientização em Cibersegurança em ambiente corporativo”

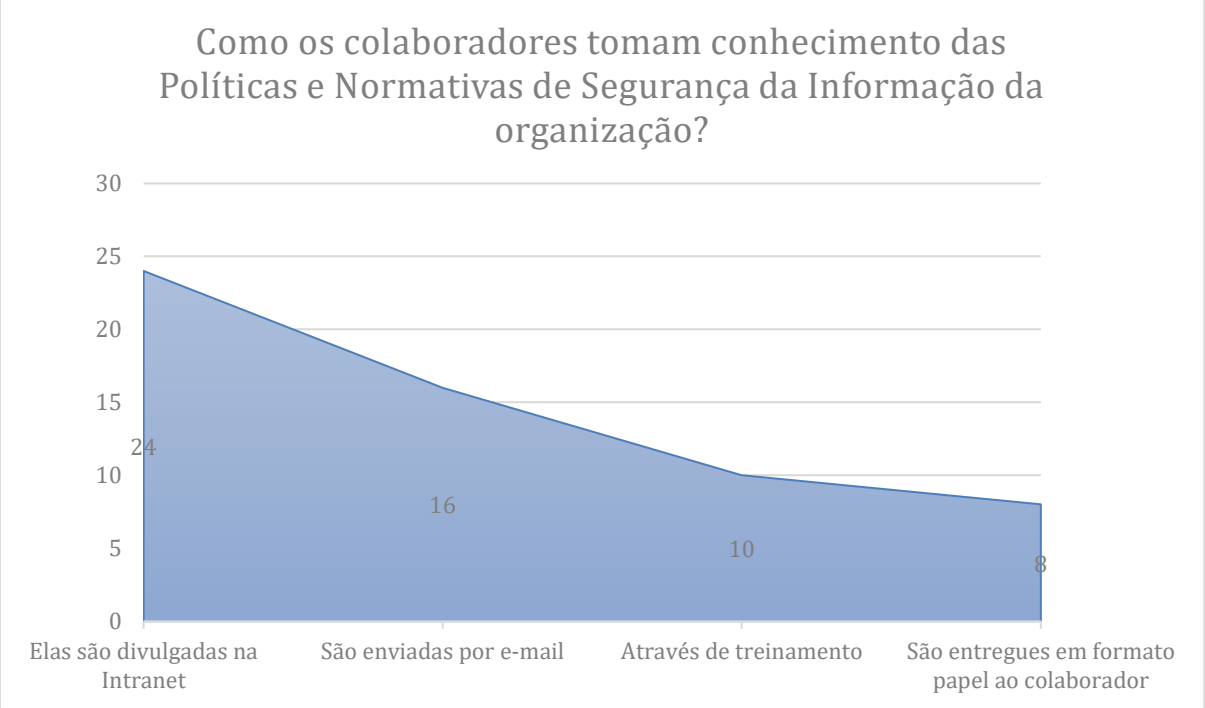


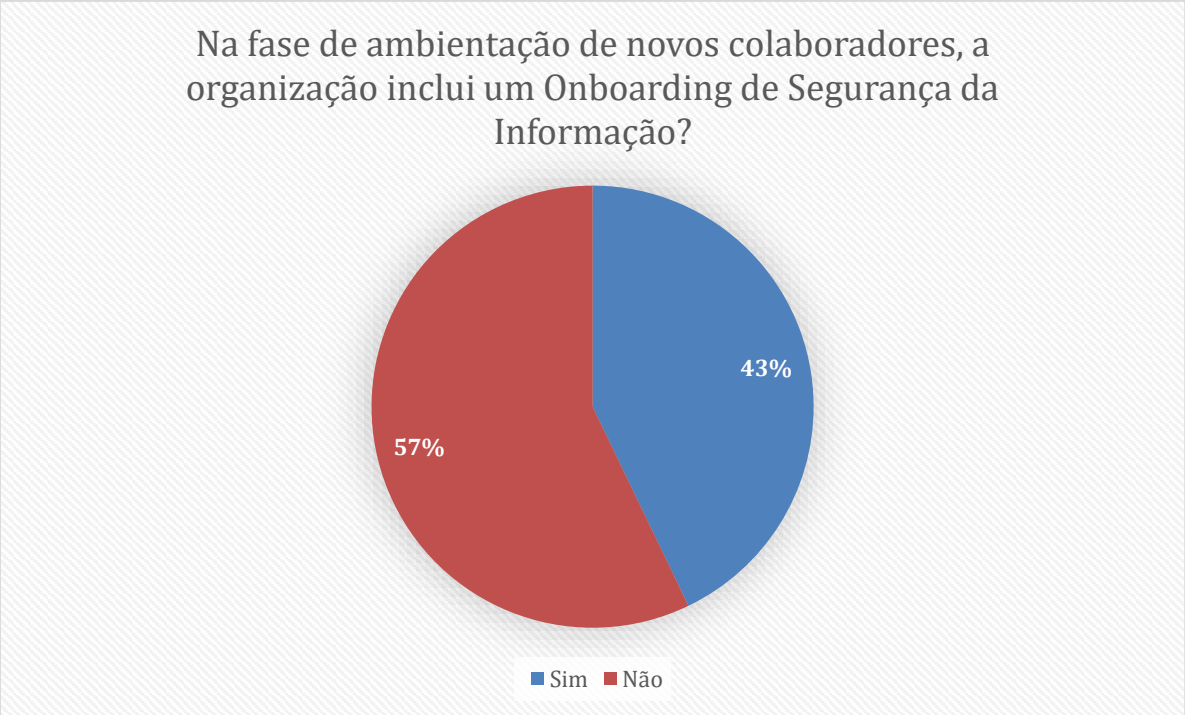


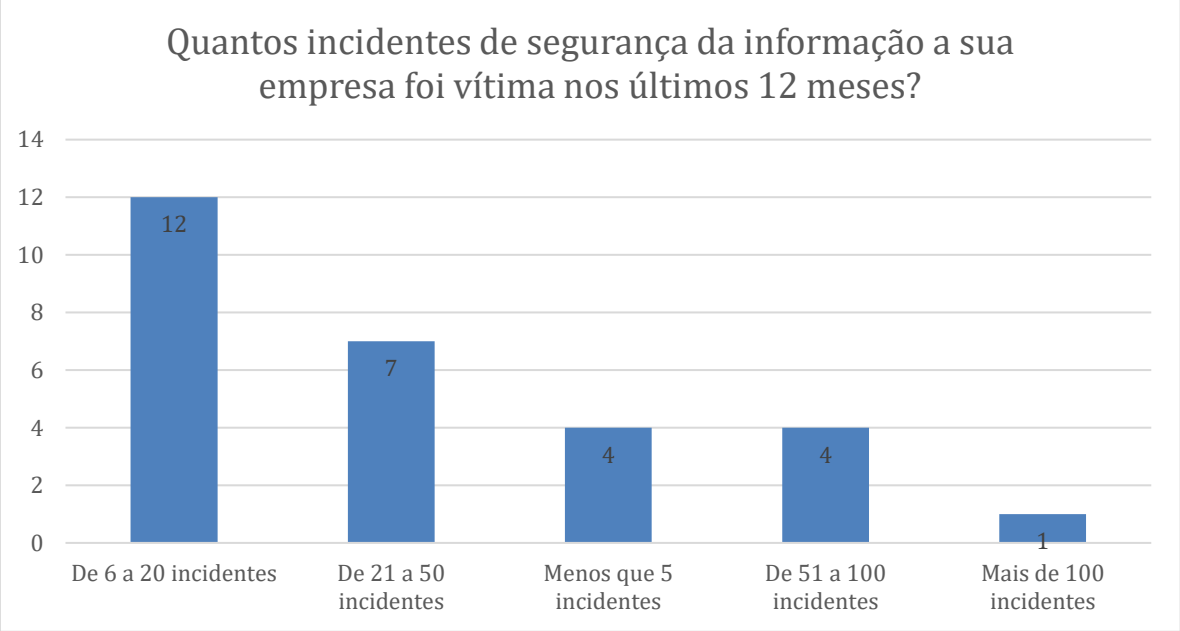

Qual a quantidade de colaboradores que estão dedicados exclusivamente a atividade de Segurança da Informação
18
16
14
12
10
8
6
4
2
0
17
5
3
3
0
De 5 a 20 colaboradores
De 2 a 5 colaboradores
Apenas 1 colaborador
Mais que 20 colaboradores
Nenhum

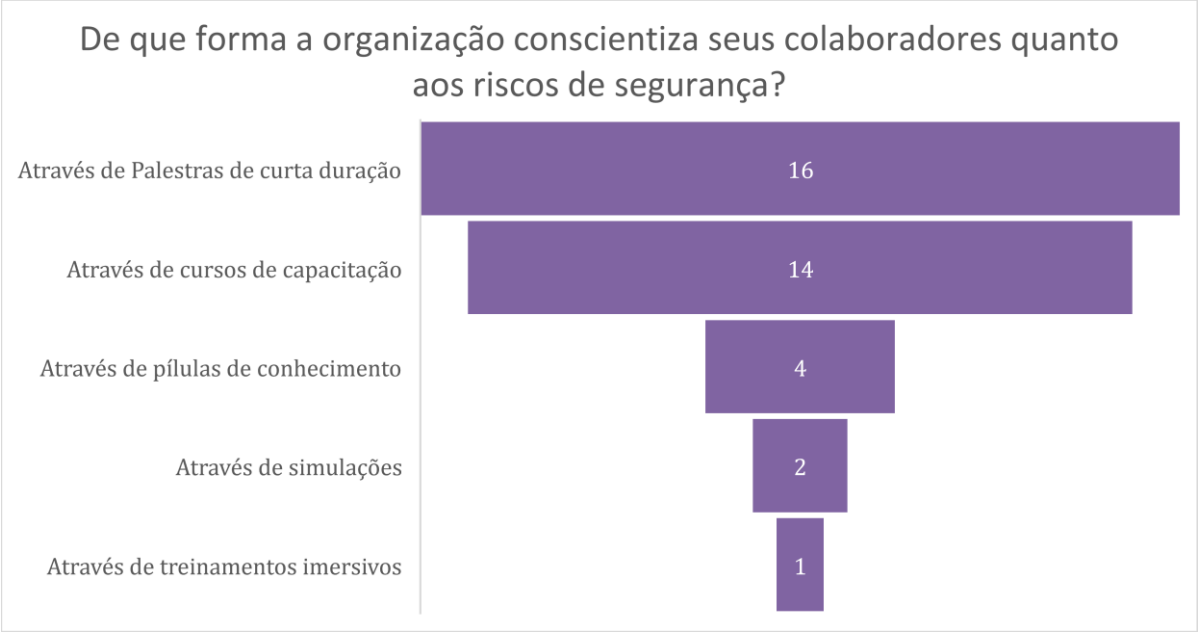

Qual o faturamento anual da organização
Mais de 500 milhões de reais
Até 1 milhão de reais
Até 500 milhões de reais
Até 3 milhões de reais
Até 100 milhões de reais
Até 50 milhões de reais
Até 10 milhões de reais
0
2
4
6
8
10
12
14

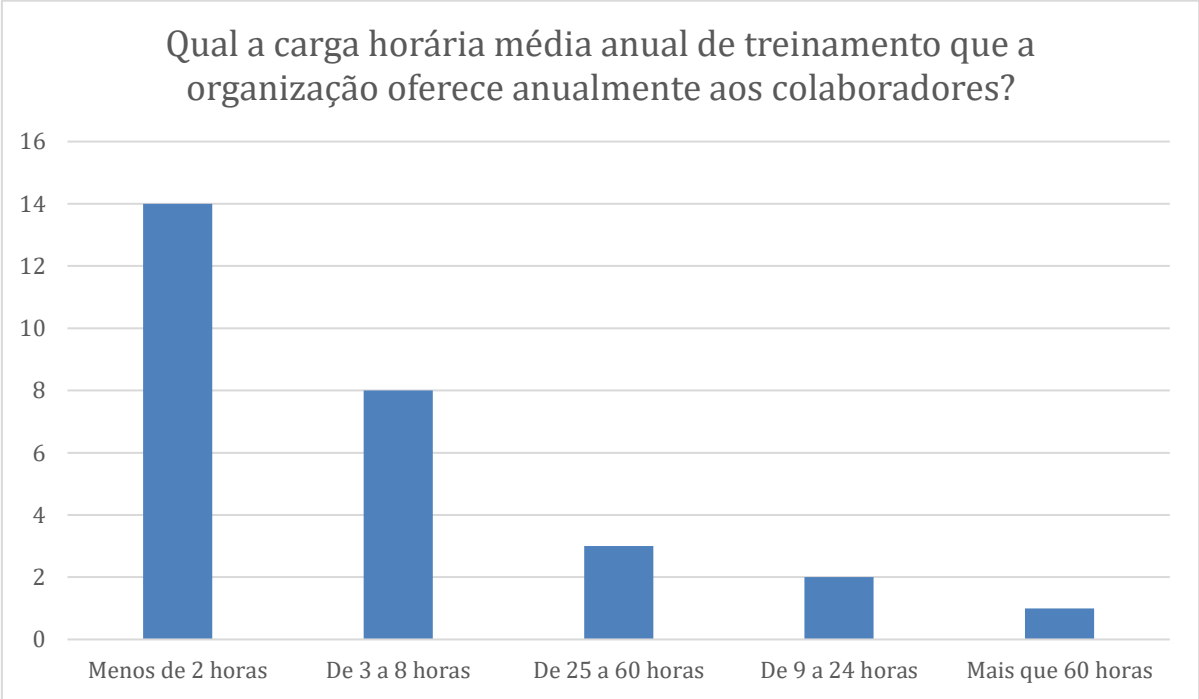

Qual o Budget de Segurança da Informação para 2020
14
12
10
8
6
4
2
0
De 101 a 500 mil reais
Não há
De 501 a 1 milhão de reais
De 51 a 100 mil reais
De 1 milhão a 5 milhões de reais
Não respondeu
Até 50 mil reais
Acima de 5 milhões de reais

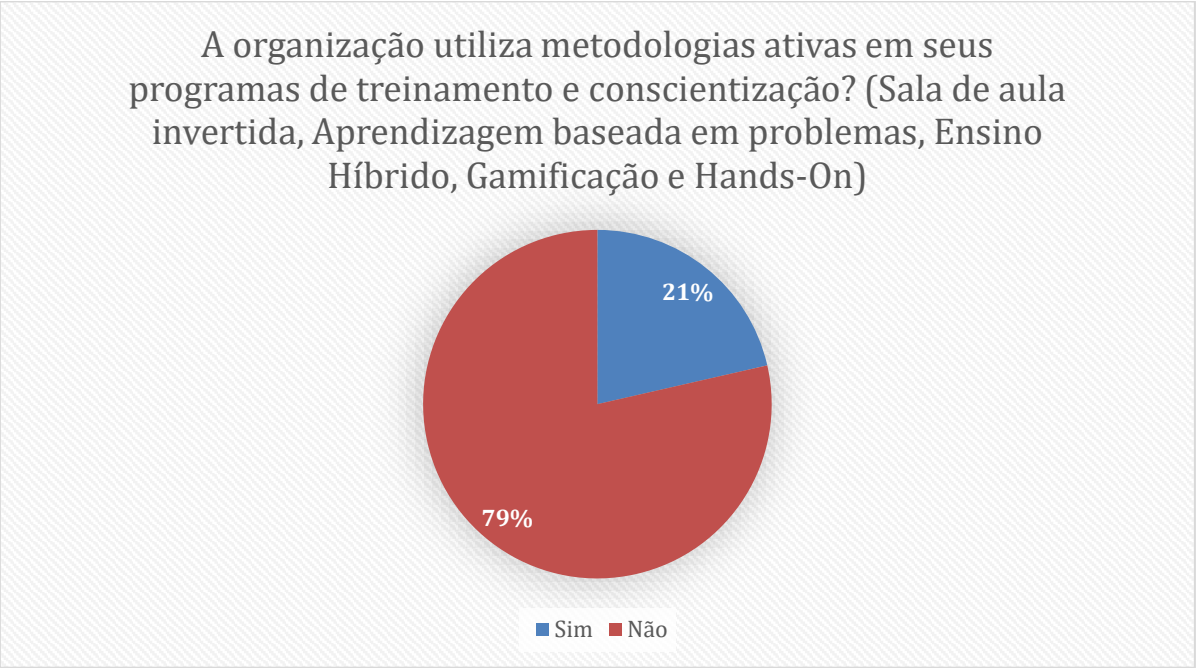

Como os colaboradores tomam conhecimento das Políticas e Normativas de Segurança da Informação da organização?
30
25
20
15
10
5
0
24
16
10
8
Elas são divulgadas na Intranet
São enviadas por e-mail
Através de treinamento
São entregues em formato papel ao colaborador

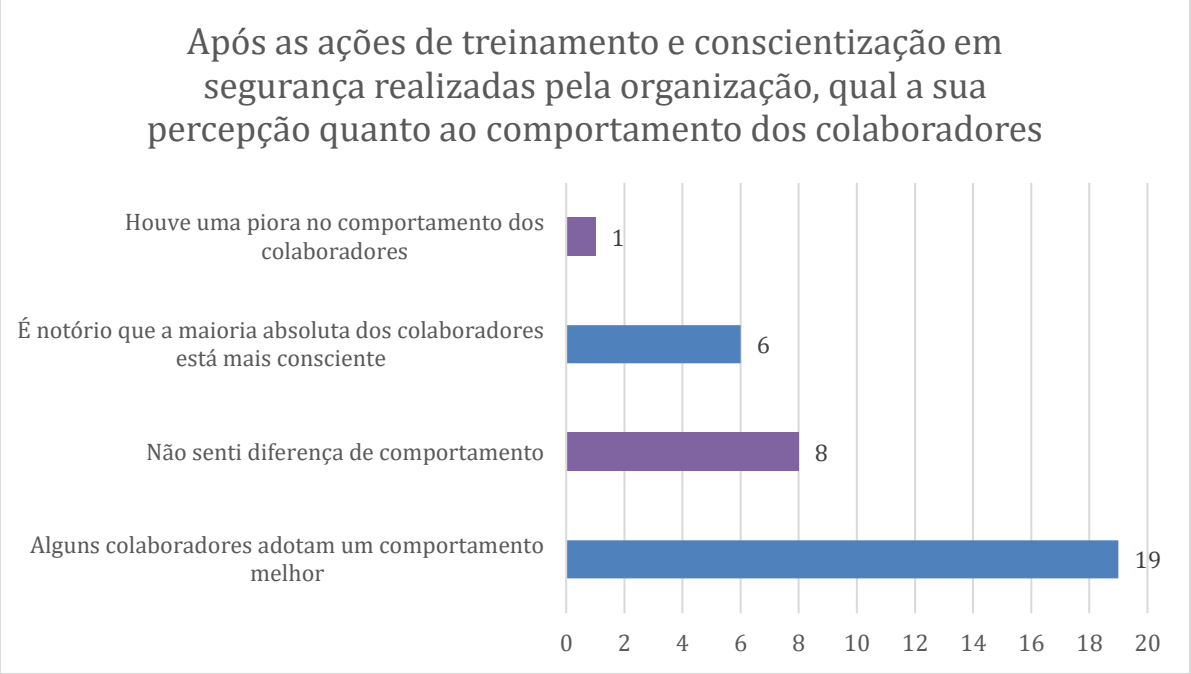

Na fase de ambientação de novos colaboradores, a organização inclui um Onboarding de Segurança da Informação?
43%
57%
Sim
Não

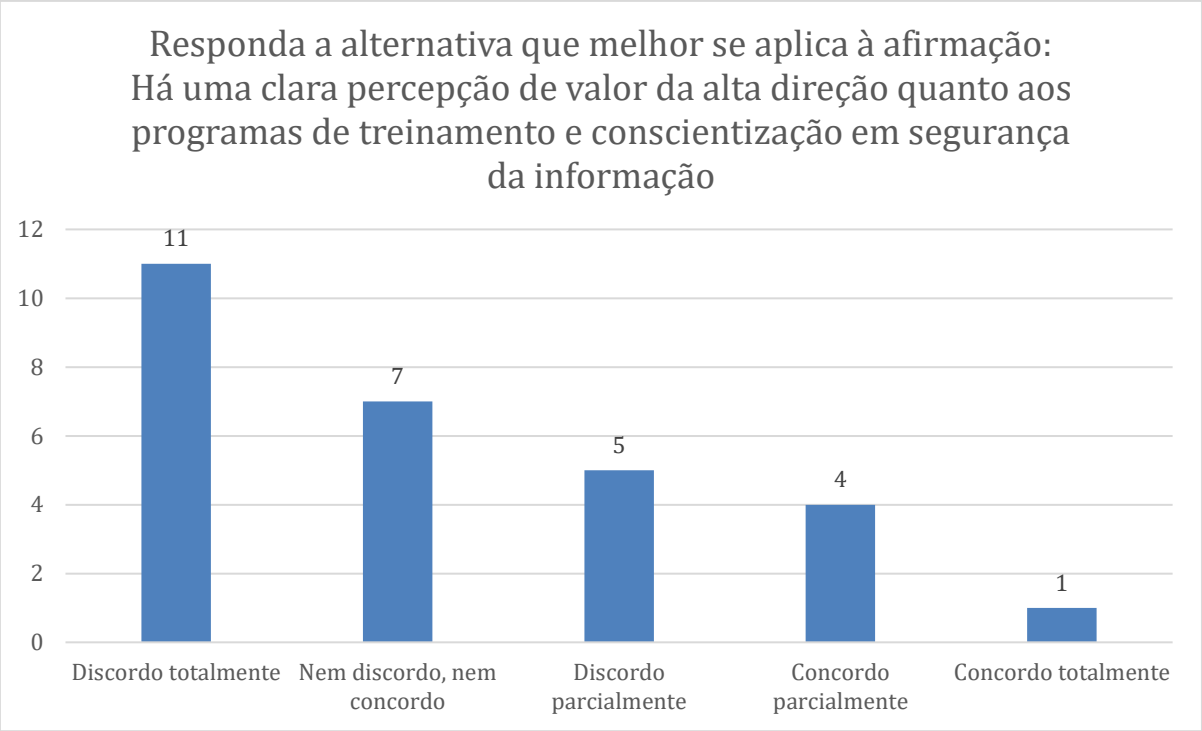

Quantos incidentes de segurança da informação a sua empresa foi vítima nos últimos 12 meses?
14
12
10
8
6
4
2
0
12
7
4
4
1
De 6 a 20 incidentes
De 21 a 50 incidentes
Menos que 5 incidentes
De 51 a 100 incidentes
Mais de 100 incidentes


De que forma a organização conscientiza seus colaboradores quanto aos riscos de segurança?
Através de Palestras de curta duração
16
Através de cursos de capacitação
14
Através de pílulas de conhecimento
4
Através de simulações
2
Através de treinamentos imersivos
1


Qual a carga horária média anual de treinamento que a organização oferece anualmente aos colaboradores?
16
14
12
10
8
6
4
2
0
Menos de 2 horas
De 3 a 8 horas
De 25 a 60 horas
De 9 a 24 horas
Mais que 60 horas


A organização utiliza metodologias ativas em seus programas de treinamento e conscientização? (Sala de aula invertida, Aprendizagem baseada em problemas, Ensino Híbrido, Gamificação e Hands-On)
21%
79%
Sim
Não


Após as ações de treinamento e conscientização em segurança realizadas pela organização, qual a sua percepção quanto ao comportamento dos colaboradores
Houve uma piora no comportamento dos colaboradores
1
É notório que a maioria absoluta dos colaboradores está mais consciente
6
Não senti diferença de comportamento
8
Alguns colaboradores adotam um comportamento melhor
19
0
2
4
6
8
10
12
14
16
18
20


Responda a alternativa que melhor se aplica à afirmação:
Há uma clara percepção de valor da alta direção quanto aos programas de treinamento e conscientização em segurança da informação
12
10
8
6
4
2
0
11
7
5
4
1
Discordo totalmente
Nem discordo, nem concordo
Discordo parcialmente
Concordo parcialmente
Concordo totalmente

	Curso:	Mestrado Profissional em Novas Tecnologias Digitais na Educação	**Ano:**	2020
	Tema:	Uso de metodologias ativas de aprendizagem no desenvolvimento de cultura em cibersegurança em ambientes corporativos	**Segmento:**	
	Pesquisador:	George João de Almeida Chaves	Corporativo	

SEQUÊNCIA DIDÁTICA

Programa de Treinamento em Cibersegurança

Apresentação

Este produto foi criado durante a Pesquisa de Mestrado Profissional em Novas Tecnologias Digitais na Educação oferecido pelo Centro Universitário Unicarioca - Unicarioca entre os anos 2018 e 2020, que teve o seguinte tema norteador: “Uso de metodologias ativas de aprendizagem no desenvolvimento de cultura em cibersegurança em ambientes corporativos”.

O produto traz a aplicação de diversas técnicas de ensino e estratégias de aprendizagem dentro do universo de segurança digital, que, combinadas, visam preparar os participantes a adotar um comportamento mais seguro ao utilizar dispositivos e ferramentas tecnológicas de qualquer natureza e em qualquer ambiente.

Objetivos do produto

- Proporcionar maior engajamento dos colaboradores em programas de conscientização em segurança da informação nas organizações;
- Reduzir o número de incidentes de segurança digital em ambiente corporativo que exploram aspectos de vulnerabilidade humana e usam técnicas de Engenharia Social.

Metodologias ativas de aprendizagem

Para alcançar os objetivos propostos, esta sequência didática considerou as seguintes técnicas de aprendizagem aplicadas em seu desenvolvimento.

- Ensino Híbrido
- Estudo de caso
- Gamificação
- Sala de aula invertida
- Mão na massa – Hands On

Campo de aplicação

O produto foi aplicado em **ambiente corporativo** e explorou os desafios dos colaboradores no dia a dia dentro da companhia. Não há, entretanto, qualquer restrição em sua aplicação em outros ambientes e na educação formal. Todavia, a aplicação do produto fora do ambiente em que foi testado, requer eventuais adaptações em sua abordagem, conteúdo e práticas.

Ferramentas utilizadas neste produto

Para o desenvolvimento das atividades deste produto, foram consideradas diversas ferramentas digitais que permitiram a aplicação das metodologias ativas de aprendizagem durante todo o programa. A escolha das ferramentas tecnológicas considerou como requisitos: a disponibilidade de versões gratuitas, versões amigáveis a dispositivos de diferentes tamanhos e resoluções e às plataformas e ferramentas já homologadas pela organização que foi campo da pesquisa. As tecnologias utilizadas e suas principais características estão descritas a seguir.

CISCO WEBEX https://www.webex.com/pt/	
Descrição	**Aplicação no produto**
Plataforma de videoconferências e reuniões a distância. O recurso, que pode ser acessado via desktop e celulares, dispensa download de programas para entrar em reuniões, basta acessar um link enviado por e-mail. Além disso, é compatível com navegadores como o Chrome, Internet Explorer, Firefox e Safari. A versão paga permite até 200 participantes simultâneos	A Plataforma Cisco Webex é considerada durante todo o programa de treinamento, permitindo que aconteça de maneira online ou híbrida, através de desktops, notebooks ou smartphones. São utilizados recursos diversos, como áudio/vídeo, conversação por chat, e gravação de tela

MENTIMETER https://www.mentimeter.com/	
Descrição	**Aplicação no produto**
Plataforma online para criação e compartilhamento de apresentações de slides com interatividade. O serviço, disponível em planos gratuitos e pagos, possibilita que profissionais de diversas áreas, como instrutores e professores, criem apresentações complexas. A ferramenta oferece recursos interativos, como nuvem de palavras e questionários, que podem ser compartilhadas via Internet com seu público.	O Mentimeter é considerado em diversos momentos durante o treinamento, servindo como apoio em atividades “quebra gelo”, dinâmica de grupo, Hands-on, aprendizagem baseada em problemas, Estudos de caso e Avaliação de reação ao final de uma jornada de conhecimento.

KAHOOT! https://kahoot.it/	
Descrição	**Aplicação no produto**
Plataforma de aprendizado baseada em jogos, usada como tecnologia educacional em escolas e outras instituições de ensino. Seus jogos de aprendizado, "Kahoots", são testes de múltipla escolha que permitem a geração de usuários e podem ser acessados por meio de um navegador da Web ou do aplicativo Kahoot.	O Kahoot é aplicado para aferir o conhecimento dos participantes através de perguntas simplificadas, gamificando a aprendizagem. Os quizes criam insumos para alimentar Dashboards com diversos indicadores de performance e rankings, que promover senso de competição e pode premiar aqueles mais bem pontuados.

ONLINE QUIZ CREATOR https://www.onlinequizcreator.com/	
Descrição	**Aplicação no produto**
Plataforma que permite criar rapidamente seus próprios quizzes. Eles são divertidos de jogar, têm diversos recursos, opções de estilo e dados estatísticos que podem ser utilizados durante sessões de aprendizagem.	Aplicado para aferir o conhecimento dos colaboradores em uma jornada de aprendizagem, gerando insumos para criação de Dashboards de performance do programa

MICROSOFT TEAMS https://www.microsoft.com/pt-br/microsoft-teams/	
Descrição	**Aplicação no produto**
Plataforma desenvolvida para a colaboração de equipes. O conceito inicial do aplicativo foi desenhado para colaboração de equipes corporativas, mas ultimamente tem sido utilizado também para fins educacionais.	O Microsoft Teams é aplicado em atividades de dinâmicas de grupo online, cocriação e design, podendo explorar todo o conjunto de ferramentas da Microsoft, como Editor de Textos, Planilha Eletrônica, Apresentações, Formulários, dentre outros.

MICROSOFT POWER BI https://powerbi.microsoft.com/pt-br/	
Descrição	**Aplicação no produto**
Serviço de análise de negócios da Microsoft que tem o objetivo de fornecer visualizações interativas e recursos de business intelligence com uma interface simples para que os usuários finais criem os seus próprios relatórios e dashboards.	Ferramenta aplicada para dar visão aos indicadores de performance do programa, gerados a partir dos formulários de avaliação de reação, dos quizes e testes online.

Contextualização

Ao mesmo tempo em que os avanços tecnológicos trouxeram muitos benefícios, surgiram novas demandas e as organizações tiveram que passar por transformações, de forma a resguardar os seus processos de negócio dos crimes digitais, aqueles praticados por meio da internet.

O Estudo **Cyber Incident & Breach Trends Report 2018** divulgado pela Online Trust Alliance (OTA), traz dados contundentes sobre ataques cibernéticos. Em 2018, os danos causados pelos cibercriminosos totalizaram US$ 45 bilhões e cerca de 2 milhões de incidentes de segurança foram reportados. O relatório da OTA é baseado em estatísticas, dados e informações de várias empresas e organizações de segurança cibernética, incluindo o FBI e o Cybersecurity Ventures, dentre outras.

O relatório aponta que cerca de 95% das violações poderiam ter sido evitadas. Esse número indica que as pessoas e as empresas não se preocuparam tanto com a segurança de dados e informações quanto deveriam ou as organizações não adotaram estratégias adequadas para a proteção dos dados. Os impactos relacionados a interrupção de sistemas, fraude ou vazamentos de dados podem gerar consequências financeiras ou danos à Figura corporativa das empresas.

A engenharia social é o ato de obter acesso não autorizado a um sistema ou informações sensíveis, como senhas, através do uso de confiança e construção de relacionamento com aqueles que têm acesso a essas informações. Segundo **Relatório de Ameaças da Symantec de 2019**, mais de 80% dos incidentes de segurança reportados pelas organizações tiveram indícios de uso de técnicas de Engenharia Social.

Na reunião da **Organização para a Cooperação e o Desenvolvimento Econômico** (OCDE) ocorrida em março de 2009, foi realçado o tema Cultura de Segurança como vetor estratégico das Nações, e foi colocado em evidência que cada parte envolvida na organização tem um importante papel para assegurar a segurança em função de suas competências, e devem ser sensibilizados sobre os riscos associados à segurança de sistemas e redes de informação.

Aliado aos mecanismos de segurança implementados pela organização para a proteção de seus ativos, é fundamental que os colaboradores façam uso de boas práticas em segurança.

Esta sequência didática faz uso de metodologias ativas de aprendizagem e, combinada com o E-book que a acompanha, tem o objetivo de desenvolver nos colaboradores um comportamento mais alinhado às boas práticas de segurança digital, promovendo um ambiente mais resiliente e seguro contra ameaças cibernéticas.

Objetivos

Objetivo geral
Adotar postura proativa e alinhada às boas práticas de segurança digital frente às ameaças cibernéticas que colocam a organização em risco

Objetivos específicos

- Identificar e avaliar riscos digitais aos ativos de informação
- Compreender seu papel dentro do Sistema de Gestão de Segurança da Informação
- Reconhecer ameaças e reportar potenciais incidentes de segurança
- Identificar atividades suspeitas de engenheiros sociais
- Utilizar os dispositivos e sistemas tecnológicos de maneira segura
- Proteger informações pessoais de titulares de dados

Conteúdos e atividades

Fundamentos de Segurança da Informação

- O valor da informação
- Dinâmica: “Onde meus dados pessoais estão armazenados?”
- Princípios de Segurança Digital
- Dinâmica: “Meus dados vazaram?”
- Relação entre riscos, ameaças e vulnerabilidades
- Impactos da ausência de segurança
- Estudo de Caso: “Sequestro de arquivos”

Medidas de segurança

- Sala de aula invertida: “Estratégia nacional de Segurança Cibernética”
- Tipos de ameaças e vulnerabilidades
- Aspectos de segurança
- Medidas de prevenção, detecção e correção
- Barreiras de segurança
- Hand-On: “Controles de Segurança”

Ameaças digitais

- Classificação e características de malwares
- Dinâmica de grupo: “Malwares”
- Ameaças com pendrives
- Ameaças persistentes avançadas
- Hackers e motivações de ataques
- Engenharia Social e Ameaças físicas
- Gamificação: “Links maliciosos”

Ataques cibernéticos

- Dinâmica: “Teste de Senhas robustas”
- Tipos de ataques de senha
- Ataques de interceptação
- Ataques de envenenamento
- Estudo de caso: “Vulnerabilidades e ameaças em portas de comunicação”
- Ataques de negação de serviço
- Ataques em redes sem fio

Proteção de Dados e Criptografia

- Dinâmica: “Experiência até aqui”
- Estudo de caso: “Informação estratégica confidencial”
- Lei Geral de Proteção de Dados
- Categorias de dados visados por criminosos
- Tipos de criptografia
- Meios de proteção de dados
- Hands-on: “Prática de criptografia”

Sistema de Gestão de Segurança da Informação

- PBL: “BYOD”
- Segurança em camadas
- Políticas de segurança
- Medidas operacionais de segurança
- Camada humana na proteção da informação
- PBL: “Mapeamento de controles da ISO 27002”

Riscos cibernéticos

- Dinâmica: “Ativos críticos da organização”
- Gestão de Riscos
- Identificação, Análise e Avaliação de Riscos
- Análise Qualitativa e Quantitativa de Riscos
- Tratamento de Riscos
- Dinâmica de grupo: Gestão de Riscos

Segurança e Privacidade na era do 5G

- Estudo de caso: Guerra Cibernética como Risco Global
- Autenticação silenciosa e reconhecimento facial
- Indústria 4.0 e Cidades Inteligentes
- Internet das Coisas
- Dinâmica: Segurança e privacidade na era do 5G

4. Metodologia

1º Encontro: Fundamentos de Segurança da Informação

1ª sessão – 20 minutos

- Apresente aos participantes a visão da quantidade de dados armazenados em repositórios digitais de todo o mundo

2ª sessão – 20 minutos

- Dinâmica: “Onde meus dados pessoais estão armazenados?”. Utilizando o MENTIMETER, crie uma apresentação de feedback em tempo real com a seguinte pergunta: “Onde seus dados pessoais estão armazenados?”, com até 10 respostas abertas. O objetivo é trazer a discussão para a realidade dos colaboradores. Faça comentários enquanto os resultados começarem a aparecer na tela



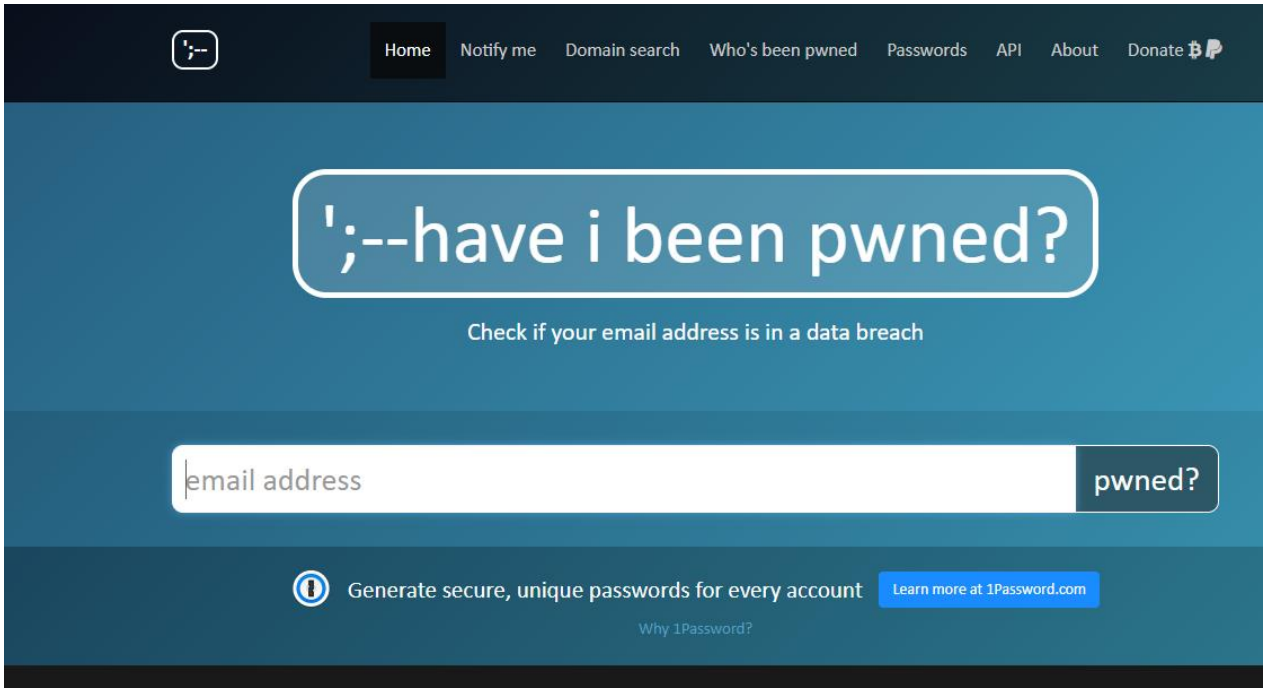
Conhecimento prévio do aluno é a chave para a aprendizagem significativa, segundo Davi Ausubel. O teórico afirma que quanto mais sabemos, mais aprendemos

3ª sessão – 20 minutos

- Apresente os conceitos por trás do valor da informação

4ª sessão – 60 minutos

- Dinâmica: “Fui vazado?”. Peça que os participantes acessem o Website https://haveibeenpwned.com, e lancem seus e-mails no campo destinado. Queira saber qual a resposta dos participantes e os motive a tomar medidas de proteção caso indiquem que seus dados tenham sido vazados. Oriente-os e faça, na prática, os procedimentos necessários para tonar seus dados seguros. Estimule-os a responder o que mais pode ser feito para proteger seus dados.



A interação é importante para o aprendizado. Segundo Vygotsky o aluno se desenvolve por meio da socialização. Ou seja, a busca pelo processo de aprendizagem socializado.

5ª sessão – 20 minutos

- Apresente as definições gerais de segurança e a relação entre risco, ameaça, vulnerabilidade e impacto.

6ª sessão – 30 minutos

- “Estudo de caso: Sequestro de arquivos”.

  Pano de fundo:
  Ataque cibernético em grande Instituição de Ensino Superior
  Uma Instituição Privada de Ensino Superior foi vítima de um ataque cibernético, que causou interrupção em diversos serviços digitais.

  Imagine o cenário. Secretaria Acadêmica sem acesso às informações dos alunos, estudantes sem acesso às notas nas disciplinas, financeiro sem histórico de pagamento das mensalidades, comunicação interrompida entre os funcionários, diversos sistemas inoperantes. Essa foi a realidade de um grande Faculdade do Rio de Janeiro após sofrer um ataque hacker.

  Orientações:

- Ler artigo completo em: https://bit.ly/2FOnwvy
- Identificar quais os princípios de Segurança da Informação foram afetados após o ataque à Universidade. Explicar por que tais princípios foram afetados.
- Apontar quais as possíveis origens de infecção por RANSOMWARE
- Sugerir quais medidas de proteção podem ser adotadas contra esse programa malicioso

- Colocar referência de alguma empresa que já foi vítima desse ataque (print da notícia, nome da empresa afetada e prejuízo estimado)

7ª sessão – 10 minutos

- Sala de aula invertida: “Estratégia Nacional de Segurança Cibernética”. Peça que os participantes façam a leitura do decreto Nº 10.222. até antes de iniciar o segundo encontro.

2º Encontro: Medidas de segurança

1ª sessão – 60 minutos

- Dinâmica: “Estratégia Nacional de Segurança Cibernética”.

Bolsonaro assina decreto que aprova Estratégia Nacional de Segurança Cibernética

A medida é uma orientação do governo sobre as principais ações por ele pretendidas, em termos nacionais e internacionais, na área da segurança cibernética

Por Matheus Schuch, Fabio Murakawa e Fabio Graner, Valor — Brasília

05/02/2020 18h19 · Atualizado há um dia

O presidente Jair Bolsonaro assinou nesta quarta-feira (5) o decreto que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber). O texto terá validade no quadriênio 2020-2023.

Pano de fundo: Com a Leitura prévia do decreto, estimule os participantes a responderem o que consideraram de mais relevante. As seguintes questões podem ser consideradas para aquecer o debate:

a) Quais os riscos cibernéticos apontados de maneira direta ou indireta pelo decreto?
b) Quais os desdobramentos possíveis você entende que podem vir a acontecer a partir da assinatura do Decreto?
c) Qual deve ser a postura ou o compromisso do Estado Brasileiro nas questões relacionadas a Segurança Cibernética, tanto para os cidadãos como para as empresas estabelecidas em território nacional?
d) O Decreto apresenta números e cenários desafiadores para o Brasil a respeito da Segurança Cibernética. Qual deles lhe chamou mais a atenção e por que?
e) Quais tecnologias ou medidas de proteção às informações ou sistemas são citadas no Decreto?

A metodologia de Sala de Aula Invertida prega que o professor induza ao aprendizado ativo, preparando o estudante para um mundo cada vez mais complexo e incerto.

2ª sessão – 30 minutos

- Apresente os perímetros a serem considerados para a proteção da informação.
- Apresente os tipos de ameaças e vulnerabilidades, fazendo analogias com outros tipos de segurança (patrimonial, pessoal, residencial, veicular, dentre outros)

3ª sessão – 20 minutos

- Apresente as 6 barreiras de segurança: Desencorajar, Dificultar, Discriminar, Detectar, Deter e Diagnosticar

4ª sessão – 10 minutos

- Apresente uma visão geral do NIST 800-53, em especial, dos controles de segurança

5ª sessão – 50 minutos

- Hands-on: “Controles de segurança”

Pano de fundo:

Segundo o NIST 800-53, “Controles de segurança são salvaguardas ou contramedidas gerenciais, operacionais ou técnicas, prescritas para sistemas de informação visando proteger a confidencialidade, integridade e disponibilidade do sistema e suas informações”

Vimos no framework que os controles podem incluir qualquer processo, política, dispositivo, prática, ou qualquer outra ação que modifique o risco.

Podemos categorizar os Controles nos seguintes **TIPOS**:

Administrativo ou Gerencial	**Físico**	**Técnico**
São controles definidos como políticas, procedimentos, e atividades que protegem os ativos de informação da organização.	São recursos dispostos com a finalidade de proteger a estrutura física, pessoal e os recursos da organização.	São os componentes de Hardware ou Software empregados na garantia da segurança da informação

Já quanto às suas **FUNCIONALIDADES**, os controles são voltados a objetivos específicos, descritos abaixo:

Diretivos ou Administrativos	Fornece orientação sobre o comportamento esperado e aceitável em relação à Segurança da Informação dentro da organização
Desencorajamento	Tem o objetivo de desencorajar potenciais atacantes. Por vezes utiliza-se de ameaças ou avisos sobre violações
Prevenção	Possui a finalidade de impedir que um incidente ocorra
Correção	Medidas definidas para reagir à detecção de um incidente, visando reduzir ou eliminar a possibilidade de recorrência
Recuperação	Uma vez que um incidente já tenha comprometido as propriedades de segurança de um ativo, sua implementação é necessária para retomar as operações
Detecção	Visa identificar e reagir a incidentes

Orientações:

Imagine o seu ambiente de trabalho e os controles de segurança implementados pela sua organização. Em seguida, enumere-os abaixo, classificando-os quanto ao tipo e suas funcionalidades

Controle	Descrição	Tipo	Funcionalidade	Princípio de segurança
Cite um controle de segurança identificado	*Descreva o controle implementado e o que ele visa proteger*	*Classifique o controle quanto ao tipo*	*Classifique o controle quanto a sua funcionalidade*	*Identifique o Princípio de segurança*

3º Encontro: Ameaças digitais

1ª sessão – 10 minutos

- Apresente uma visão geral do panorama de ameaças digitais nas organizações, demonstrando como os crimino60sos buscam explorar aspectos das vulnerabilidades presentes no ser-humano para conseguir informações ou acessos indevidos.

2ª sessão – 30 minutos

- Apresente as características e tipos de malwares existentes
- Apresente as ameaças de pendrives
- Apresente o vídeo de Ameaças Persistentes Avançadas – APT´s: https://www.youtube.com/watch?v=fUv3VvOHEdI&t=1s

3ª sessão – 40 minutos

- Dinâmica de grupo: “Malwares”. Peça aos participantes se organizarem em grupo e envie eles o link de uma Planilha eletrônica no Microsoft Teams, Google Docs ou outra aplicação similar que permita edição simultânea de arquivos. Cada grupo deverá realizar o preenchimento da tabela e responder às perguntas abaixo:

  1) Pergunta: Cite maneiras de se proteger contra os malwares em geral
  a) Ao utilizar e-mail
  b) Ao utilizar redes sociais
  c) Ao utilizar smartphones

  2) Preencha a tabela abaixo no que diz respeito a:
  Forma de infecção | Forma de propagação | Objetivo do malware (Roubo de dados, indisponibilidade do sistema, etc) | Criticidade/Impacto (Baixa, Média, Alta)

MALWARE	FORMA DE INFECÇÃO	FORMA DE PROPAGAÇÃO	OBJETIVO DO MALWARE	CRITICIDADE
Vírus				
Worm				
Trojan				
Adware & Spyware				
Ransomware				
Rootkit				
Keylogger & Screenlogger				

4ª sessão – 30 minutos

- Apresente o perfil de atacantes e suas motivações

5ª sessão – 30 minutos

- Apresente os aspectos de Engenharia Social na exploração de vulnerabilidades
- Apresente as ameaças físicas

6ª sessão – 30 minutos

- **Atividade gamificada**.

  Pano de fundo: Inicie a sessão informando ser fundamental que as pessoas devem identificar potenciais indícios de engenharia social em seu dia a dia. No meio digital, o uso de técnicas que exploram aspectos da vulnerabilidade humana, está associado aos mais diversos tipos de phishing, seja por e-mail, SMS, redes sociais ou aplicativos de conversação.

  Deixe-os saber que é dever de cada um assumir uma postura do tipo “questionadora”, antes de abrir qualquer arquivo ou abrir qualquer link, uma vez que qualquer ação indevida, pode trazer riscos à organização ou até mesmo à sua vida particular. Faça-os compreender que são um elo importante da linha de defesa de segurança da empresa.

Diga para eles que muitas vezes precisarão tomar decisões e essas decisões, eventualmente estão associadas a clicar ou não em um link suspeito.

Utilizando a plataforma **OnlineQuizCreator**, crie um quiz para fazê-los a identificar links potencialmente inseguros, com base em apenas seu texto. Sugere-se que tenham até 20 segundos para tomada de decisão se deverão clicar ou não naquele link. Para cada link aparente na tela, coloque apenas duas opções: CLICO e NÃO CLICO. A cada novo link a plataforma irá apresentar um ranking com os resultados da rodada.

Resposta esperada	URL
Clico	Globo.com/Cartola-fc
Clico	Cartolafc.globo.com
Não clico	Cartolafcglobo.com
Não clico	globocom.cartolafc
Clico	Ingresso.com/promocao/sohoje/naoperca/imperdivel
Não clico	promocaoIngresso.com
Não clico	Ingressocom.promocao.br
Não clico	receitafederal.com.br



Verifique a possibilidade de premiar os melhores participantes deste game junto à organização. Pode ser um brinde simples, algum voucher de desconto em restaurantes, livrarias, ou com alguma outra empresa que a organização possui parceria.

6ª sessão – 10 minutos

- Apresente o resultado da atividade anterior e informe os motivos de não se clicar em cada um dos links potencialmente inseguros

4º Encontro: Ataques cibernéticos

1ª sessão – 30 minutos

- Dinâmica: “Senhas robustas”. Utilizando o website https://password.kaspersky.com/br/, peça que os participantes digitem senhas que eles potencialmente utilizariam em seu dia a dia. Peça para eles responderem o que o Website apresentou como resultado do tempo necessário para quebra de senha.
- Em seguida, informe aos participantes o quanto uma credencial deve fazer uso de requisitos mínimos para ser considerada segura

2ª sessão – 30 minutos

- Apresente os tipos de ataques de força bruta e ataques de dicionário que os atacantes utilizam para descobrir senhas de usuários

3ª sessão – 20 minutos

- Apresente os tipos de ataque que envolvem a criação de Backdoor e Envenenamento
- Apresente os tipos de ataque de interceptação

4ª sessão – 60 minutos

- **Estudo de caso: “Vulnerabilidades e ameaças em portas de comunicação”**

  Contextualização: Em linhas gerais, a comunicação entre dispositivos em um universo de redes de computadores se dá através do Endereço IP + Porta de Comunicação.

  Exemplificando, ao acessar uma página na Web padrão, o Protocolo HTTP será usado através da Porta 80. Ao se efetuar um download de arquivos, comumente, o Protocolo FTP será usado através da porta 21. Já para acessar um computador remotamente pelo serviço Remote Desktop da Microsoft, será utilizado o protocolo RDP com a porta 3389.

  Um dos primeiros passos de um atacante é identificar quais os serviços disponíveis na rede através da leitura de Endereços IP e Portas. Através delas ele pode identificar vulnerabilidades dos serviços e planejar ataques.

  Orientações:

  1. Veja a lista de portas dos Protocolos TCP e UDP:
  https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

  2. Indique pelo menos 3 serviços ou protocolos que podem ser usados para executar ataques em uma rede de computadores:

Serviço/Protocolo	Porta	Tipo de vulnerabilidade ou ataque	Como remediar

5ª sessão – 20 minutos

- Apresente os tipos de ataque de negação de serviço

6ª sessão – 20 minutos

- Apresente os tipos de ataque em redes sem fio

5º Encontro: Proteção de dados e criptografia

1ª sessão – 20 minutos

- Dinâmica: “Experiência até aqui”. Com 50% do treinamento executado, solicite aos participantes que relatem sua experiência com a aprendizagem até o momento. Utilize o MENTIMETER para promover essa atividade, com respostas abertas



2ª sessão – 40 minutos

- **Estudo de caso: Informação estratégica confidencial**

  Organize os participantes em duplas. Em seguida, apresente a eles uma situação hipotética e entregue a eles uma planilha eletrônica que deve ser feita de maneira cocriada através de ferramentas como Microsoft Teams, Google Docs ou outra similar.

  Contextualização: Em uma reunião, uma nova definição foi estabelecida: A informação estratégica confidencial da empresa. A mesma é anotada em papel e armazenada posteriormente em um cofre adequado. No momento imediatamente posterior, o diretor delega à secretária que digite tal informação e a envia por correio eletrônico aos envolvidos.

  Depois de completada a tarefa, a secretária não adotou os procedimentos adequados de descarte, e consequentemente, jogou sem qualquer critério e tratamento, o material original em papel na lixeira mais próxima.

Um outro funcionário no perímetro físico da secretaria, interessado, mas que não participara da reunião e tem objetivos obscuros, foi até o local onde a secretária descartou o papel e o recolheu. Este funcionário tinha sido desligado da corporação naquela semana.

Orientações:

1. Identificar 3 pontos de vulnerabilidades ou erros de falta de segurança

2. Apresentar 1 mecanismo de segurança da informação para 1 dos pontos de vulnerabilidade ou erros de falta de segurança encontrados no item 1

TAREFA 1			TAREFA 2
PONTO CRÍTICO		VULNERABILIDADE	MEDIDA(S) DE SEGURANÇA
1			
2			
3			

2ª sessão – 20 minutos

- Apresente aos participantes o contexto geral de vazamento de dados, ilustrando com notícias atuais de incidentes que já foram expostos ao público em geral
- Crie uma discussão a respeito dos tipos de dados que eventualmente são buscados por criminosos

3ª sessão – 20 minutos

- Apresente mecanismos de proteção contra roubo de credenciais, como autenticação em dois fatores e utilização de criptografia

4ª sessão – 20 minutos

- Apresente os aspectos gerais da Lei Geral de Proteção de Dados e como as organizações deverão se preparar para proteção dos direitos dos titulares de dados

5ª sessão – 30 minutos

- Apresente os aspectos gerais de criptografia e como ela funciona
- Apresente os tipos de criptografia e os motivadores de sua utilização

6ª sessão – 30 minutos

- Apresente o funcionamento de Criptografia e Esteganografia, na prática, com a utilização de ferramentas como Cryptool e StegoTool

6º Encontro: Sistema de Gestão de Segurança da Informação

1ª sessão – 20 minutos

- Apresente os desafios para proteção da informação em cenário corporativo

- Apresente os direcionadores de um alinhamento estratégico de segurança, expondo a necessidade de equilibrar as ameaças aos processos de negócio da organização

2ª sessão – 60 minutos

- **Aprendizagem baseada em problemas: BYOD**

Contextualização: Apresente aos participantes o cenário de profusão de uso de dispositivos pessoais em ambiente do trabalho. Dê exemplos e apresente os riscos relacionados a essa prática.

Peça que os participantes façam a leitura do artigo Segurança BYOD - Desafio e melhores práticas para as empresas. https://www.alleasy.com.br/2018/07/22/seguranca-byod-desafios-e-melhores-praticas-para-empresas/

Utilize alguma ferramenta de Formulário Online para aferir o conhecimento dos participantes quanto às políticas de normativas de segurança relacionadas a utilização de dispositivos pessoais no ambiente de trabalho.

Esse questionário está relacionado ao tema BYOD. Todas as respostas serão anonimizadas e usaremos o resultado apenas para levantar discussões durante o treinamento.

Você conhece a política relacionada a BYOD em sua organização?
- Sim
- Não

Nos últimos 3 anos, quantos dispositivos pessoais (notebook, smartphone, tablet ou desktop) você levou ao trabalho
- Nunca levei
- 1
- Até 3 dispositivos
- Até 5 dispositivos
- Perdi a conta

Que tipo de sistemas corporativos você já acessou ou acessa fora do âmbito da organização através de seu próprio dispositivo?
- Acesso ao e-mail corporativo
- Acesso ao sistema de chamados
- Acesso ao sistema ERP
- Acesso a servidores
- Acesso a elemento de rede
- Acesso remoto a desktop ou notebook corporativo

Sua organização estabelece procedimentos específicos ao disponibilizar acesso a sistemas fora do âmbito da organização?
- Não
- Sim, porém, menos do que eu acho que deveria

- Sim, existem procedimentos que eu considero seguros
- Sim, mas os procedimentos acabam tornando o acesso lento ou burocrático

O que você faria (passo a passo) caso descobrisse que algum dispositivo pessoal que você utiliza para acessar um sistema da empresa tivesse a segurança comprometida fora de seu horário de expediente?
Resposta aberta

Por fim, cite algumas boas práticas que você acredita serem importantes ao utilizar dispositivo pessoal no acesso a sistemas da organização.
Resposta aberta

Ao término da atividade, abra a respostas e discuta com os participantes o que foi respondido por eles

3ª sessão – 20 minutos

- Apresente o princípio de Segurança em Camadas e exemplifique quais medidas de proteção podem ser adotadas em cada uma
- Apresente os tipos de medidas organizacionais para proteção dos ativos de informação em ambiente corporativo

4ª sessão – 20 minutos

- Apresente os princípios, a importância e dê exemplos de Políticas de Segurança da Informação

5ª sessão – 20 minutos

- Apresente os aspectos relacionados a Segurança em Recursos humanos, abordando os princípios de menor privilégio, segregação de tarefas, rotatividade e férias obrigatórios

6ª sessão – 40 minutos

- **PBL: Mapeamento de Controles da ISO 27001**

  Cenário: Durante a realização da análise de risco como parte de trabalho para a implementação de um SGSI - Sistema de Gestão de Segurança da Informação, foram identificadas diversas vulnerabilidades.

  Você deve indicar o controle ou os controles da norma NBR ISO/IEC 27002:2013 que devem ser implementados para tratar cada uma dessas vulnerabilidades, associando indique as sessões, objetivos de controle e controle de cada vulnerabilidade, com a sua descrição. Utilize a Norma como referência para esse trabalho.

  Orientação: Utilize um arquivo único para que todos os participantes o preencham simultaneamente. Com o Microsoft Teams ou Google Docs é possível realizar essa atividade cocriada.

Vulnerabilidade	Respostas esperadas		
	Sessão	**Objetivo de controle**	**Controle**
Mesma senha utilizada por vários usuários.	9. Controle de acesso	9.2 Gerenciamento de acesso do usuário	9.2.4 Gerenciamento da informação de autenticação secreta de usuários
Inexistência de controle de mudanças no desenvolvimento de software	14. Aquisição, desenvolvimento e manutenção de sistemas	14.2 Segurança em processos de desenvolvimento e de suporte	14.2.2 Procedimento para controle de mudança de sistemas
Proteção física (porta) de acesso à sala dos servidores inadequada.	11. Segurança física e do ambiente	11.1 Áreas seguras	11.1.3 Segurança em escritórios, salas e instalações
Controle inadequado/inexistente para realização de trabalho remoto.	6 Organização da segurança da informação	6.2 Dispositivos móveis e trabalho remoto	6.2.2 Trabalho remoto
Rede elétrica instável.	11 Segurança física e do ambiente	11.2 Equipamentos	11.2.2 Utilidades
Controle de recrutamento inadequado de mão de obra.	7 Segurança em recursos humanos	7.1 Antes da contratação	7.1.1 Seleção
Falta de conscientização de segurança.	7 Segurança em recursos humanos	7.2 Durante a contratação	7.2.2 Conscientização, educação e treinamento em segurança da informação
Transferência de chaves e senhas em texto puro.	10 Criptografia	10.1 Controles criptográficos	10.1.2 Gerenciamento de chaves
Falta de proteção contra vírus e códigos maliciosos.	12 Segurança nas operações	12.2 Proteção contra códigos maliciosos	12.2.1 Controles contra códigos maliciosos
Controle inadequado de serviços terceirizados.	15 Relacionamento na cadeia de suprimento	15.2 Gerenciamento da entrega do serviço do fornecedor	15.2.1 Monitoramento e análise crítica de serviços com fornecedores
Falta de procedimento para remoção de equipamentos para manutenção.	15 Relacionamento na cadeia de suprimento	15.1 Segurança da informação na cadeia de suprimento.	15.1.1 Política de segurança da informação no relacionamento com os fornecedores
O colaborador que desconhece o procedimento em caso de eventos de segurança.	16 Gestão de incidentes de segurança da informação	16.1 Gestão de incidentes de segurança da informação e melhorias	16.1.2 Notificação de eventos de segurança da informação

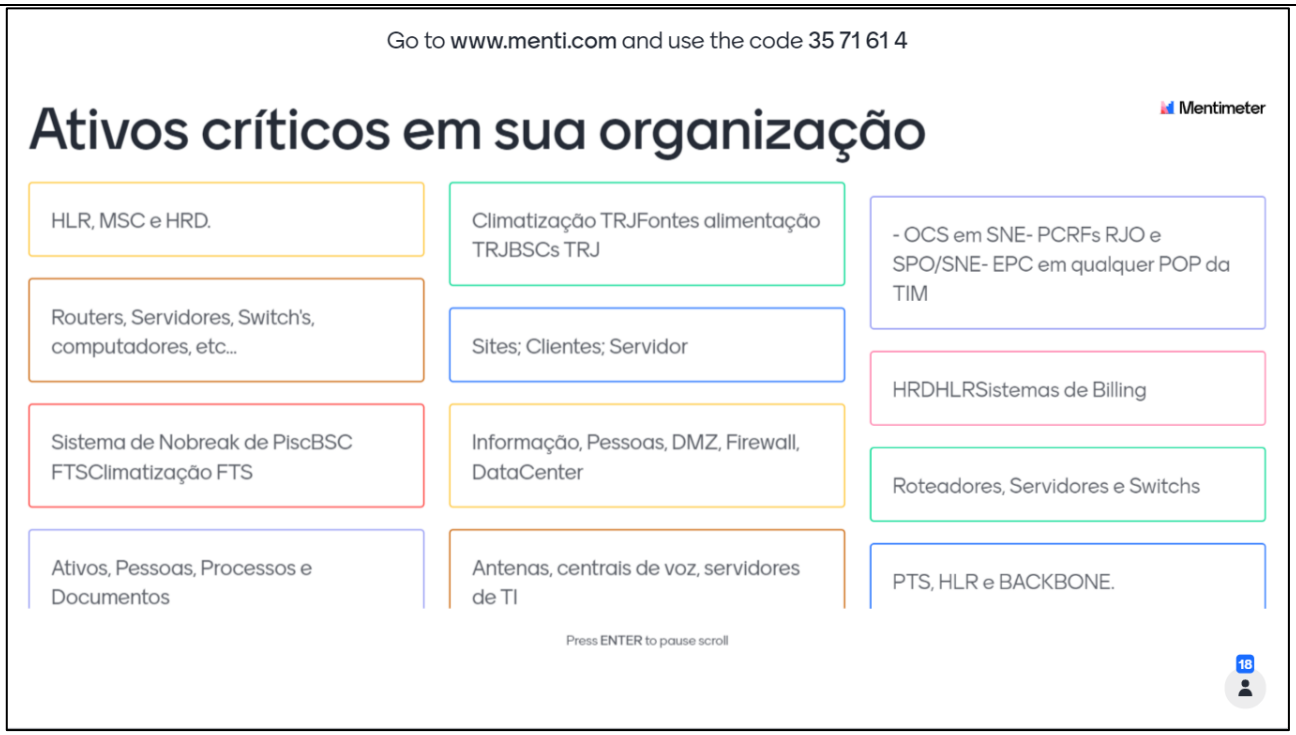
- Após o preenchimento integral do arquivo, discuta com os participantes sobre a atividade desenvolvida

7º Encontro: Riscos cibernéticos

1ª sessão – 30 minutos

- **Dinâmica de grupo: “Ativos críticos da organização”**

- Utilize o MENTIMETER para solicitar aos participantes que informem os ativos que eles consideram mais críticos em sua organização. O objetivo é fazer com que eles reconheçam que determinados equipamentos, sistemas ou ambientes requerem maiores ou melhores controles para sua proteção.



- Enquanto os ativos aparecerem na tela, discuta os resultados com os participantes

2ª sessão – 30 minutos

- Apresente os conceitos básicos sobre riscos conforme as Normas ISO 31000 e ISO 27005

3ª sessão – 20 minutos

- Apresente os controles para Gestão de Riscos

4ª sessão – 20 minutos

- Apresente o processo para identificação, análise e avaliação de riscos

5ª sessão – 20 minutos

- Apresente as técnicas para Análise de riscos e Tratamento de Riscos

6ª sessão – 60 minutos

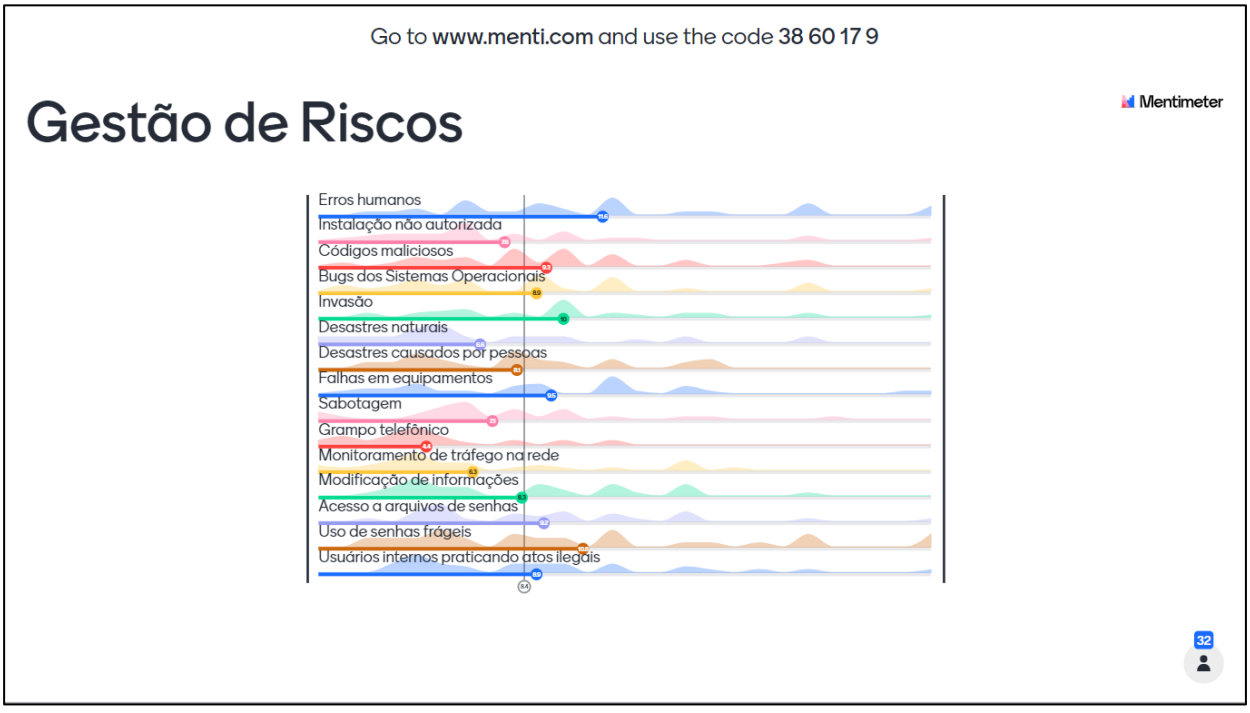
- Hands-on: **“Gestão de Riscos”**

  Essa atividade é composta de duas etapas. A primeira, individual, requer que cada participante indique qual o impacto e qual a probabilidade de uma ameaça gerar um incidente de segurança dentro da organização. A segunda, voltada para todos os participantes, vai combinar os resultados individuais em uma visão consolidada.

  1ª etapa: Solicite que os participantes preencham as colunas IMPACTO e PROBABILIDADE a cada Ameaça listada. O valor pode ser de 0 a 5 em cada linha. A coluna RISCO é o produto dos valores preenchidos nas colunas anteriores.

Ameaças	Impacto	Probabilidade	Risco
Erros humanos			
Instalação de hardware e software não autorizados			
Códigos maliciosos			
Bugs dos Sistemas Operacionais			
Invasão			
Desastres naturais			
Desastres causados por pessoas			
Falhas em equipamentos			
Sabotagem			
Grampo telefônico			
Monitoramento de tráfego na rede			
Modificação de informações			
Acesso a arquivos de senhas			
Uso de senhas frágeis			
Usuários internos praticando atos ilegais			

2ª etapa: Crie uma dinâmica no MENTIMETER e solicite que os participantes lancem o valor do RISCO em cada Ameaça listada. Enquanto a plataforma exibe a média do Risco calculado, discuta sobre os resultados com os participantes.



8º Encontro: Segurança e privacidade na era do 5G

1ª sessão – 20 minutos

- Inicie a última sessão apresentando os principais insights do Relatório “The Global Risks Report” do World Economic Forum.

2ª sessão – 60 minutos

- **Estudo de caso: "Guerra Cibernética como Risco Global"**

  Contextualização: Uma geopolítica turbulenta em ano eleitoral nos EUA, uma maré crescente de ativismo global e um novo nível de ameaças cibernéticos estão entre os "5 maiores riscos para as empresas em 2020", segundo estudo publicado pela Control Risks, uma consultoria global especializada em riscos.

  O documento "5 Maiores Riscos" foi divulgado como parte do relatório anual RiskMap da Control Risks, uma previsão de riscos globais para líderes empresariais e formuladores de política em todo o mundo, publicado hoje.

  Presente em terceira posição na lista como "Cyber warfare hits a new level", a Guerra Cibernética aparece como preocupação para líderes mundiais em todo o Mundo e, como não poderia deixar de ser, passa a ser também um grande desafio para as grandes corporações.

  Instruções:

  1. Leia o artigo: https://www.controlrisks.com/riskmap/top-5-risks/cyber-warfare-risks-increase

  2. Responda as perguntas a seguir:

     a) Na visão da Consultoria Control Risks, por que a Guerra Cibernética está entre os 5 maiores riscos globais para o ano de 2020?
     b) Quais são os países se destacam nas discussões relacionadas à Guerra Cibernética?
     c) Em sua visão, o que deve ser feito pelas grandes organizações brasileiras para saberem lidar com os riscos cibernéticos apontados no Estudo?

3ª sessão – 20 minutos

- Apresente as tecnologias emergentes que sustentarão os modelos de negócio com o 5G

4ª sessão – 20 minutos

- Apresente uma visão geral de tecnologias como reconhecimento facial, autenticação silenciosa, cidades inteligentes e Internet das Coisas

5ª sessão – 60 minutos

- **Estudo de caso: "Segurança e privacidade na era do 5G"**

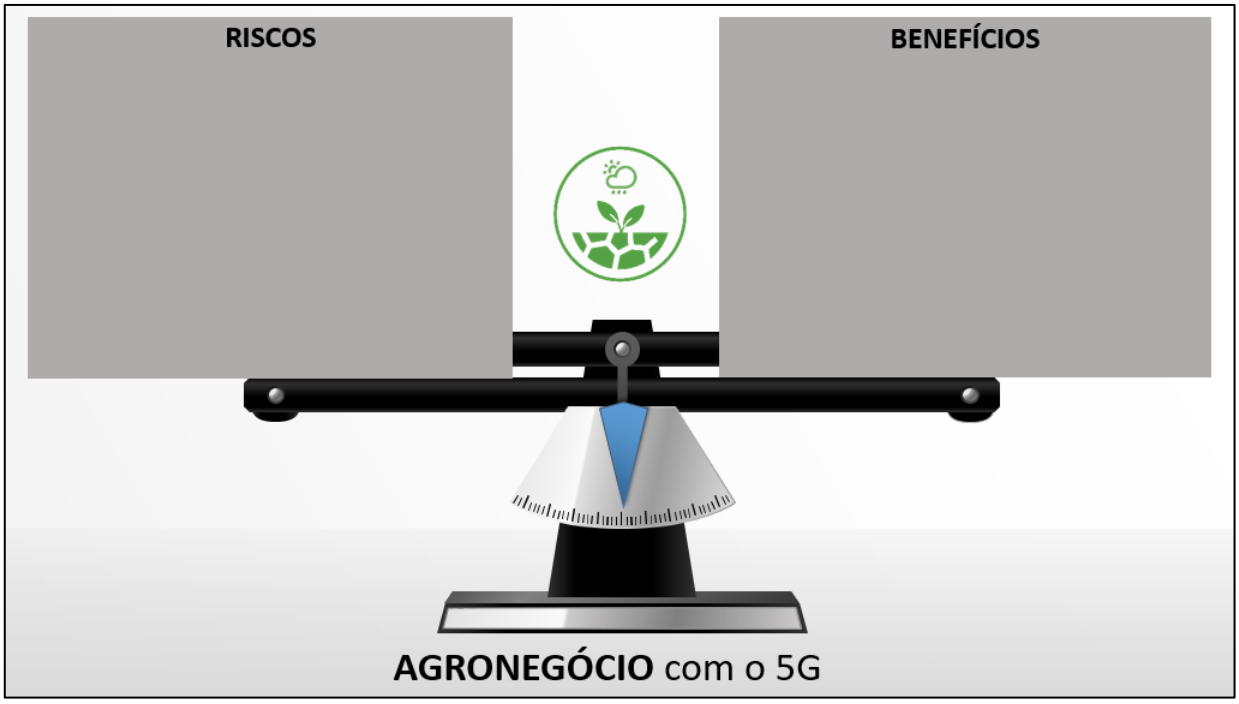
  Instruções: Como discutido nesta sessão, passaremos por uma nova era da Transformação Digital na próxima década, desta vez, fomentada com o advento do 5G, que permitirá a criação de novos modelos de negócio e trará profundas mudanças em todas as esferas da sociedade.

Para cada nova tecnologia ou processo de negócio temos também as questões relacionadas à Segurança Digital.

Neste Estudo de Caso, você está convidado a colocar em uma balança quais os benefícios alcançados com o 5G e que estarão diretamente relacionados à um novo panorama de ameaças dado um segmento específico.



Em seguida, divididos em 5 grupos, escolha um segmento e preencha a Apresentação compartilhada com os RISCOS à segurança digital e os BENEFÍCIOS da inovação tecnológica.



Ao final, apresente o resultado para os demais participantes.