INSTITUTO SUPERIOR
DE TECNOLOGIAS
AVANÇADAS DE LISBOA

Prevenir um ataque de *phishing*

A importância da formação dos Colaboradores

Paulo Ricardo Saramago Dias

N.º aluno: 99991939

Dissertação para obtenção do Grau de Mestre em

INFORMÁTICA

Júri

Presidente: Professora Doutora Andreia Cristina Teles Vieira

Arguente: Professor Dr. Arnaldo Emanuel de Almeida da Silveira Costeira

Orientador: Professor Doutor Pedro Ramos dos Santos Brandão

Dezembro, 2021

Agradecimento

Este meu percurso académico, que se iniciou com a Licenciatura, enveredou pela Pós-Graduação e culminou com o Mestrado, foi um desafio pessoal, profissional e familiar, concluído com o apoio de todos nas diversas esferas.

Ao nível profissional, agradeço o apoio da empresa onde trabalho, em particular dos meus responsáveis hierárquicos e Colegas, que me possibilitaram desenvolver a investigação empírica em ambiente real e ajustado ao meu contexto laboral. A experiência foi desafiante mas rica na medida em que pude contribuir para melhorar o contexto organizacional.

No âmbito académico, agradeço a todos os Professores e equipa do ISTEC, pela sua disponibilidade constante e pela exigência que tornou este percurso mais profícuo. Um agradecimento especial ao meu orientador, Professor Pedro Brandão, e ao Professor Paulo Duarte pelo acompanhamento ímpar na preparação desta dissertação.

Agradeço também à minha família e amigos pela compreensão e apoio nas ausências em momentos importantes e nos constantes momentos de recolhimento ao longo deste tempo. Terminar esta dissertação só foi possível convosco ao meu lado.

Resumo

A crescente utilização dos Sistemas de Informação e o aumento de utilizadores, no contexto empresarial, têm trazido desafios acrescidos no âmbito da Cibersegurança. Estudos e estatísticas indicam que a maioria dos ataques explora os comportamentos e vulnerabilidades humanos. Os ataques de Engenharia Social, nomeadamente os ataques de *phishing*, têm aumentado, revelando a importância do desenvolvimento de uma Cultura de Cibersegurança no seio organizacional.

Para salvaguardar a Cibersegurança, ao mesmo tempo que se assegura a produtividade e autonomia dos utilizadores dos Sistemas de Informação, a formação apresenta-se como uma solução eficaz, uma vez que contribui ativamente para a construção de uma Cultura de Cibersegurança e promove a resiliência dos Colaboradores.

A presente investigação, desenvolvida no contexto particular de um operador de Transporte Público Urbano de Superfície de Passageiros, teve como objetivo desenvolver um módulo formativo que contribua para prevenir potenciais ataques de *phishing* e promover a Cultura de Cibersegurança. Explora a forma como os Colaboradores respondem a um ataque de *phishing*, a sua perceção sobre a Cultura de Cibersegurança da empresa e sobre o seu papel enquanto agentes ativos na construção desta Cultura. Reforça, ainda, a importância da formação na prevenção de um ataque de Engenharia Social.

Palavras-chave: *phishing*, fator humano, Cultura de Cibersegurança, formação em Cibersegurança.

Abstract

The increasing use of Information Systems and the increase of users in the business context have brought increased challenges in the field of Cybersecurity. Studies and statistics indicate that most attacks exploit human behaviors and vulnerabilities. The attacks of Social Engineering, namely the phishing attacks, have increased, revealing the importance of the development of a Cybersecurity Culture in the organizational environment.

In order to safeguard Cybersecurity, while ensuring the productivity and autonomy of the users of Information Systems, training presents itself as an effective solution, since it actively contributes to the construction of a Cybersecurity Culture and promotes the resilience of Employees.

This research, developed in the particular context of a Public Urban Passenger Area Transport Operator, aimed to develop a training module that contributes to prevent potential phishing attacks and promote the Cybersecurity Culture. Explore how Employees respond to a phishing attack, their perception of the company's Cybersecurity Culture, and their role as active agents in building this Culture. It also reinforces the importance of training in the prevention of a Social Engineering attack.

Keywords: *phishing, human factor, Cybersecurity Culture, Cybersecurity training.*

ÍNDICE

Lista de abreviaturas e siglas

AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação
CISO - Chief Information Security Officer
CNCS - Centro Nacional de Cibersegurança
ENISA - The European Union Agency for Cybersecurity
EOP - Exchange Online Protection
INCoDe.2030 - Iniciativa integrada de política pública dedicada ao reforço de competências digitais
ITU - International Telecommunication Union
RGPD – Regulamento Geral de Proteção de Dados
SI - Sistemas de Informação

Índice de gráficos

Introdução

A presente dissertação focou-se na importância da formação dos Colaboradores na prevenção de um ataque de *phishing*. A investigação decorreu no contexto de um operador de Transporte Público Urbano de Superfície de Passageiros que opera na cidade de Lisboa.

Numa análise preliminar à investigação, identificou-se uma utilização indevida dos *e-mails* institucionais para fins pessoais, nomeadamente, para registo em sites e plataformas externas. Através da análise das plataformas tecnológicas de segurança internas da Empresa, constatou-se a efetiva receção de *e-mails* de *spam* com conteúdo potencialmente malicioso, de carácter pessoal, e enviados para as caixas de correio profissionais dos utilizadores.

Com base neste contexto, e de forma a definir as fases metodológicas da investigação empírica, foi formulado o problema:

1. De que forma os Colaboradores respondem a um ataque de *phishing*?
2. Qual a perceção dos Colaboradores sobre a Cultura de Cibersegurança da empresa?
3. Qual a perceção dos Colaboradores sobre o seu papel enquanto agentes ativos da Cultura de Cibersegurança da empresa, em particular, na prevenção de um ataque de *phishing*?
4. Qual a importância da formação na prevenção de um ataque de *phishing*?

O objetivo geral da dissertação foi desenvolver um módulo formativo que contribua para prevenir potenciais ataques de *phishing* e promover a Cultura de Cibersegurança na organização.

Os objetivos operacionais da investigação deram resposta às questões formuladas na problemática. Foram realizados dois ataques simulados, um num momento inicial, outro no momento final, para aferir de que forma os Colaboradores da empresa respondem a um ataque de *phishing*. Após a realização do primeiro ataque simulado, foi aplicado um inquérito para auscultar a perceção dos Colaboradores sobre a Cultura de Cibersegurança da empresa e sobre os métodos que contribuem para prevenir um ataque de *phishing*, entre eles o papel dos próprios utilizadores. Seguiu-se a disseminação de uma ação de sensibilização sobre o tema da Cibersegurança. Concluiu-se a investigação empírica com a realização de um segundo ataque simulado, o que permitiu comparar resultados.

Identificaram-se como termos chave da presente dissertação: o *phishing*, o fator humano, a Cultura de Cibersegurança e a formação em Cibersegurança.

A investigação demonstrou relevância para o contexto organizacional, no sentido de minimizar os riscos de um potencial ataque de *phishing*, dando provimento à Estratégia Nacional

de Segurança no Ciberespaço[1] que integra como objetivo estratégico, promover a educação, a consciencialização e a prevenção. Iniciou-se com o desenvolvimento do Estado de Arte, reunindo informação teórica e empírica, relevante, que enquadrou o tema da dissertação e reforçou a sua pertinência. Seguiu-se a definição das fases metodológicas de suporte à investigação empírica. Concluiu-se com uma reflexão crítica sobre os resultados obtidos na investigação empírica, correlacionados com as referências do Estado de Arte, encaminhando para uma proposta futura de implementação de um módulo formativo relacionado com a prevenção de ataques de *phishing*. A estrutura do presente documento corresponde às fases de investigação anteriormente detalhadas.

[1] Estratégia Nacional de Segurança do Ciberespaço – Fonte: https://dre.pt/home/-/dre/67468089/details/maximized

Capítulo 1 – Estado de Arte

No presente capítulo é reunida informação teórica e empírica, relevante, que enquadra o tema da dissertação e reforça a pertinência da investigação, que deu origem ao desenvolvimento de um módulo formativo, com o objetivo de prevenir potenciais ataques de *phishing* e promover a cultura de Cibersegurança na organização em análise.

O enquadramento teórico teve por base a revisão bibliográfica que permitiu abordar a correlação entre os Sistemas de Informação e os ataques de Engenharia Social, em particular os ataques de *phishing*, bem como a importância da Cultura de Segurança e da formação no âmbito da Cibersegurança ao nível empresarial. No contexto da Cultura de Segurança, existem três grandes vetores – tecnologias, processos e pessoas – sendo que a abordagem nesta dissertação foi direcionada para o fator humano, evidenciando as vulnerabilidades que lhe são associadas. Da revisão bibliográfica e da análise de alguns estudos empíricos, resultou, ainda, a escolha da metodologia adequada para a investigação empírica desenvolvida.

1.1. Os Sistemas de Informação nas empresas

Os Sistemas de Informação (SI) têm permitido às empresas uma vantagem competitiva, aliada à facilidade e adaptabilidade com que trocam, armazenam e manipulam informação crítica para os negócios. Entre as vantagens dos Sistemas de Informação, é possível identificar: a rapidez e eficiência com que se comunica; a globalização, no sentido de quebrar barreiras geográficas e culturais; a disponibilidade da informação; e o aumento significativo da produtividade. Os Sistemas de Informação asseguram o acesso a dados e informação, devendo ser, no entanto, devidamente monitorizados, seguros e protegidos. Estes sistemas recorrem maioritariamente a tecnologias de informação e comunicação, de acordo com os objetivos que servem dentro da organização (Gouveia & Ranito, 2004).

Al-Mamary *et al* (2014) identificam diversos tipos de Sistemas de Informação utilizados pelas empresas. De acordo com os autores, podem ser utilizados sistemas de: processamento de transações para registar as rotinas diárias do negócio; automatização de tarefas administrativas; monitorização dos processos industriais e/ou físicos; informação de gestão; suporte à tomada de decisões estratégicas e de negócio; entre outros. Estes sistemas podem ser utilizados de forma individualizada ou combinada.

No contexto atual, é possível afirmar que o sucesso de uma empresa é diretamente proporcional à diversidade e qualidade dos Sistemas de Informação que são utilizados, bem como

à capacidade de utilizar corretamente os recursos disponíveis (Lipaj & Davidavičienė, 2013). Stair e Reynolds (2015) reforçam esta afirmação, defendendo que, para usufruir de todo o potencial dos Sistemas de Informação, é necessária uma cultura computacional e uma cultura dos Sistemas de Informação, isto é, obter os recursos mas, também, desenvolver o conhecimento e as competências para os utilizar devidamente.

Quando se aborda o tema da implementação e utilização dos Sistemas de Informação, numa organização, não é somente a vertente tecnológica que está em causa. O fator humano é determinante para o sucesso, pelo que se torna imprescindível envolver os utilizadores, promovendo-se a aceitação e o interesse relativamente aos sistemas com que interagem (Dezdar & Sulaiman, 2009).

Os Sistemas de Informação são uma combinação das tecnologias e dos recursos humanos que as utilizam nos processos e procedimentos de uma empresa (Awais *et al*, 2012). Esta definição encaminha para uma correlação entre as tecnologias, os processos e as pessoas.

Hardcastle (2008) identifica cinco recursos básicos que compõem os Sistemas de Informação empresariais: pessoas, *Hardware*, *Software*, comunicações e dados. No grupo dos recursos humanos (pessoas), inclui os programadores e técnicos de suporte, os gestores e administradores de sistemas, bem como os utilizadores.

Ao nível dos utilizadores, é de relevar a atribuição de computadores individuais, fator que permite a agilização dos processos e a autonomia de quem os utiliza, mas que se pode manifestar num conjunto de desafios acrescidos em termos de controlo das utilizações individualizadas e dos riscos inerentes (Hardcastle, 2008).

Considerando esta correlação entre os recursos tecnológicos e os recursos humanos, Gouveia e Ranito (2004) apresentam uma visão sociotecnológica dos Sistemas de Informação. Nesta perspetiva, os recursos humanos são vistos como um fator de extrema importância para o sistema, não só, porque os Sistemas de Informação utilizados devem ser ajustados às suas necessidades e ao seu nível de interação com os dados e informação, como, também, deve ser considerada a formação dos utilizadores uma vez que esta interação exige o desenvolvimento de diversas competências.

Ao abordar os Sistemas de Informação, outros conceitos emergem, nomeadamente o de segurança. Existem diversas ameaças que podem pôr em causa a segurança dos sistemas e da própria informação. Entre as mais comuns, Hardcastle (2008) refere: as catástrofes naturais, a sabotagem (industrial ou individual), o vandalismo, o roubo, o *hacking* e os vírus.

Algumas estimativas sugerem que 40% a 65% dos danos provocados nos Sistemas de Informação, e nos dados críticos das empresas, são resultado de um erro humano. Os valores revelam que uma grande percentagem das falhas de segurança é, portanto, da responsabilidade dos utilizadores, podendo ser intencional ou derivada da falta de conhecimento e/ou de competências (Hardcastle, 2008).

Esta correlação e o aumento de ataques de *hacking* estão intimamente ligados à utilização da Internet, e ao acesso generalizado à mesma, para fins organizacionais. Sobre a utilização da Internet, a visão sociotecnológica evidencia o papel do utilizador, uma vez que, neste livre acesso a um mundo de informação, é da sua responsabilidade avaliar a qualidade e fidedignidade dos recursos disponíveis (Gouveia & Ranito, 2004).

Perante as ameaças de segurança, existem quatro grandes abordagens que permitem garantir a integridade dos Sistemas de Informação: contenção ou controlo de acesso à informação; dissuasão ou reforço das penalizações por utilização não autorizada; ofuscamento, na medida em que a informação está distribuída ou mesmo oculta; e recuperação dos dados (Hardcastle, 2008).

Existem, ainda, diferentes tipologias de controlo aplicáveis aos Sistemas de Informação. De referir: a proteção física; o controlo biométrico; o controlo das telecomunicações; o controlo de falhas; e a realização de auditorias (Hardcastle, 2008).

Para reforçar a segurança e a integridade dos Sistemas e da Informação é, também, aconselhado um conjunto de técnicas, nomeadamente: a implementação de uma política formal de segurança, que deve ser do conhecimento de todos os intervenientes e compreendida pelos mesmos; a utilização de diferentes níveis de validação do utilizador, para além do uso generalizado de *passwords;* a encriptação de dados críticos; a implementação de procedimentos organizacionais que derivam da política de segurança; e a realização constante de *backups* (Hardcastle, 2008).

De facto, as organizações dependem, cada vez mais, do domínio cibernético para funcionarem. Este domínio integra: os utilizadores (pessoas); os dispositivos e *Software* com que estes interagem; a lógica utilizada pelos dispositivos e sistemas; os circuitos e respetiva localização; e os sistemas físicos. O fator humano não pode ser dissociado do domínio cibernético. A crescente dependência da informação e da tecnologia vem acompanhada de uma crescente preocupação com as ameaças e riscos relacionados com a confidencialidade e integridade dos sistemas existentes nas organizações (Wout, 2019).

Constata-se, assim, que o fator humano é indissociável dos Sistemas de Informação, e que não é possível abordar este conceito sem relacioná-lo com o de Cibersegurança.

As empresas enfrentam o desafio de definir políticas, procedimentos e ferramentas de segurança, cruciais para proteger os dados, a informação e a própria infraestrutura. Segundo Gouveia e Ranito (2004), este desafio torna-se, ainda mais, evidente quando aplicado a empresas e organismos do setor público que trabalham dados muito sensíveis e oficiais, o que se aplica à organização analisada na presente dissertação.

1.2. Ataques de Engenharia Social – O *phishing*

A Engenharia Social é o processo pelo qual se tenta convencer alguém de algo fictício, explorando a ingenuidade do alvo. Os ataques de Engenharia Social tendem a influenciar e controlar os comportamentos da vítima explorando as suas vulnerabilidades emocionais (Centro Nacional de Cibersegurança [CNCS], s.d.).

De acordo com o Centro Nacional de Cibersegurança (CNCS, s.d.)[2] a Engenharia Social é um dos maiores riscos de segurança das pessoas e das organizações.

Numa perspetiva sociotecnológica, este tipo de ataques acontece devido ao desconhecimento dos utilizadores, quer em relação às políticas de segurança, quer em relação às reais consequências que os seus comportamentos podem originar. Evidenciam-se as habilidades psicológicas do atacante para conseguir manipular e controlar a vítima, de forma a conseguir extrair informação sensível (Pais *et al*, 2020).

Existem duas categorias principais para classificação dos ataques de Engenharia Social. Os ataques baseados nos computadores ou tecnologias e os ataques de manipulação direta dos indivíduos. O *phishing* enquadra-se na primeira categoria, ou seja, trata-se de um ataque baseado na tecnologia, embora o indivíduo seja um meio para atingir o fim (Thapar, 2007).

O *phishing* é uma tentativa fraudulenta de aceder a informação pessoal ou financeira. A vítima pode ser abordada por *e-mail*, chamada telefónica ou mensagem. A comunicação é aparentemente credível e remete para fontes oficiais, tais como entidades bancárias ou financeiras. Estes ataques são realizados de forma maciça para diversos utilizadores/clientes (Pais *et al*, 2020). Encoberto pela necessidade de verificação de dados, o atacante solicita à vítima os dados que lhe irão permitir aceder ao sistema, tais como o utilizador, *password*, número de cartão ou códigos de acesso, entre outros (Thapar, 2007).

[2] Centro Nacional de Cibersegurança (CNCS) – Autoridade nacional, especialista em matéria de Cibersegurança, que atua junto de diferentes entidades e operadores garantindo a utilização otimizada do ciberespaço, em Portugal. Fonte: https://www.cncs.gov.pt/

Salahdine e Kaabouch (2019), referem cinco tipologias de *phishing*: *spear phishing, whaling phishing, vishing phishing, interactive voice response phishing* e *business e-mail compromise phishing*.

No caso particular da técnica de *spear phishing*, trata-se de um ataque focalizado, levando a que a vítima acredite que o *e-mail* recebido é proveniente de alguém dentro da organização ou de alguém com outro tipo de autoridade. Ao aceder aos dados pessoais do utilizador, o atacante pretende aceder ao Sistema de Informação da empresa (Pais *et al*, 2020). Esta tipologia de ataque revela a importância, para as organizações, de sensibilizar os colaboradores, minimizando os riscos de acesso a informação crítica ou colocar em causa a integridade dos sistemas e da infraestrutura da empresa.

Em 2017, Portugal era o 8º país da União Europeia com maior risco de cibercrime e o 3º país da União Europeia maior vítima de cibercrimes. Embora os níveis de utilização do domínio cibernético sejam menores que noutros países, este posicionamento demonstra a relevância de se abordar o tema da Cibersegurança, dedicando uma especial atenção aos ataques de Engenharia Social (Barros, 2018).

O desconhecimento no âmbito da Cibersegurança é alarmante e deve ser corrigido uma vez que potencia comportamentos de risco por parte dos utilizadores. Mais de 99% dos ataques exploram as características e comportamentos humanos em vez de explorarem as vulnerabilidades dos sistemas informáticos. A maioria dos cibercriminosos define as suas ações e motivações de ataque, focando-se no fator humano (Gonçalves & Nunes, 2019).

Entre os principais incidentes com origem no fator humano, encontra-se: a abertura de anexos ou *links* de *e-mails* de *spam* e/ou de fontes não fidedignas, muitas delas com características maliciosas; partilha indevida de *passwords* e de informações privadas e corporativas; utilização do *e-mail* profissional para fins pessoais; e acesso a *websites* não fidedignos (Gonçalves & Nunes, 2019). De relevar que alguns destes incidentes foram identificados durante a investigação empírica, desenvolvida no âmbito desta dissertação, corroborando o nível de ocorrências em contexto empresarial.

Wout (2019) aborda a compreensão do domínio humano, como uma das dimensões imperativas para uma Cultura de Cibersegurança nas organizações. O autor defende que esta compreensão passa por uma investigação profunda sobre cada colaborador, sobre o que pensa e, sobretudo, sobre o que o faz "clicar" em algo desconhecido.

Na atualidade do mundo cibernético o risco é iminente. Ao abrir um *e-mail* de *phishing*, o utilizador/colaborador poderá ceder ao atacante um ponto de entrada no Sistema de Informação

da empresa. Já dentro do sistema, o atacante poderá aceder e bloquear informações críticas para o negócio. Assim, constata-se que a ameaça interna do comportamento humano é um dos aspetos de segurança mais difíceis de controlar (Huang & Pearlson, 2019).

Segundo Bowen *et al* (2011), o comportamento vulnerável das pessoas pode levar a riscos indesejados, tornando a empresa suscetível a ataques, nomeadamente de *phishing*. Neste sentido, torna-se preponderante que as organizações dediquem a necessária atenção ao fator humano, assegurando que os seus colaboradores estão devidamente sensibilizados e que têm o conhecimento necessário no âmbito da Cibersegurança. Esta preocupação leva à construção de uma Cultura de Cibersegurança na organização cujo sucesso depende do investimento que lhe é dedicado.

1.3. Importância da Cultura de Cibersegurança nas organizações

Da análise dos subcapítulos anteriores, é possível constatar que a crescente utilização dos Sistemas de Informação, por parte das organizações, levará a um consequente crescimento do risco de ciberataques, uma vez que haverá uma maior exposição da informação e um maior número de utilizadores a interagir com o domínio cibernético. Fica, igualmente, claro que os ataques de Engenharia Social têm vindo progressivamente a aumentar e que o fator humano não pode ser descurado. Uma vez que as organizações são compostas por pessoas, é explorado no presente subcapítulo o conceito de Cultura de Cibersegurança.

Ao contexto organizacional associa-se, então, o conceito de Cultura de Cibersegurança. A ENISA - *The European Union Agency for Cybersecurity*[3] (2018, p. 5) define este conceito como o conjunto de "conhecimento, crenças, perceções, atitudes, suposições, normas e valores das pessoas em relação à segurança cibernética e como eles se manifestam no comportamento das pessoas com as tecnologias da informação". A agência refere que esta cultura é parte da própria cultura organizacional, podendo ser moldada e transformada. No entanto, a Cultura de Cibersegurança requer uma necessidade de adaptabilidade muito maior, uma vez que os negócios e os ambientes estão em permanente mudança.

A ENISA (2018) afirma que uma Cultura de Cibersegurança bem sucedida influencia a forma de pensar de todos os indivíduos, promovendo resiliência contra ciberataques, em particular os que derivam da Engenharia Social, evitando impor outras medidas de segurança que inibam a eficácia do desempenho de funções de cada colaborador. Outro fator preponderante para o sucesso

[3] ENISA - *The European Union Agency for Cybersecurity* – Agência da União Europeia que se dedica a alcançar um elevado nível de Cibersegurança, comum a toda a Europa. Fonte: https://www.enisa.europa.eu/

é o envolvimento dos próprios colaboradores na criação da Cultura de Cibersegurança. Não sendo imposta, será mais facilmente apropriada e compreendida. A par destas premissas, será necessário que todos os colaboradores disponham das ferramentas, conhecimento, competências e compreensão sobre o seu papel e contributo.

De acordo com as referências nos subcapítulos anteriores, a maior ameaça à privacidade e segurança da organização são os próprios Colaboradores. A consciencialização sobre os riscos é fundamental para a cadeia de segurança da empresa, uma vez que, embora devidamente protegida pelas ferramentas tecnológicas, se mantém desprotegida sem uma Cultura de Cibersegurança (Georgiadou *et al*, 2020).

Georgiadou *et al* (2020) desenvolveram uma investigação onde constataram que a tendência da segurança na informação está a abandonar a abordagem meramente técnica, passando para uma abordagem sociocultural. Nesta abordagem, aumentar a consciência de segurança passa por: definir métodos de avaliação interativos; utilizar técnicas e ferramentas apelativas que envolvam os colaboradores; implementar programas de formação; e identificar as vulnerabilidades humanas. Esta consciência concorre para o fortalecimento da Cultura de Cibersegurança.

De facto, a cibersegurança organizacional vai muito além das tecnologias utilizadas, sendo necessário que todas as pessoas dentro da empresa ajam no sentido de reduzir o risco (Huang & Pearlson, 2019).

A ENISA (2018), identifica que o fator humano continua a ser o elo mais fraco na cadeia de segurança e que o investimento na Cultura de Cibersegurança, na organização, pode mitigar este risco.

A Cultura de Cibersegurança distingue-se da segurança da informação. Exige muito mais do que um mero compromisso e cumprimento da política de segurança instituída. Implica um verdadeiro envolvimento de todas as pessoas que compõem a organização (Huang & Pearlson, 2019).

A partilha de informação e a aprendizagem organizacional geram sistemas e práticas de Cibersegurança altamente relevantes que contribuem para a resiliência da organização e para que os indivíduos estejam mais conscientes dos riscos. Esta aprendizagem servirá igualmente para identificar os colaboradores mais vulneráveis a tornarem-se vítimas de um ataque de Engenharia Social (Trim *et al*, 2014).

Huang e Pearlson (2019) identificam seis mecanismos principais que contribuem para a criação e potenciação de uma Cultura de Cibersegurança nas organizações. Em primeiro lugar, a

definição e reconhecimento de um indivíduo, ou equipa, responsável formalmente por construir e cultivar essa cultura, identificado pelo termo em inglês "CISO" - *Chief Information Security Officer*. Em segundo lugar, a inclusão das competências e comportamentos relativos à Cibersegurança no processo formal de avaliação de cada colaborador. Em terceiro lugar, a criação de um sistema de incentivos e penalizações com relação direta aos comportamentos preventivos ou de risco, respetivamente, no âmbito da Cibersegurança. Em quarto lugar, os sistemas de aprendizagem organizacional que podem passar por sessões de *mentoring* ou outros sistemas de partilha de informação, formal ou informal. Em quinto lugar, a comunicação interna, baseada em mensagens sobre Cibersegurança transmitidas de forma bem estruturada e com *design* apelativo. Por último, e considerando o tema mais relevante para a presente dissertação, a formação em Cibersegurança.

Manifesta-se, assim, evidente a importância da formação e da sensibilização na construção de uma Cultura de Cibersegurança bem sucedida nas organizações, pelo que no subcapítulo seguinte é explorada a forma como podem ser implementadas.

1.4. A Formação como um dos contributos para a Cultura de Cibersegurança

Um estudo da Associação Portuguesa para a Promoção da Segurança da Informação[4] refere que:

> "Os temas da sensibilização e da formação em Segurança da Informação são cruciais para a implementação e manutenção de uma Cultura de Segurança nas instituições. Em questões de segurança o conhecimento é a chave para a tomada de decisões corretas e quanto mais disseminado estiver maior a resiliência das instituições." (Associação Portuguesa para a Promoção da Segurança da Informação [AP2SI], 2015, p. 7)

Da aplicação do inquérito, no âmbito do mesmo estudo, constatou-se que a formação é, na realidade, uma área deficitária nas organizações e que o *phishing* é um dos incidentes mais frequentes.

Em 2015, o Governo Português definiu a Estratégia Nacional de Segurança no Ciberespaço[5] que integrou seis objetivos estratégicos, um dos quais, promover a educação, a consciencialização

[4] Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI) – Associação sem fins lucrativos e de natureza privada que contribui para o desenvolvimento da Segurança da Informação em Portugal, através da sensibilização e da promoção de orientações que reforçam a qualificação dos indivíduos e organizações. Fonte: https://ap2si.org/

[5] Estratégia Nacional de Segurança do Ciberespaço – Fonte: https://dre.pt/home/-/dre/67468089/details/maximized

e a prevenção.

Em 2017, um estudo publicado pela *International Telecommunication Union* (ITU)[6], referia que uma das áreas mais críticas em Portugal, em termos de Cibersegurança, era precisamente a formação.

Num documento redigido pela ENISA, em novembro de 2017, a agência refere que a sensibilização e a formação influenciam o conhecimento e, em combinação com a cultura organizacional, determinam o comportamento dos indivíduos e contribuem para uma melhor Cultura de Cibersegurança. Defende, igualmente, que todos os Colaboradores da organização devem receber formação, mesmo que num nível básico, de forma a construírem uma consciência do risco e desenvolverem competências relacionadas com as funções que desempenham. Potenciar um comportamento seguro implica ministrar formação de forma personalizada e significativa (ENISA, 2018).

Em Portugal, um relatório emitido pelo Gabinete de Estratégia e Estudos do Ministério da Economia, destaca a iniciativa Portugal INCoDe.2030[7] como um elemento potenciador das competências digitais, nomeadamente em termos de Cibersegurança, referindo que a "aposta na formação digital dos recursos humanos poderá permitir antecipar e prevenir questões de Cibersegurança mas a mudança de mentalidades na gestão das empresas passa também por uma maior formação dos gestores das empresas.", relevando o foco na importância da formação (Barros, 2018, p. 49).

A sensibilização e a transmissão de conhecimentos afiguram-se como uma das formas de criar bons hábitos, mitigando os comportamentos de risco em matéria de Cibersegurança. É importante manter os conhecimentos atualizados e adaptar os conteúdos a transmitir aos desafios que vão surgindo, para obter o sucesso e a eficácia, tornando a Cultura de Cibersegurança sólida. Esta cultura pode ser alcançada através da consciencialização, formação e educação das pessoas (Gonçalves & Nunes, 2019).

A formação em Cibersegurança deve incluir módulos formativos e exercícios que permitam desenvolver competências e conhecimentos no âmbito da Cibersegurança. Este tipo de formação tem como objetivo promover a segurança da informação, sensibilizar os utilizadores para a importância da Cibersegurança, formar tecnicamente utilizadores com acesso a informação crítica ou, ainda, aprofundar competências nas equipas de segurança internas (Huang & Pearlson, 2019).

[6] *International Telecommunication Union* (ITU) – Agência especializada das Nações Unidas para as Tecnologias de Informação e Comunicação. Fonte: https://www.itu.int/en/Pages/default.aspx

[7] INCoDe.2030 – Iniciativa integrada de política pública dedicada ao reforço de competências digitais. Fonte: https://www.incode2030.gov.pt/

Algumas organizações optam por um módulo de formação inicial, no momento da contratação, outras optam por um curso periódico de atualização de conhecimentos. Existem, também, organizações que aplicam formações pontuais, de acordo com algumas necessidades identificadas, ou optam pelo envio de *pop-ups* esporádicos que remetem para determinados conteúdos de Cibersegurança. Na prática, constata-se que a diversidade de métodos e a regularidade da formação são pontos muito relevantes para o sucesso e eficácia da mesma (Huang & Pearlson, 2019).

O plano de formação deve integrar uma série de momentos que promovam a consciencialização sobre a Cibersegurança. Simultaneamente, devem promover a coesão e motivação necessárias à adesão às regras e políticas definidas pela empresa. Podem ser, também, concebidos outros eventos ou momentos formativos baseados em necessidades específicas. Para que seja bem sucedido, o plano formativo deve focar-se em alguns aspetos importantes, nomeadamente: a identificação de formadores credenciados de forma a assegurar uma formação atualizada e eficaz; a realização de módulos de sensibilização e formação exclusivamente dedicados ao tema da Cibersegurança; e a escolha das metodologias corretas para cada necessidade identificada (Wout, 2019).

Em suma, pode afirmar-se que a forma mais eficaz de prevenir um ciberataque é manter toda a organização formada e sensibilizada. Do mesmo modo, a formação contribui ativamente para a construção de uma Cultura de Cibersegurança mais eficaz e o desenvolvimento da resiliência dos Colaboradores. No caso particular dos ataques de *phishing*, a formação e as ações de sensibilização permitem que os utilizadores se mantenham alerta, assumindo um grau mais elevado de suspeição sobre potenciais ataques maliciosos. Desta forma, poderão ser reduzidos os riscos de invasão dos Sistemas de Informação da empresa, o acesso indevido a informação crítica ou sensível, e eventuais danos na infraestrutura. A par dos mecanismos de defesa físicos e tecnológicos, a formação permite que os Colaboradores sejam um fator de segurança.

Capítulo 2 – Metodologia

No âmbito da presente dissertação, foi desenvolvida uma investigação empírica no contexto organizacional de um operador de Transporte Público Urbano de Superfície de Passageiros, que opera na região de Lisboa.

A investigação, com foco numa ação de melhoria, baseou-se numa metodologia orientada para a prática, utilizando uma lógica de dedução que permitiu a obtenção de conclusões, partindo dos pressupostos e problemática identificados e da análise de dados recolhidos junto da empresa e da população-alvo.

Numa análise preliminar à empresa, detetou-se uma utilização indevida dos *e-mails* corporativos, por parte da população-alvo, que sugeriu a sequência de fases metodológicas detalhadas no presente capítulo, nomeadamente, a aplicação de ataques simulados, a realização de um inquérito, a aplicação de uma ação de sensibilização e uma conclusão resultante da análise dos resultados globais de cada uma das fases de investigação.

Face ao contexto global da organização, foi objetivo da investigação empírica analisar a relação entre o papel da formação em Cibersegurança e a redução de potenciais riscos associados ao fator humano, sustentado pelo enquadramento teórico, referido no Capítulo 1, da presente dissertação.

A investigação empírica, respetivas fases e instrumentos metodológicos, pretendeu analisar o comportamento e conhecimento da população-alvo evidenciando a pertinência do desenvolvimento de um módulo formativo sobre *phishing*, justificando de que forma este poderá prevenir ou minimizar os riscos de um ciberataque. O enquadramento teórico, aliado às conclusões obtidas durante a investigação empírica teve, também, como objetivo demonstrar aos decisores da empresa que a formação em Cibersegurança potencia a Cultura de Cibersegurança.

2.1. Contexto da investigação

A empresa sobre a qual se desenvolveu a investigação empírica é um operador de Transporte Público Urbano de Superfície de Passageiros. Opera na área urbana de Lisboa, prolongando algumas das suas linhas aos concelhos limítrofes desta cidade, nomeadamente Amadora, Loures, Odivelas e Oeiras.

A empresa tem acompanhado o crescimento da cidade de Lisboa, contribuindo ativamente para o sistema de mobilidade urbana, cada vez mais integrado numa lógica de intermodalidade.

Dos três pilares estratégicos que regem a atividade da empresa destaca-se, para efeitos da presente dissertação, a modernização e qualificação da organização. Neste âmbito, os eixos de renovação dos sistemas de gestão e de monitorização, a revitalização dos quadros da empresa, a implementação de novas tecnologias e o incremento da formação[8], são os que mais impactam a investigação empírica.

A 31 de dezembro de 2020, a empresa tinha 2588 Colaboradores no seu efetivo global, dos quais 1870 Tripulantes (Motoristas e Guarda-Freios) e 718 afetos a áreas corporativas, manutenção e suporte.

A média de idades era de 42 anos no grupo de Tripulantes e de 50 anos no restante efetivo. A antiguidade média, por sua vez, era de 12 anos no grupo de Tripulantes e de 23 anos no restante efetivo.

A estratificação por género era de 1745 homens e 125 mulheres, no grupo de Tripulantes, e de 572 homens e 146 mulheres, nas áreas corporativas.[9]

De referir, ainda, que a política de mobilidade interna da empresa depreende a afetação de Colaboradores a novas funções, ou seja, Colaboradores que desempenham, por exemplo, funções operacionais, podem ser reenquadrados por motivo de inaptidão, passando a desempenhar funções administrativas. Neste contexto, um utilizador, que nunca teve qualquer tipo de interação com os Sistemas de Informação da empresa, passa a ter, pelo que o desenvolvimento de competências e a aquisição de conhecimentos se manifesta relevante.

Desde 2010 que a totalidade dos Colaboradores da empresa tem caixa de correio eletrónico corporativa. Antes desta data, a atribuição de um *e-mail* institucional era exclusiva para os trabalhadores que tinham um posto de trabalho fixo. Em 2010, foi estendida esta atribuição a todos os Colaboradores admitidos na empresa. No caso do grupo de Tripulantes e dos Colaboradores afetos às áreas de manutenção e suporte, as caixas de correio têm alojamento e gestão externos à empresa. No caso dos Colaboradores afetos às áreas corporativas, as caixas de correio têm alojamento na infraestrutura da empresa e gestão interna.

Desde 2017, a empresa tem investido no eixo tecnológico, quer na perspetiva do serviço prestado aos Clientes, quer nos Sistemas de Informação internos, de suporte à gestão dos processos e procedimentos, na perspetiva dos seus Colaboradores.

[8] Fonte: Plano de Atividades e Orçamento 2021 da empresa
[9] Fonte: Direção de Gestão de Pessoas da empresa. Referência dos dados: 31-12-2020.

2.2. Ações de investigação e instrumentos

As várias fases de investigação tiveram como objetivo principal analisar a relação entre o papel da formação em Cibersegurança e a redução de potenciais riscos, associados ao fator humano, na prevenção de ataques de *phishing*.

2.2.1. Caracterização e população-alvo

A investigação empírica iniciou-se com a recolha de informação necessária à caracterização do contexto e da população-alvo. Com este objetivo, foram consultados documentos oficiais e normativos internos da empresa e contactadas as áreas corporativas da empresa com acesso à informação não disponível publicamente.

Para efeitos de investigação, foi selecionada uma população, com características profissionais, e de relação com os Sistemas de Informação da empresa, comuns. Esta seleção teve como objetivo generalizar os resultados. Embora a restante população possa não representar o mesmo risco ao nível da Cibersegurança interna, pode assumir-se a generalização dos resultados obtidos no que diz respeito à Cultura de Cibersegurança.

A seleção da população foi criterial. A caracterização global do efetivo permitiu focar a investigação empírica num grupo de Colaboradores que possuem caixa de correio corporativa, alojada na infraestrutura interna/híbrida. Trata-se de um total de 300 utilizadores, cujos comportamento e ações foram analisados no trabalho de campo da presente dissertação. Profissionalmente, utilizam um computador individual, o *e-mail* institucional como ferramenta de trabalho, e um conjunto de sistemas, plataformas e aplicativos adequados às particularidades das funções que desempenham. Estes utilizadores têm, igualmente, acesso à Internet com restrições impostas pela Política de Cibersegurança da empresa.

2.2.2. Análise de plataformas tecnológicas internas de segurança

No momento inicial da investigação analisou-se um conjunto de comportamentos e ações, na população-alvo. Constatou-se que alguns dos Colaboradores utilizaram indevidamente o *e-mail* institucional para fins pessoais, nomeadamente, para registo em sites e plataformas externas.

Esta utilização indevida gera um risco acrescido de ataques de *phishing*. Pela análise das plataformas tecnológicas de segurança internas, constatou-se a efetiva receção de *e-mails* de *spam*

com conteúdo potencialmente malicioso, de carácter pessoal, enviados para as caixas de correio profissional dos utilizadores.

A análise do servidor de *E-mail Security Service* da Anubis e do serviço *Exchange Online Protection* (EOP) da *Microsoft*, permitiu identificar *e-mails* comprometidos, ao nível de *malware*, tentativas de *phishing* e de *spam*.

No Anexo I estão representados os dados analisados nas plataformas tecnológicas, extraídos no momento anterior à realização do primeiro ataque simulado aos utilizadores.

2.2.3. Realização do primeiro ataque simulado

Após a identificação dos riscos, e durante o período da investigação, a empresa contratou um serviço de auditoria externa para realização de ataques simulados de *phishing*, de onde se apuraram resultados relevantes no âmbito da dissertação.

O primeiro ataque simulado ocorreu logo após a identificação da problemática. O teste de *phishing* incluiu a escolha de um template de *email*, a compra do domínio de *phishing*, a configuração e criação da *landing page* e o envio de *emails* de *phishing* (Anexo II).

Foi realizada uma campanha de *phishing* para 300 *e-mails*/colaboradores. Os *e-mails* foram personalizados para cada um dos 300 colaboradores, com nome, apelido, e respetivos *links* únicos para a *landing page*. Foi escolhido um domínio o mais semelhante possível ao original.

A campanha permitiu identificar a falta de informação por parte dos colaboradores, quanto ao risco de ataques de *phishing*, uma vez que mais de metade dos colaboradores abriram o *e-mail* e acederam à respetiva *landing page*.

Embora a *landing page* não apresentasse formulário de *login*, para aferir quantos destes colaboradores colocariam as suas credenciais, a simples visita à *landing page* de um possível atacante poderia levar a que os *browsers* e respetivos sistemas fossem comprometidos, o que poderia colocar em causa a confidencialidade, integridade e a disponibilidade da informação.

Dos 300 *e-mails* enviados, 176 foram abertos e 153 colaboradores abriram o *link* para a *landing page* (Anexo III).

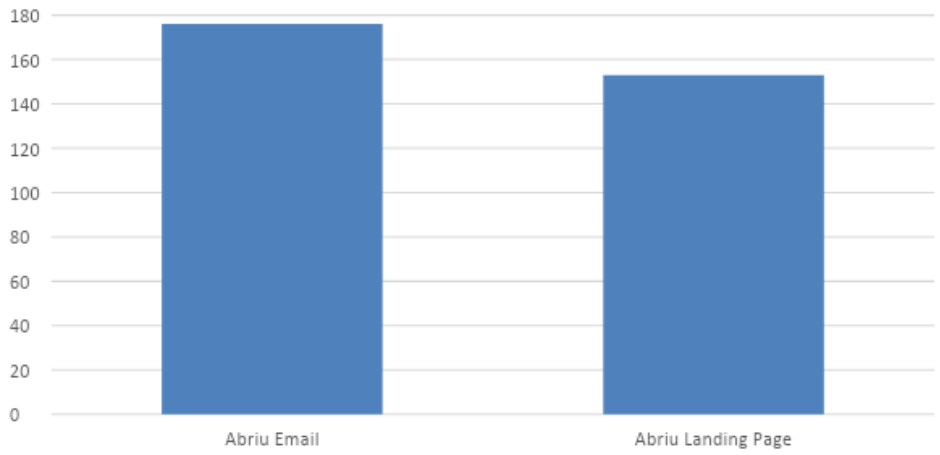


Gráfico 1 - Número de utilizadores que abriram o *e-mail* e a *landing page* durante o primeiro ataque simulado.

2.2.4. Aplicação do inquérito

Na sequência do primeiro ataque de *phishing* foi aplicado um inquérito à população-alvo (Anexo IV), de tipologia descritiva e explicativa.

O inquérito foi construído na ferramenta *Microsoft Forms*, utilizada pela empresa para realização de questionários internos.

A população-alvo, no total de 300 utilizadores, representa 11,6% do efetivo global da empresa. Os utilizadores selecionados correspondem aos Colaboradores a quem foi dirigido o ataque simulado de *phishing*.

Para efeitos de validação da amostra, foi determinado um grau de confiança de 95% e margem de erro de 10%, representando um total de 73 respostas[10]. Foram inquiridos 300 utilizadores e obtidas 87 respostas ao questionário (Anexo V).

[10] Calculador do tamanho da amostra utilizado: https://pt.surveymonkey.com/mp/sample-size-calculator/

Caracterização dos respondentes

No que se refere à caracterização dos respondentes, apuraram-se os seguintes dados:

a) Sexo

A proporção de respondentes do sexo feminino e masculino foi equilibrada.

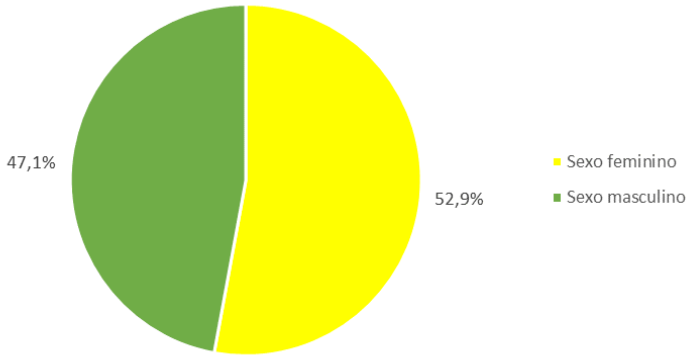


Gráfico 2 - Caracterização dos respondentes por sexo.

b) Idade

93,1% dos respondentes situou-se entre os 31 e os 60 anos, distribuídos de forma homogénea. Nas idades limite "30 ou menos" e "61 ou mais" a percentagem foi residual.

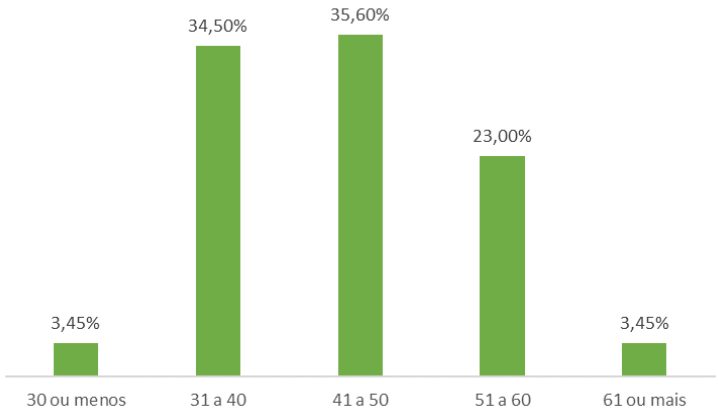


Gráfico 3 - Caracterização dos respondentes por idade.

c) Função desempenhada

39,1% dos respondentes indicaram desempenhar funções administrativas, 31% de Quadro superior sem função de Chefia, 25,3% de Quadro superior com função de Chefia e 4,6% indicaram estar afetos a funções Operacionais ou de Manutenção.

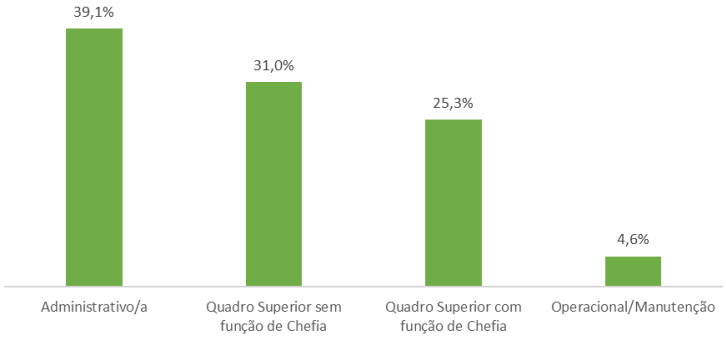


Gráfico 4 - Caracterização dos respondentes por função.

d) Nível de interação com os Sistemas de Informação da empresa

77% dos respondentes indicaram utilizar com muita frequência, 21,8% com frequência e apenas 1,2% indicaram ter uma interação pouco frequente.

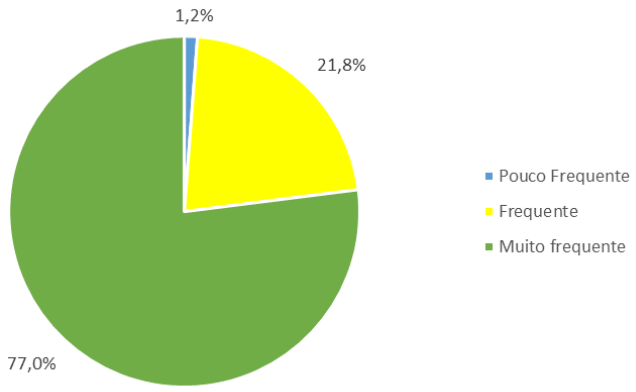


Gráfico 5 - Nível de interação dos respondentes com os Sistemas de Informação da Empresa.

À exceção da caracterização do sexo dos respondentes, todos os dados recolhidos apresentam valores categóricos. Os dados categóricos permitiram validar a amostra selecionada como população-alvo. 100% dos respondentes indicaram desempenhar funções pertencentes às áreas corporativas da empresa. 99% dos respondentes indicaram utilizar com "Muita frequência" ou com "Frequência" os Sistemas de Informação da empresa, evidenciando o acesso a um computador, a um *e-mail* institucional, como ferramenta de trabalho, e a um conjunto de sistemas, plataformas e aplicativos adequados às particularidades das funções que desempenham.

Análise das perguntas relacionadas com as variáveis da problemática

No que diz respeito à tipologia explicativa, as perguntas selecionadas tiveram como objetivo estabelecer relações com as variáveis identificadas na problemática.

a) Perceção dos indivíduos relativamente à Política e Cultura de Cibersegurança da empresa

A maioria dos respondentes (46%) considerou que a empresa não divulga a sua Política de Cibersegurança. No entanto, também a maioria (66%) considerou que a empresa promove a Cultura de Cibersegurança e 74,7% indicou saber qual a área/pessoa responsável pela Segurança Informática da empresa.

Foi possível inferir que, apesar de não conhecerem a Política de Cibersegurança, os utilizadores percecionam a existência de sistemas e tecnologias de segurança e sabem quem é o responsável pelos mesmos. Correlacionando esta perceção com a dos influenciadores da Cultura de Cibersegurança, a maioria dos respondentes atribui uma maior responsabilidade à Equipa de Tecnologias de Informação, seguida dos Decisores, da área de Formação e, por último, aos próprios utilizadores.

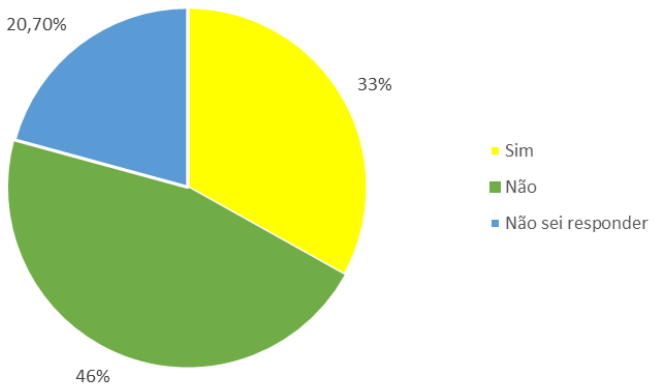


Gráfico 6 - Opinião sobre a divulgação das Políticas de Cibersegurança pela Empresa.

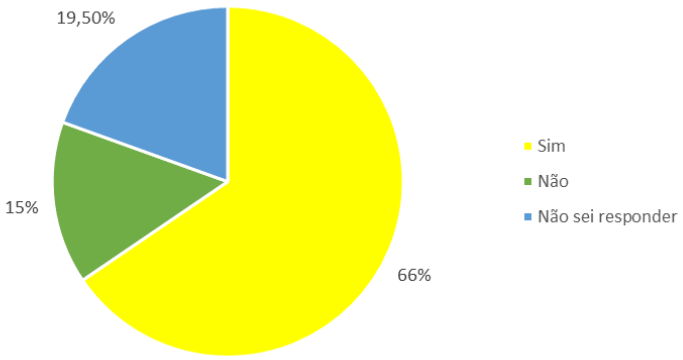


Gráfico 7 - Opinião sobre a promoção de uma Cultura de Cibersegurança pela Empresa.

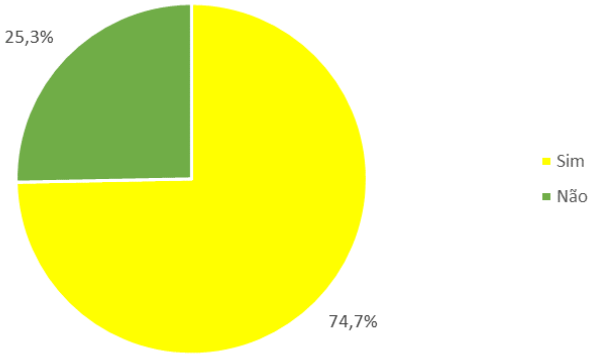
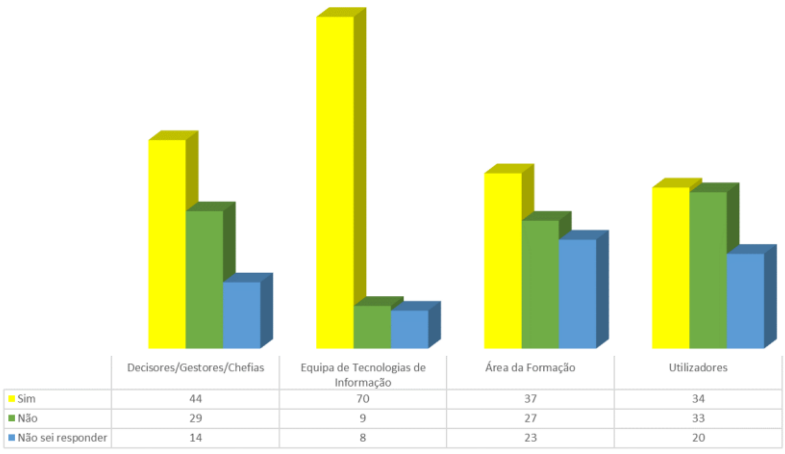


Gráfico 8 - Percentagem de respondentes que reconhecem a área/pessoa responsável pela Segurança Informática na Empresa.

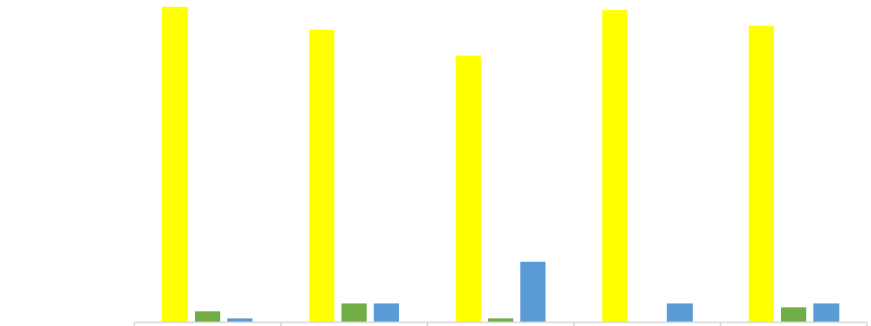


	Decisores/Gestores/Chefias	Equipa de Tecnologias de Informação	Área da Formação	Utilizadores
Sim	44	70	37	34
Não	29	9	27	33
Não sei responder	14	8	23	20

Gráfico 9 - Perceção dos respondentes sobre os influenciadores da Cultura de Cibersegurança.

b) Conhecimento geral sobre boas práticas no âmbito da prevenção de ciberataques

Da análise das respostas, constatou-se que a maioria dos respondentes consegue identificar as boas práticas que promovem a prevenção de ciberataques, incluindo a utilização de palavras-chave seguras e o desenvolvimento de ações de sensibilização.



	Utilizar palavras-chave seguras	Definir níveis de acesso diferentes para vários tipos de utilizadores	Utilizar uma firewall	Implementar software de antivírus, anti-spam e anti-phishing	Realizar ações de sensibilização sobre cibersegurança
Sim	83	77	70	82	78
Não	3	5	1	0	4
Não sei responder	1	5	16	5	5

Gráfico 10 - Perceção sobre os comportamentos que contribuem para prevenir um Ciberataque.

c) Perceção sobre o papel do utilizador enquanto fator preventivo de potenciais ataques de *phishing*:

Embora a análise das plataformas tecnológicas internas de Segurança da empresa tenha evidenciado a utilização do *e-mail* profissional para fins pessoais, a maioria dos respondentes (92%) afirmou não o fazer. Acresce que a maioria (76%) também identificou esta prática como um risco para a Segurança da Informação e dos Sistemas da Empresa. Constatou-se que os utilizadores estão conscientes do seu papel enquanto fator de prevenção.

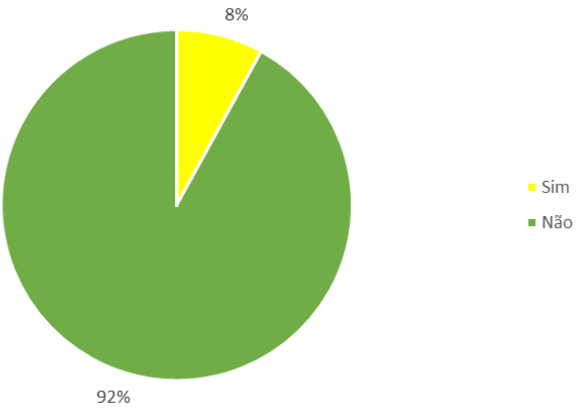


Gráfico 11 - Respondentes que utilizam o e-mail profissional para fins pessoais.

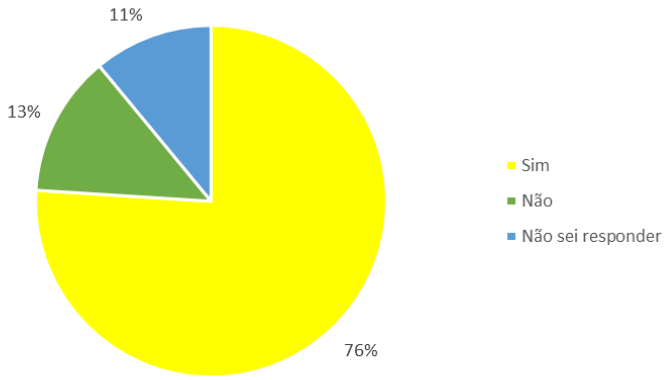


Gráfico 12 - Opinião sobre o risco de utilização do e-mail profissional para fins pessoais.

d) Opinião sobre a formação ministrada no âmbito da cibersegurança

A maioria dos respondentes (93,1%) respondeu nunca ter realizado formação, em Cibersegurança, promovida pela empresa. A falta de investimento nesta área foi corroborada pelos respondentes, sendo que 56,3% afirmou que a empresa não investe na formação em Cibersegurança.

No campo de resposta, aberto, sobre a formação realizada incluiu-se uma pergunta específica e outra de aferição de factos. A pergunta de aferição de factos permitiu uma análise mais detalhada sobre os 5,7% de respondentes que afirmaram ter tido formação. Destes, apenas três (3) pessoas realizaram formação ministrada pela empresa, no âmbito do Regulamento Geral de Proteção de Dados (RGPD), e uma (1) pessoa realizou formação em Cibersegurança a título particular.

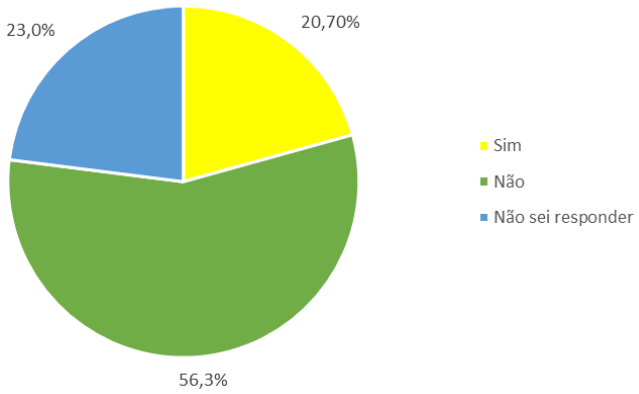


Gráfico 13 - Percentagem de respondentes que considerou que a empresa investe na formação em Cibersegurança.

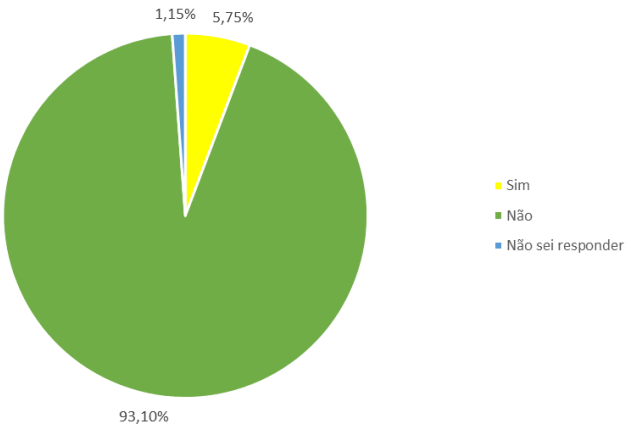


Gráfico 14 - Percentagem de respondentes que realizou ações de formação em Cibersegurança promovidas pela Empresa.

Este grupo de perguntas foi organizado por secções referentes aos temas: Cultura e Cibersegurança na Empresa; Comportamentos preventivos; e Formação em Cibersegurança; permitindo inferir opiniões e perceções sobre os temas representados.

Na aplicação do questionário, foi utilizado um formato transversal, considerando que os dados foram recolhidos num único momento a uma amostra representativa da população global da empresa. As perguntas foram redigidas com o pressuposto de serem curtas e claras, permitindo abranger todo o universo de respondentes independentemente do seu grau de literacia.

2.2.5. Realização de ação de sensibilização

Em articulação com a Direção de Tecnologias de Informação e com a área de Formação da empresa, foi divulgada uma ação de sensibilização, dirigida aos Colaboradores da empresa, sobre o tema da Cibersegurança. A divulgação ocorreu após a aplicação do inquérito de auscultação.

A ação de sensibilização foi de participação voluntária e inscrição gratuita e pretendeu sensibilizar todos os Colaboradores para a utilização segura e informada das Tecnologias de Informação e de Comunicação (TIC), reduzindo a sua exposição aos riscos do ciberespaço.

O curso, promovido pela entidade NAU[11], visou garantir um conjunto de competências que permitissem que qualquer cidadão, enquanto utilizador do ciberespaço, se sentisse apto a navegar na Internet, de forma segura. Teve uma carga total de 3 horas, dividida em três módulos: Casa,

11 NAU – Ensino e Formação Online para Grandes Audiências – plataforma de suporte ao ensino e formação, dirigido a grandes audiências. Fonte: https://www.nau.edu.pt/pt/sobre/

Trabalho e Exterior. Cada módulo incluiu quatro tópicos: Identidade; Redes e Navegação; Comportamento Social; e Posto de Trabalho/Posto Doméstico/Passaporte (Anexo VII).

Da população-alvo da presente dissertação, um total de 30 utilizadores frequentaram a ação de sensibilização.

2.2.6. Realização do segundo ataque simulado

Após disseminação da ação de sensibilização, foi realizado um novo ataque simulado.

O objetivo foi comparar a eficácia da ação de sensibilização na alteração dos comportamentos e consciência dos utilizadores sobre os potenciais riscos associados a um ataque de *phishing*.

Na última fase de investigação, foi realizado um segundo ataque simulado, utilizando *templates* de *email* e de *landing page* diferenciados do primeiro ataque (Anexo IX).

Foi realizada uma campanha de *phishing* para 296 *e-mails*/colaboradores. Os *e-mails* foram personalizados para cada um dos colaboradores, e criados *links* únicos para a *landing page*. Foi escolhido um domínio o mais semelhante possível ao original.

Dos 296 *e-mails* enviados, 84 foram abertos e 45 colaboradores abriram o *link* para a *landing page*. Foi possível concluir que, após a ação de sensibilização, o número de Colaboradores que incorreu numa falha de segurança foi significativamente menor.

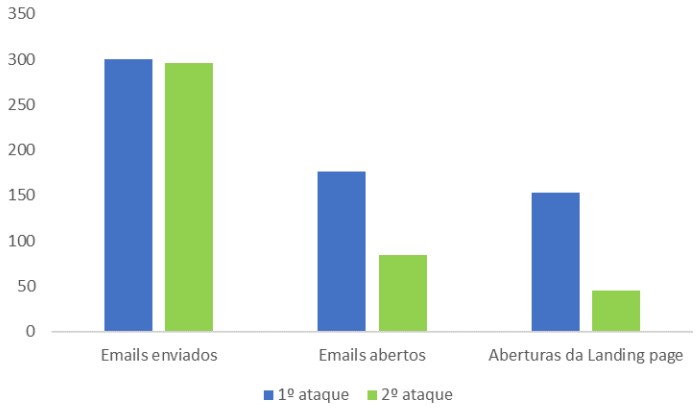


Gráfico 15 - Dados comparativos dos dois ataques simulados

Conclusão

De acordo com a visão sociotecnológica dos Sistemas de Informação, os recursos humanos são um fator de extrema importância para a Cibersegurança de uma organização. Igual importância tem a formação e consequente desenvolvimento de competências dos utilizadores (Gouveia & Ranito, 2004). É relevante recordar que uma grande percentagem das falhas de segurança é da responsabilidade dos utilizadores. Alguns são acontecimentos intencionais, outros derivados da falta de conhecimento e/ou de competências (Hardcastle, 2008). Correlacionando estes dois fatores – formação e influência dos utilizadores – e analisando os resultados obtidos no questionário, concluiu-se que a maioria dos inquiridos não se reconhece como um fator influenciador da Cultura de Cibersegurança, atribuíndo maior responsabilidade à Equipa de Tecnologias de Informação. Por outro lado, 56,3% considera que a empresa não investe na formação em cibersegurança. Esta correlação evidenciou a pertinência de se delinear um plano de formação que promova a tomada de consciência dos utilizadores sobre o seu papel na redução dos riscos de um ciberataque.

Ainda do ponto de vista sociotecnológico, os utilizadores têm a responsabilidade de avaliar a qualidade e fidedignidade dos recursos (Gouveia & Ranito, 2004), no entanto, durante a investigação empírica, constatou-se que os Colaboradores não manifestaram esta competência. Quando confrontados com um primeiro ataque simulado de *phishing,* dos 300 *e-mails* enviados, 176 foram abertos e 153 colaboradores abriram efetivamente o *link* para a *landing page* maliciosa. Estes resultados evidenciaram a abertura de links de *e-mails* de *spam,* e o acesso a *websites* de fontes não fidedignas, como os principais incidentes com origem no fator humano (Gonçalves & Nunes, 2019). Ou seja, mais de metade dos utilizadores incorreram numa falha de segurança, não avaliaram os riscos nem conseguiram identificar a fonte não fidedigna do ataque.

Segundo Pais *et al* (2020), para além do desconhecimento ou falta de competências dos utilizadores, este tipo de ataques acontece também devido ao desconhecimento das Políticas de Segurança implementadas. Quando inquiridos sobre este tema, 46% dos respondentes não consideraram que a empresa divulga as suas Políticas de Cibersegurança, acrescendo 20,7% que não souberam responder evidenciando igual desconhecimento. Este foi um dos pontos para o qual se pretendeu sensibilizar com o módulo formativo, desenvolvido nesta dissertação, o facto de um plano de formação e de comunicação eficazes, sobre o tema da Cibersegurança, influenciar o comportamento dos utilizadores, minimizando os riscos de ciberataques, em particular os ataques de Engenharia Social, de que é exemplo o *phishing*.

De acordo com a ENISA (2018), uma Cultura de Cibersegurança, bem sucedida, influencia a forma de pensar de todos os indivíduos, promovendo resiliência contra ciberataques,

em particular os que derivam da Engenharia Social. Analisando os resultados do questionário, 66% dos respondentes consideraram que a empresa promove uma Cultura de Cibersegurança. No entanto, quando inquiridos sobre a influência de cada grupo funcional no desenvolvimento desta Cultura, a maioria das respostas incidiu sobre a Equipa de Tecnologias de Informação, seguida dos Decisores, da área da formação e, por último, dos próprios utilizadores o que evidenciou que estes não estão devidamente envolvidos no desenvolvimento da Cultura de Cibersegurança.

Inferiu-se que a perceção sobre a promoção da Cultura de Cibersegurança pode estar associada às medidas de segurança implementadas, de forma automática e de atualização periódica, tendo em conta que a maioria dos respondentes reconheceu, nas suas respostas, que a utilização de palavras-chave, a definição de níveis de acesso diferenciados para diferentes tipos de utilizadores, a existência de uma *firewall*, e a utilização de *software* de anti-virus, anti-*spam* e anti-*phishing* são comportamentos preventivos. Ou seja, foi possível identificar que as Políticas de Cibersegurança Tecnológicas, embora não sendo divulgadas pela Empresa, são percecionadas pelos utilizadores como existentes e relevantes.

Sendo a Formação em Cibersegurança um tema crucial para o desenvolvimento de uma Cultura de Cibersegurança (AP2SI, 2015, p. 7), evidenciou-se, mais uma vez, a relevância da implementação de um módulo formativo neste âmbito. O resultado do segundo ataque de *phishing* simulado, após realização da ação de sensibilização sobre Cibergurança, evidenciou a importância da formação, considerando-se a redução visível do número de utilizadores que incorreu numa falha de segurança e a capacitação para identificação de um ataque malicioso.

Considerando que o plano de formação deve integrar vários momentos, podendo estes ser concebidos com base em necessidades específicas (Wout, 2019), o módulo de formação proposto, na presente dissertação, focou-se no tema do *phishing*, cujos potenciais riscos foram evidenciados ao longo da investigação empírica.

Como ações de melhoria, sugere-se: divulgação eficaz e sistemática das Políticas de Cibersegurança internas, reforçando as boas práticas que são da responsabilidade individual dos utilizadores; implementação de um sistema de alerta, do tipo *pop-up*, que sensibilize, de forma periódica e frequente, os utilizadores para os riscos de Cibersegurança; aplicação de um módulo formativo que sensibilize para o conceito de Cultura de Cibersegurança, esclareça o conceito de *phishing* e sensibilize os Colaboradores para o seu papel no desenvolvimento da Cultura de Cibersegurança interna e na prevenção de um ataque de *phishing* (Anexo VIII).

Referências

Al-Mamary, H., Shamsuddin, A., & Aziati, N. (2014). The role of different types of information systems in business organizations : A review. *International Journal of Research (IJR), 1*(7), pp. 1279 - 1286. Obtido de https://www.researchgate.net/publication/264556488_The_Role_of_Different_Types_of_Information_Systems_In_Business_Organizations_A_Review

Associação Portuguesa para a Promoção da Segurança da Informação. (2015). *Inquérito aberto à segurança da informação nas instituições em Portugal: Sumário*. Obtido de https://ap2si.files.wordpress.com/2016/04/sumc3a1rio-primeiro-inquc3a9rito-aberto-c3a0-seguranc3a7a-da-informac3a7c3a3o-nas-instituic3a7c3b5es-em-portugal.pdf

Awais, M., Irfan, M., Bilal, M., & Samin, T. (2012). Helpful business value of advance bal information system. *International Journal of Computer Science Issues (IJCSI), 9*(2), pp. 415-422. Obtido de https://www.researchgate.net/publication/321192951_Helpful_Business_Value_of_Advance_Bal_Information_System

Barros, G. (28 de agosto de 2018). *TE56 - A cibersegurança em Portugal*. Obtido de Gabinete de Estratégia e Estudos: https://www.gee.gov.pt/pt/estudos-e-seminarios/estudos-de-temas-economicos-category/34-temas-economicos/17741-a-ciberseguranca-em-portugal

Bowen, B., Devarajan, R., & Stolfo, S. (novembro de 2011). Measuring the human factor of cyber security. *IEEE Homeland Security Technology Conference.* Columbia. doi:10.1109/THS.2011.6107876

Centro Nacional de Cibersegurança Portugal. (s.d.). *Engenharia social*. Obtido de https://www.cncs.gov.pt/engenharia-social/

Dezdar, S., & Sulaiman, A. (2009). Successful enterprise resource planning implementation: Taxonomy of critical factors. *Industrial Management & Data Systems, 109*(8), pp. 1037-1052. doi:10.1108/02635570910991283

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, pp. 1-11. doi:10.1080/08874417.2020.1845583

Gonçalves, R., & Nunes, S. (dezembro de 2019). O fator humano da cibersegurança nas organizações. *Atas da conferência Ibero-Americana WWW/Internet 2019.* Lisboa. doi:10.33965/ciawi2019_201914L007

Gouveia, L., & Ranito, J. (2004). *Sistemas de informação de apoio à gestão.* SPI – Sociedade Portuguesa de Inovação. Obtido de https://bdigital.ufp.pt/bitstream/10284/264/1/Manual_VII.pdf

Hardcastle, E. (2008). *Business information systems.* Elizabeth Hardcastle & Ventus Publishing ApS. Obtido de https://paginas.fe.up.pt/~apm/ESIN/docs/bis.pdf

Huang, K., & Pearlson, K. (janeiro de 2019). For what technology can't fix: Building a model of organizational cybersecurity culture. *52nd Hawaii International Conference on System Sciences.* Cambridge. Obtido de http://web.mit.edu/smadnick/www/wp/2019-02.pdf

International Telecommunication Union. (julho de 2017). *Global Cybersecurity Index*. Obtido de ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Lipaj, D., & Davidavičienė, V. (2013). Influence of information systems on business performance. *Mokslas - Lietuvos Ateitis, 5*(1), pp. 38-45. doi:10.3846/mla.2013.06

Pais, R., Moreira, F., & Varajão, J. (2020). Engenharia social (ou o carneiro que afinal era um lobo). *144 LivroEGP - Engenharia Social*. Obtido de http://repositorio.uportu.pt/jspui/bitstream/11328/1347/1/144%20LivroEGP%20-%20EngenhariaSocial.pdf

Resolução do Conselho de Ministros n.º 36/2015. (2015). *N.º 13, Série I*. Diário da República. Obtido de https://data.dre.pt/eli/resolconsmin/36/2015/06/12/p/dre/pt/html

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(89), pp. 1-17. doi:10.3390/fi11040089

Stair, R., & Reynolds, G. (2015). *Princípios de sistemas de informação* (11ª ed.). Cengage Learning. Obtido de https://fdocumentos.com/document/principios-de-sistemas-de-informacao-traducao-da-11a-edicao-norte-americana.html

Thapar, A. (2007). *Whitepaper on social engineering - An attack vector most intricate to tackle!* University of Toronto. Course Hero. Obtido de https://www.coursehero.com/file/27129635/Social-Engineering-AThaparpdf/

The European Union Agency for Cybersecurity. (6 de fevereiro de 2018). *Cyber security culture in organisations*. Obtido de Enisa: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Trim, P., Lee, Y.-I., Ko, E., & Kim, K. (março de 2014). Cyber security culture and ways to improve security management. Em P., E., K., Trim, & Youm (Edits.), *Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership* (pp. 21-26). Republic of Korea. Obtido de http://www.iaac.org.uk/media/1067/reporttrimyoumcybersecuritymarch14.pdf

Wout, M. (28 de fevereiro de 2019). Develop and maintain a cybersecurity organisational culture. *ICCWS 2019 14th International Conference on Cyber Warfare and Security*. South Africa. Obtido de https://www.researchgate.net/publication/334052953_Develop_and_Maintain_a_Cybersecurity_Organisational_Culture

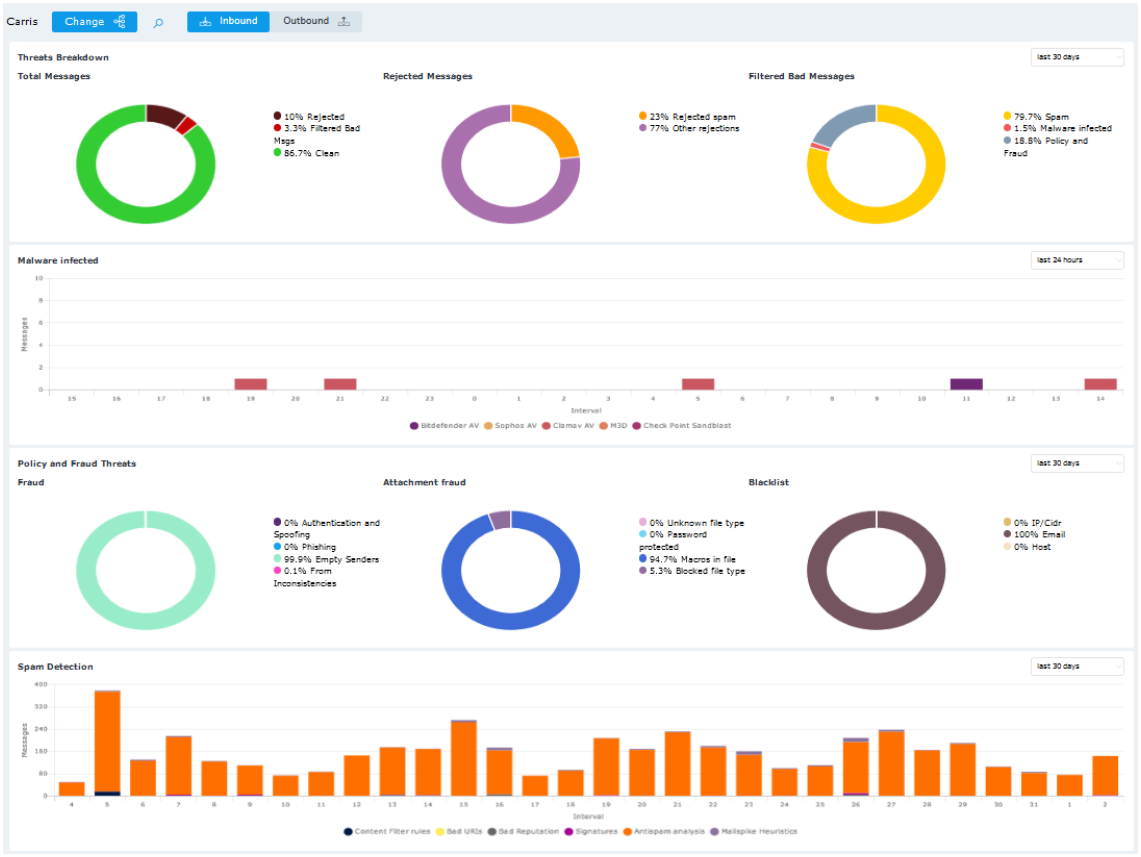
ANEXOS

ANEXO I - Analisa das plataformas de segurança internas

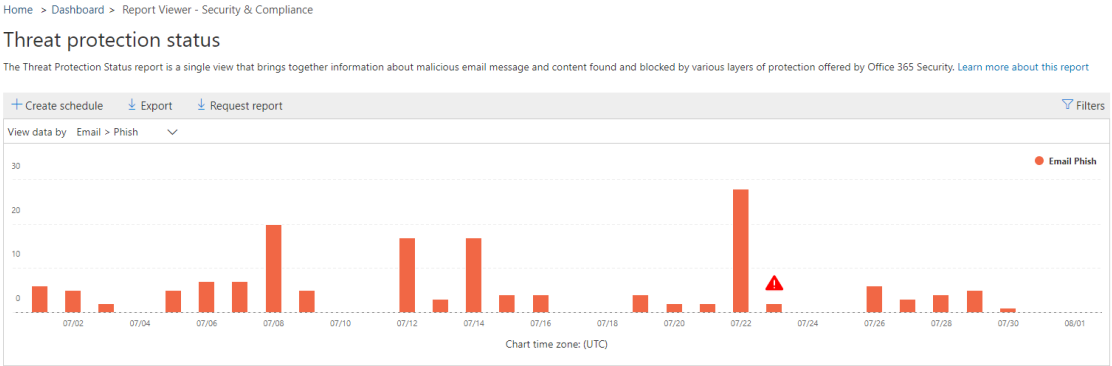
Exemplo de *e-mails* rejeitados pelo *Smart Host Anubis Network.*

SENDER	TO	CLIENT IP	REJECTION CAUSE
shimizu@miya-s.com	[redacted]	61.126.38.32	Message was milter rejected.
sent@npsa.co.za		41.193.6.206	Message was milter rejected.
geral@materialdeprotecao.pt		51.178.153.245	Message was milter rejected.
geral@materialdeprotecao.pt		51.38.210.178	Message was milter rejected.
pcnws@standingtrees.info		146.59.11.166	Message was milter rejected.
pcnws@standingtrees.info		146.59.11.166	Message was milter rejected.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
facturacao.electronica@galp.com		40.107.7.112	Recipient address rejected: Access denied.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
flaggingup@flaggingup.info		135.125.132.182	Recipient address rejected: Access denied.
vominhlam1512@gmail.com		209.85.167.193	Message was milter rejected.
no_reply@winaico.com		103.151.122.244	RBL blocking rule.
bounce-mc.us17_89482513.519057...		198.2.183.215	Message was milter rejected.
info@nnpcgroup.com.ng		184.188.201.186	RBL blocking rule.
linhhaianh@gmail.com		209.85.128.68	Message was milter rejected.
geral@materialdeprotecao.pt		178.33.9.160	Message was milter rejected.
tmbpc@smoothchange.info		135.125.132.233	Recipient address rejected: Access denied.
iiwegon@honicel.com		112.17.118.54	RBL blocking rule.
zohra.kourgli@ediel.net		41.111.144.182	Recipient address rejected: Access denied.
a.gerard@workinasia.net		210.245.112.17	Sender address rejected: Domain not found.
a.gerard@workinasia.net		210.245.112.17	Sender address rejected: Domain not found.
bounce-mc.us12_50115165.358828...		205.201.128.81	Message was milter rejected.
		52.100.20.244	Recipient address rejected: Access denied.

Exemplo de *dashboard* com *e-mails* comprometidos (*malware*, *phishing* e *spam*) extraído do *E-mail Security Service* da Anubis, antes da realização do primeiro ataque simulado.

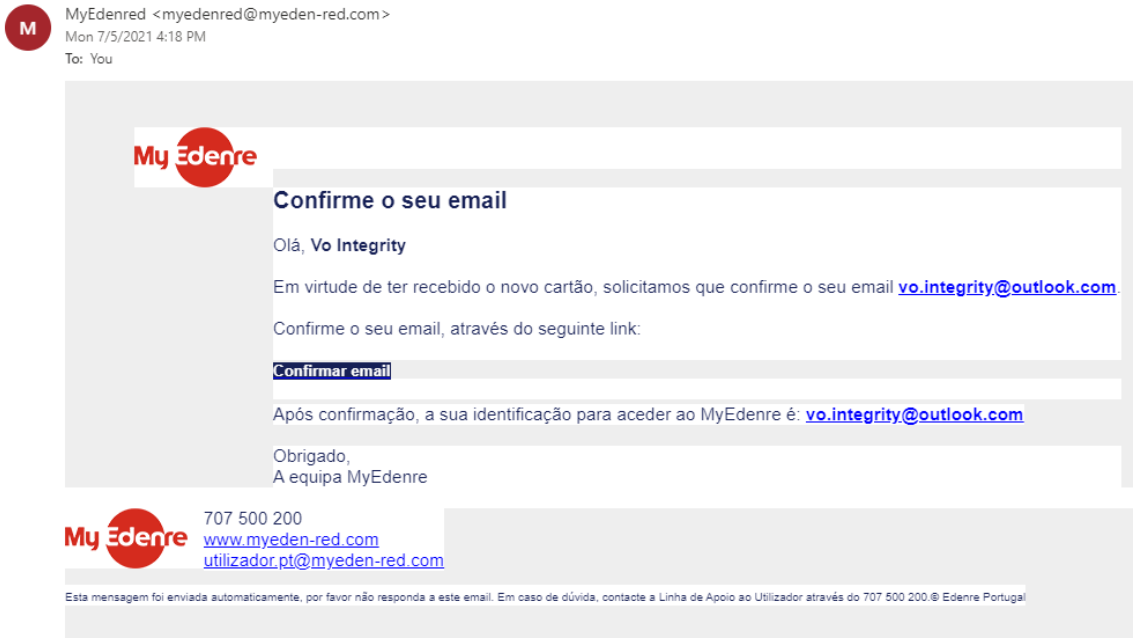


Excerto do *dashboard* extraído do *Exchange Online Protection* (EOP) da *Microsoft*, com *report* de *e-mails* de *phishing* detetados.

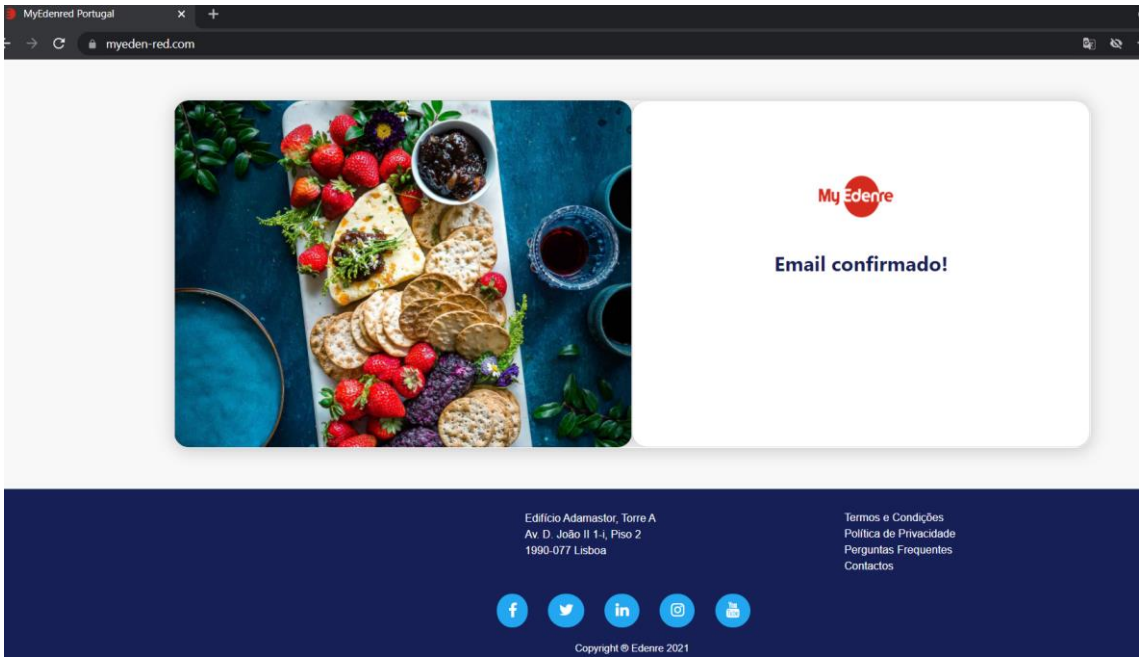


ANEXO II - *Templates* utilizados no primeiro ataque simulado

Template de *e-mail* enviado no primeiro ataque simulado



Template da *Landing Page* enviada no primeiro ataque simulado



ANEXO III – Tabela detalhada de resultados do primeiro ataque simulado

Email	Abriu Email	Abriu Landing Page
001_user@ xxxx.pt	Não	Não
002_user@ xxxx.pt	Não	Não
003_user@ xxxx.pt	Sim	Sim
004_user@ xxxx.pt	Sim	Sim
005_user@ xxxx.pt	Sim	Sim
006_user@ xxxx.pt	Sim	Sim
007_user@ xxxx.pt	Sim	Sim
008_user@ xxxx.pt	Sim	Sim
009_user@ xxxx.pt	Sim	Sim
010_user@ xxxx.pt	Sim	Sim
011_user@ xxxx.pt	Sim	Sim
012_user@ xxxx.pt	Não	Não
013_user@ xxxx.pt	Sim	Sim
014_user@ xxxx.pt	Sim	Sim
015_user@ xxxx.pt	Sim	Sim
016_user@ xxxx.pt	Sim	Sim
017_user@ xxxx.pt	Sim	Sim
018_user@ xxxx.pt	Sim	Sim
019_user@ xxxx.pt	Sim	Sim
020_user@ xxxx.pt	Sim	Sim
021_user@ xxxx.pt	Sim	Sim
022_user@ xxxx.pt	Não	Não
023_user@ xxxx.pt	Não	Não
024_user@ xxxx.pt	Não	Não
025_user@ xxxx.pt	Sim	Sim
026_user@ xxxx.pt	Sim	Sim
027_user@ xxxx.pt	Sim	Não
028_user@ xxxx.pt	Sim	Sim
029_user@ xxxx.pt	Não	Não
030_user@ xxxx.pt	Sim	Sim
031_user@ xxxx.pt	Não	Não
032_user@ xxxx.pt	Não	Não
033_user@ xxxx.pt	Sim	Sim
034_user@ xxxx.pt	Sim	Sim
035_user@ xxxx.pt	Sim	Não
036_user@ xxxx.pt	Sim	Sim
037_user@ xxxx.pt	Não	Não
038_user@ xxxx.pt	Sim	Sim
039_user@ xxxx.pt	Não	Não
040_user@ xxxx.pt	Não	Não
041_user@ xxxx.pt	Não	Não
042_user@ xxxx.pt	Sim	Sim

043_user@ xxxx.pt	Sim	Sim
044_user@ xxxx.pt	Sim	Sim
045_user@ xxxx.pt	Não	Não
046_user@ xxxx.pt	Não	Não
047_user@ xxxx.pt	Sim	Sim
048_user@ xxxx.pt	Não	Não
049_user@ xxxx.pt	Não	Não
050_user@ xxxx.pt	Sim	Sim
051_user@ xxxx.pt	Não	Não
052_user@ xxxx.pt	Sim	Sim
053_user@ xxxx.pt	Sim	Sim
054_user@ xxxx.pt	Sim	Não
055_user@ xxxx.pt	Não	Não
056_user@ xxxx.pt	Sim	Sim
057_user@ xxxx.pt	Sim	Sim
058_user@ xxxx.pt	Sim	Sim
059_user@ xxxx.pt	Sim	Sim
060_user@ xxxx.pt	Sim	Sim
061_user@ xxxx.pt	Não	Não
062_user@ xxxx.pt	Não	Não
063_user@ xxxx.pt	Sim	Sim
064_user@ xxxx.pt	Não	Não
065_user@ xxxx.pt	Sim	Não
066_user@ xxxx.pt	Sim	Sim
067_user@ xxxx.pt	Não	Não
068_user@ xxxx.pt	Sim	Sim
069_user@ xxxx.pt	Não	Não
070_user@ xxxx.pt	Sim	Sim
071_user@ xxxx.pt	Não	Não
072_user@ xxxx.pt	Não	Não
073_user@ xxxx.pt	Sim	Sim
074_user@ xxxx.pt	Sim	Sim
075_user@ xxxx.pt	Sim	Sim
076_user@ xxxx.pt	Não	Não
077_user@ xxxx.pt	Sim	Sim
078_user@ xxxx.pt	Sim	Sim
079_user@ xxxx.pt	Não	Não
080_user@ xxxx.pt	Não	Não
081_user@ xxxx.pt	Não	Não
082_user@ xxxx.pt	Sim	Sim
083_user@ xxxx.pt	Sim	Sim
084_user@ xxxx.pt	Não	Não
085_user@ xxxx.pt	Não	Não
086_user@ xxxx.pt	Não	Não
087_user@ xxxx.pt	Sim	Sim
088_user@ xxxx.pt	Sim	Não

089_user@ xxxx.pt	Sim	Sim
090_user@ xxxx.pt	Sim	Sim
091_user@ xxxx.pt	Sim	Sim
092_user@ xxxx.pt	Sim	Sim
093_user@ xxxx.pt	Sim	Sim
094_user@ xxxx.pt	Não	Não
095_user@ xxxx.pt	Sim	Sim
096_user@ xxxx.pt	SIm	Sim
097_user@ xxxx.pt	Sim	Sim
098_user@ xxxx.pt	Sim	Sim
099_user@ xxxx.pt	Sim	Não
100_user@ xxxx.pt	Não	Não
101_user@ xxxx.pt	Sim	Sim
102_user@ xxxx.pt	Sim	Sim
103_user@ xxxx.pt	Sim	Sim
104_user@ xxxx.pt	Sim	Sim
105_user@ xxxx.pt	Não	Não
106_user@ xxxx.pt	Não	Não
107_user@ xxxx.pt	Sim	Sim
108_user@ xxxx.pt	Sim	Não
109_user@ xxxx.pt	Sim	Sim
110_user@ xxxx.pt	Sim	Sim
111_user@ xxxx.pt	Não	Não
112_user@ xxxx.pt	Não	Não
113_user@ xxxx.pt	Sim	Sim
114_user@ xxxx.pt	Sim	Sim
115_user@ xxxx.pt	Sim	Sim
116_user@ xxxx.pt	Sim	Sim
117_user@ xxxx.pt	Não	Não
118_user@ xxxx.pt	Não	Não
119_user@ xxxx.pt	Sim	Não
120_user@ xxxx.pt	Não	Não
121_user@ xxxx.pt	Sim	Sim
122_user@ xxxx.pt	Não	Não
123_user@ xxxx.pt	Não	Não
124_user@ xxxx.pt	Sim	Sim
125_user@ xxxx.pt	Sim	Não
126_user@ xxxx.pt	Sim	Não
127_user@ xxxx.pt	Sim	Sim
128_user@ xxxx.pt	Sim	Sim
129_user@ xxxx.pt	Não	Não
130_user@ xxxx.pt	Não	Não
131_user@ xxxx.pt	Sim	Sim
132_user@ xxxx.pt	Sim	Sim
133_user@ xxxx.pt	Sim	Não
134_user@ xxxx.pt	Sim	Sim

135_user@ xxxx.pt	Não	Não
136_user@ xxxx.pt	Sim	Sim
137_user@ xxxx.pt	Sim	Não
138_user@ xxxx.pt	Não	Não
139_user@ xxxx.pt	Sim	Sim
140_user@ xxxx.pt	Não	Não
141_user@ xxxx.pt	Não	Não
142_user@ xxxx.pt	Sim	Sim
143_user@ xxxx.pt	Sim	Sim
144_user@ xxxx.pt	Sim	Sim
145_user@ xxxx.pt	Sim	Sim
146_user@ xxxx.pt	Não	Não
147_user@ xxxx.pt	Não	Não
148_user@ xxxx.pt	Sim	Não
149_user@ xxxx.pt	Não	Não
150_user@ xxxx.pt	Não	Não
151_user@ xxxx.pt	Não	Não
152_user@ xxxx.pt	Não	Não
153_user@ xxxx.pt	Não	Não
154_user@ xxxx.pt	Não	Não
155_user@ xxxx.pt	Não	Não
156_user@ xxxx.pt	Não	Não
157_user@ xxxx.pt	Não	Não
158_user@ xxxx.pt	Não	Não
159_user@ xxxx.pt	Não	Não
160_user@ xxxx.pt	Não	Não
161_user@ xxxx.pt	Sim	Não
162_user@ xxxx.pt	Sim	Sim
163_user@ xxxx.pt	Sim	Sim
164_user@ xxxx.pt	Sim	Sim
165_user@ xxxx.pt	Sim	Sim
166_user@ xxxx.pt	Não	Não
167_user@ xxxx.pt	Sim	Sim
168_user@ xxxx.pt	Sim	Sim
169_user@ xxxx.pt	Não	Não
170_user@ xxxx.pt	Não	Não
171_user@ xxxx.pt	Sim	Sim
172_user@ xxxx.pt	Sim	Sim
173_user@ xxxx.pt	Sim	Sim
174_user@ xxxx.pt	Sim	Sim
175_user@ xxxx.pt	Sim	Sim
176_user@ xxxx.pt	Não	Não
177_user@ xxxx.pt	Sim	Sim
178_user@ xxxx.pt	Sim	Sim
179_user@ xxxx.pt	Não	Não
180_user@ xxxx.pt	Sim	Sim

181_user@ xxxx.pt	Sim	Não
182_user@ xxxx.pt	Não	Não
183_user@ xxxx.pt	Sim	Sim
184_user@ xxxx.pt	Não	Não
185_user@ xxxx.pt	Sim	Sim
186_user@ xxxx.pt	Não	Não
187_user@ xxxx.pt	Não	Não
188_user@ xxxx.pt	Sim	Não
189_user@ xxxx.pt	Não	Não
190_user@ xxxx.pt	Não	Não
191_user@ xxxx.pt	Sim	Sim
192_user@ xxxx.pt	Sim	Sim
193_user@ xxxx.pt	Sim	Sim
194_user@ xxxx.pt	Sim	Sim
195_user@ xxxx.pt	Sim	Sim
196_user@ xxxx.pt	Não	Não
197_user@ xxxx.pt	Não	Não
198_user@ xxxx.pt	Sim	Sim
199_user@ xxxx.pt	Não	Não
200_user@ xxxx.pt	Não	Não
201_user@ xxxx.pt	Sim	Sim
202_user@ xxxx.pt	Sim	Não
203_user@ xxxx.pt	Sim	Sim
204_user@ xxxx.pt	Sim	Sim
205_user@ xxxx.pt	Sim	Sim
206_user@ xxxx.pt	Não	Não
207_user@ xxxx.pt	Sim	Sim
208_user@ xxxx.pt	Sim	Sim
209_user@ xxxx.pt	Sim	Sim
210_user@ xxxx.pt	Sim	Sim
211_user@ xxxx.pt	Não	Não
212_user@ xxxx.pt	Sim	Sim
213_user@ xxxx.pt	Não	Não
214_user@ xxxx.pt	Sim	Sim
215_user@ xxxx.pt	Não	Não
216_user@ xxxx.pt	Não	Não
217_user@ xxxx.pt	Sim	Sim
218_user@ xxxx.pt	Não	Não
219_user@ xxxx.pt	Não	Não
220_user@ xxxx.pt	Sim	Sim
221_user@ xxxx.pt	Não	Não
222_user@ xxxx.pt	Sim	Sim
223_user@ xxxx.pt	Sim	Sim
224_user@ xxxx.pt	Sim	Sim
225_user@ xxxx.pt	Sim	Não
226_user@ xxxx.pt	Sim	Sim

227_user@ xxxx.pt	Sim	Sim
228_user@ xxxx.pt	Sim	Não
229_user@ xxxx.pt	Sim	Sim
230_user@ xxxx.pt	Não	Não
231_user@ xxxx.pt	Sim	Sim
232_user@ xxxx.pt	Não	Não
233_user@ xxxx.pt	Sim	Sim
234_user@ xxxx.pt	Sim	Sim
235_user@ xxxx.pt	Sim	Não
236_user@ xxxx.pt	Não	Não
237_user@ xxxx.pt	Sim	Sim
238_user@ xxxx.pt	Não	Não
239_user@ xxxx.pt	Não	Não
240_user@ xxxx.pt	Não	Não
241_user@ xxxx.pt	Sim	Sim
242_user@ xxxx.pt	Sim	Não
243_user@ xxxx.pt	Não	Não
244_user@ xxxx.pt	Sim	Não
245_user@ xxxx.pt	Não	Não
246_user@ xxxx.pt	Sim	Sim
247_user@ xxxx.pt	Sim	Sim
248_user@ xxxx.pt	Não	Não
249_user@ xxxx.pt	Não	Não
250_user@ xxxx.pt	Não	Não
251_user@ xxxx.pt	Não	Não
252_user@ xxxx.pt	Sim	Sim
253_user@ xxxx.pt	Sim	Sim
254_user@ xxxx.pt	Não	Não
255_user@ xxxx.pt	Sim	Sim
256_user@ xxxx.pt	Sim	Sim
257_user@ xxxx.pt	Não	Não
258_user@ xxxx.pt	Não	Não
259_user@ xxxx.pt	Não	Não
260_user@ xxxx.pt	Sim	Sim
261_user@ xxxx.pt	Não	Não
262_user@ xxxx.pt	Sim	Sim
263_user@ xxxx.pt	Sim	Sim
264_user@ xxxx.pt	Sim	Sim
265_user@ xxxx.pt	Sim	Sim
266_user@ xxxx.pt	Não	Não
267_user@ xxxx.pt	Não	Não
268_user@ xxxx.pt	Não	Não
269_user@ xxxx.pt	Não	Não
270_user@ xxxx.pt	Sim	Sim
271_user@ xxxx.pt	Não	Não
272_user@ xxxx.pt	Não	Não

273_user@ xxxx.pt	Sim	Sim
274_user@ xxxx.pt	Não	Não
275_user@ xxxx.pt	Sim	Sim
276_user@ xxxx.pt	Não	Não
277_user@ xxxx.pt	Sim	Sim
278_user@ xxxx.pt	Não	Não
279_user@ xxxx.pt	Sim	Sim
280_user@ xxxx.pt	Sim	Sim
281_user@ xxxx.pt	Não	Não
282_user@ xxxx.pt	Não	Não
283_user@ xxxx.pt	Não	Não
284_user@ xxxx.pt	Sim	Sim
285_user@ xxxx.pt	Sim	Sim
286_user@ xxxx.pt	Não	Não
287_user@ xxxx.pt	Sim	Sim
288_user@ xxxx.pt	Sim	Sim
289_user@ xxxx.pt	Sim	Sim
290_user@ xxxx.pt	Sim	Não
291_user@ xxxx.pt	Sim	Sim
292_user@ xxxx.pt	Sim	Sim
293_user@ xxxx.pt	Sim	Sim
294_user@ xxxx.pt	Não	Não
295_user@ xxxx.pt	Não	Não
296_user@ xxxx.pt	Não	Não
297_user@ xxxx.pt	Não	Não
298_user@ xxxx.pt	Não	Não
299_user@ xxxx.pt	Não	Não
300_user@ xxxx.pt	Não	Não

ANEXO IV - Estrutura do inquérito aplicado aos utilizadores

Perguntas | Respostas 87

Auscultação sobre Cibersegurança

Este questionário pretende aferir a sua opinião sobre a Cultura de Cibersegurança da empresa, a formação ministrada neste âmbito, e a perceção sobre o papel do utilizador enquanto elemento potenciador desta Cultura.

O questionário foi desenvolvido no âmbito de uma Tese de Mestrado em Informática, em parceria com o ISTEC – Instituto Superior de Tecnologias Avançadas.

A aplicação do presente questionário, respeita o RGPD. Nenhum dado recolhido permite ou pretende caracterizar individualmente os respondentes pelo que é garantido o absoluto anonimato das respostas.

Para qualquer questão adicional, por favor contacte: pauloricardo.dias@my.istec.pt

Caracterização do/a respondente

1. Sexo *

- ○ Feminino
- ○ Masculino
- ○ Não responde

2. Idade *

- ○ 30 ou menos
- ○ 31 a 40
- ○ 41 a 50
- ○ 51 a 60
- ○ 61 ou mais

3. Função desempenhada *

- ○ Administrativo/a
- ○ Quadro Superior sem função de Chefia
- ○ Quadro Superior com função de Chefia
- ○ Operacional/Manutenção

4. Classifique o seu nível de utilização dos Sistemas de Informação da Empresa, no desempenho da sua função (E-mail, VPN, Teams, SAP, entre outros) *

- ○ Não se aplica
- ○ Pouco frequente
- ○ Frequente
- ○ Muito frequente

Cultura de Cibersegurança na Empresa

No âmbito da Cultura de Cibersegurança na Empresa, considera que a Empresa:

5. Promove uma Cultura de Cibersegurança? *

- ○ Sim
- ○ Não
- ○ Não sei responder

6. Divulga as Políticas de Cibersegurança implementadas? *

- ○ Sim
- ○ Não
- ○ Não sei responder

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança? *

- ○ Sim
- ○ Não
- ○ Não sei responder

Cultura de Cibersegurança na Empresa

Considera que os grupos funcionais abaixo identificados influenciam a promoção de uma Cultura de Cibersegurança na Empresa?

8. Decisores/Gestores/Chefias: *

- ○ Sim
- ○ Não
- ○ Não sei responder

9. Equipa de Tecnologias de Informação: *

- ○ Sim
- ○ Não
- ○ Não sei responder

10. Área da Formação: *

- ○ Sim
- ○ Não
- ○ Não sei responder

11. Utilizadores: *

- ○ Sim
- ○ Não
- ○ Não sei responder

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa? *

- ○ Sim
- ○ Não

Comportamentos preventivos

Considera que as medidas abaixo identificadas contribuem para prevenir um Ciberataque na Empresa?

13. Utilizar palavras-chave seguras: *

- ○ Sim
- ○ Não
- ○ Não sei responder

14. Definir níveis de acesso diferentes para vários tipos de utilizadores: *

- ○ Sim
- ○ Não
- ○ Não sei responder

15. Utilizar uma firewall: *

- ○ Sim
- ○ Não
- ○ Não sei responder

16. Implementar software de antivírus, anti-spam e anti-phishing: *

- ○ Sim
- ○ Não
- ○ Não sei responder

17. Realizar ações de sensibilização sobre cibersegurança: *

- ○ Sim
- ○ Não
- ○ Não sei responder

Comportamentos preventivos

18. Utiliza o seu *e-mail* profissional para efetuar registos em sites e aplicações para fins pessoais? *

- ○ Sim
- ○ Não
- ○ Não sei responder

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa? *

- ○ Sim
- ○ Não
- ○ Não sei responder

Formação em Cibersegurança

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança? *

- ○ Sim
- ○ Não
- ○ Não sei responder

21. Se respondeu "Sim" na pergunta anterior, identifique genericamente o tema abordado:

Introduza a sua resposta

ANEXO V - Resultados do inquérito aplicado aos utilizadores

Perguntas Respostas 87

Auscultação sobre Cibersegurança

87	57:32	Fechado
Respostas	Tempo médio de conclusão	Estado

Avaliar as respostas Publicar pontuações Abrir no Excel

1. Sexo

Mais Detalhes Insights

Feminino	46
Masculino	41
Não responde	0

1. Sexo

87 Respostas

ID	Nome	Respostas
1	anonymous	Feminino
2	anonymous	Masculino
3	anonymous	Feminino
4	anonymous	Feminino
5	anonymous	Feminino
6	anonymous	Feminino
7	anonymous	Masculino
8	anonymous	Masculino
9	anonymous	Feminino
10	anonymous	Feminino
11	anonymous	Feminino
12	anonymous	Feminino
13	anonymous	Masculino
14	anonymous	Masculino
15	anonymous	Masculino
16	anonymous	Feminino
17	anonymous	Masculino
18	anonymous	Feminino
19	anonymous	Feminino
20	anonymous	Feminino
21	anonymous	Feminino
22	anonymous	Feminino
23	anonymous	Feminino
24	anonymous	Feminino
25	anonymous	Masculino
26	anonymous	Feminino
27	anonymous	Feminino
28	anonymous	Feminino
29	anonymous	Masculino
30	anonymous	Feminino
31	anonymous	Masculino
32	anonymous	Masculino
33	anonymous	Masculino
34	anonymous	Masculino
35	anonymous	Feminino
36	anonymous	Feminino
37	anonymous	Masculino
38	anonymous	Feminino
39	anonymous	Masculino
40	anonymous	Feminino
41	anonymous	Feminino
42	anonymous	Masculino
43	anonymous	Masculino
44	anonymous	Feminino
45	anonymous	Masculino
46	anonymous	Masculino
47	anonymous	Feminino
48	anonymous	Feminino
49	anonymous	Masculino
50	anonymous	Feminino
51	anonymous	Masculino

52	anonymous	Masculino
53	anonymous	Masculino
54	anonymous	Feminino
55	anonymous	Masculino
56	anonymous	Masculino
57	anonymous	Masculino
58	anonymous	Masculino
59	anonymous	Masculino
60	anonymous	Feminino
61	anonymous	Masculino
62	anonymous	Feminino
63	anonymous	Masculino
64	anonymous	Feminino

65	anonymous	Masculino
66	anonymous	Masculino
67	anonymous	Masculino
68	anonymous	Masculino
69	anonymous	Feminino
70	anonymous	Feminino
71	anonymous	Masculino
72	anonymous	Feminino
73	anonymous	Masculino
74	anonymous	Feminino
75	anonymous	Masculino
76	anonymous	Feminino
77	anonymous	Feminino

78	anonymous	Feminino
79	anonymous	Masculino
80	anonymous	Feminino
81	anonymous	Feminino
82	anonymous	Masculino
83	anonymous	Feminino
84	anonymous	Masculino
85	anonymous	Masculino
86	anonymous	Feminino
87	anonymous	Feminino

2. Idade

Mais Detalhes | Insights

30 ou menos	3
31 a 40	30
41 a 50	31
51 a 60	20
61 ou mais	3

2. Idade

87 Respostas

ID↑	Nome	Respostas
1	anonymous	31 a 40
2	anonymous	31 a 40
3	anonymous	41 a 50
4	anonymous	31 a 40
5	anonymous	31 a 40
6	anonymous	31 a 40
7	anonymous	51 a 60
8	anonymous	31 a 40
9	anonymous	31 a 40
10	anonymous	31 a 40
11	anonymous	61 ou mais
12	anonymous	30 ou menos
13	anonymous	41 a 50
14	anonymous	41 a 50
15	anonymous	51 a 60
16	anonymous	41 a 50
17	anonymous	31 a 40
18	anonymous	41 a 50
19	anonymous	41 a 50
20	anonymous	31 a 40
21	anonymous	31 a 40
22	anonymous	61 ou mais
23	anonymous	31 a 40
24	anonymous	41 a 50
25	anonymous	31 a 40
26	anonymous	31 a 40
27	anonymous	31 a 40
28	anonymous	51 a 60
29	anonymous	30 ou menos
30	anonymous	51 a 60
31	anonymous	31 a 40
32	anonymous	41 a 50
33	anonymous	31 a 40
34	anonymous	51 a 60
35	anonymous	31 a 40
36	anonymous	41 a 50
37	anonymous	31 a 40
38	anonymous	41 a 50
39	anonymous	41 a 50
40	anonymous	61 ou mais
41	anonymous	41 a 50
42	anonymous	31 a 40
43	anonymous	41 a 50
44	anonymous	51 a 60
45	anonymous	51 a 60
46	anonymous	41 a 50
47	anonymous	31 a 40
48	anonymous	41 a 50
49	anonymous	41 a 50
50	anonymous	31 a 40
51	anonymous	41 a 50
52	anonymous	51 a 60
53	anonymous	51 a 60
54	anonymous	41 a 50
55	anonymous	41 a 50
56	anonymous	31 a 40
57	anonymous	31 a 40
58	anonymous	41 a 50
59	anonymous	51 a 60
60	anonymous	51 a 60
61	anonymous	41 a 50
62	anonymous	51 a 60
63	anonymous	51 a 60
64	anonymous	30 ou menos
65	anonymous	41 a 50
66	anonymous	51 a 60
67	anonymous	41 a 50
68	anonymous	51 a 60
69	anonymous	51 a 60
70	anonymous	41 a 50
71	anonymous	31 a 40
72	anonymous	41 a 50
73	anonymous	41 a 50
74	anonymous	41 a 50
75	anonymous	51 a 60
76	anonymous	31 a 40
77	anonymous	31 a 40
78	anonymous	41 a 50
79	anonymous	31 a 40
80	anonymous	51 a 60
81	anonymous	41 a 50
82	anonymous	41 a 50
83	anonymous	51 a 60
84	anonymous	41 a 50
85	anonymous	31 a 40
86	anonymous	51 a 60
87	anonymous	31 a 40

3. Função desempenhada

Mais Detalhes

Administrativo/a	34
Quadro Superior sem função ...	27
Quadro Superior com função ...	22
Operacional/Manutenção	4

3. Função desempenhada

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Quadro Superior sem função de Chefia
2	anonymous	Quadro Superior sem função de Chefia
3	anonymous	Quadro Superior com função de Chefia
4	anonymous	Quadro Superior com função de Chefia
5	anonymous	Administrativo/a
6	anonymous	Quadro Superior com função de Chefia
7	anonymous	Administrativo/a
8	anonymous	Quadro Superior sem função de Chefia
9	anonymous	Quadro Superior com função de Chefia
10	anonymous	Quadro Superior com função de Chefia
11	anonymous	Quadro Superior com função de Chefia
12	anonymous	Quadro Superior sem função de Chefia
13	anonymous	Administrativo/a
14	anonymous	Administrativo/a
15	anonymous	Quadro Superior sem função de Chefia
16	anonymous	Administrativo/a
17	anonymous	Quadro Superior sem função de Chefia
18	anonymous	Quadro Superior com função de Chefia
19	anonymous	Quadro Superior com função de Chefia
20	anonymous	Administrativo/a
21	anonymous	Quadro Superior sem função de Chefia
22	anonymous	Quadro Superior com função de Chefia
23	anonymous	Quadro Superior sem função de Chefia
24	anonymous	Quadro Superior com função de Chefia
25	anonymous	Quadro Superior sem função de Chefia
26	anonymous	Quadro Superior sem função de Chefia
27	anonymous	Quadro Superior sem função de Chefia
28	anonymous	Quadro Superior com função de Chefia
29	anonymous	Quadro Superior sem função de Chefia
30	anonymous	Administrativo/a
31	anonymous	Quadro Superior sem função de Chefia
32	anonymous	Quadro Superior sem função de Chefia
33	anonymous	Administrativo/a
34	anonymous	Administrativo/a
35	anonymous	Administrativo/a
36	anonymous	Quadro Superior sem função de Chefia
37	anonymous	Quadro Superior sem função de Chefia
38	anonymous	Quadro Superior sem função de Chefia
39	anonymous	Administrativo/a
40	anonymous	Administrativo/a
41	anonymous	Administrativo/a
42	anonymous	Quadro Superior com função de Chefia
43	anonymous	Operacional/Manutenção
44	anonymous	Quadro Superior sem função de Chefia
45	anonymous	Administrativo/a
46	anonymous	Administrativo/a
47	anonymous	Administrativo/a
48	anonymous	Quadro Superior com função de Chefia
49	anonymous	Quadro Superior sem função de Chefia
50	anonymous	Administrativo/a
51	anonymous	Quadro Superior com função de Chefia
52	anonymous	Operacional/Manutenção
53	anonymous	Quadro Superior com função de Chefia
54	anonymous	Administrativo/a
55	anonymous	Administrativo/a
56	anonymous	Quadro Superior com função de Chefia
57	anonymous	Quadro Superior sem função de Chefia
58	anonymous	Administrativo/a
59	anonymous	Administrativo/a
60	anonymous	Quadro Superior sem função de Chefia
61	anonymous	Quadro Superior com função de Chefia
62	anonymous	Administrativo/a
63	anonymous	Quadro Superior com função de Chefia
64	anonymous	Quadro Superior sem função de Chefia
65	anonymous	Administrativo/a
66	anonymous	Administrativo/a
67	anonymous	Administrativo/a
68	anonymous	Administrativo/a
69	anonymous	Quadro Superior sem função de Chefia
70	anonymous	Administrativo/a
71	anonymous	Quadro Superior com função de Chefia
72	anonymous	Administrativo/a
73	anonymous	Administrativo/a
74	anonymous	Quadro Superior sem função de Chefia
75	anonymous	Operacional/Manutenção
76	anonymous	Quadro Superior sem função de Chefia
77	anonymous	Administrativo/a
78	anonymous	Quadro Superior com função de Chefia
79	anonymous	Administrativo/a
80	anonymous	Administrativo/a
81	anonymous	Administrativo/a
82	anonymous	Administrativo/a
83	anonymous	Quadro Superior com função de Chefia
84	anonymous	Operacional/Manutenção
85	anonymous	Quadro Superior sem função de Chefia
86	anonymous	Quadro Superior com função de Chefia
87	anonymous	Quadro Superior sem função de Chefia

4. Classifique o seu nível de utilização dos Sistemas de Informação da Empresa, no desempenho da sua função (E-mail, VPN, Teams, SAP, entre outros)

Mais Detalhes | Insights

Não se aplica	0
Pouco frequente	1
Frequente	19
Muito frequente	67

4. Classifique o seu nível de utilização dos Sistemas de Informação da Empresa, no desempenho da sua função (E-mail, VPN, Teams, SAP, entre outros)

87 Respostas

ID	Nome	Respostas
1	anonymous	Muito frequente
2	anonymous	Muito frequente
3	anonymous	Muito frequente
4	anonymous	Muito frequente
5	anonymous	Muito frequente
6	anonymous	Muito frequente
7	anonymous	Muito frequente
8	anonymous	Muito frequente
9	anonymous	Muito frequente
10	anonymous	Muito frequente
11	anonymous	Muito frequente
12	anonymous	Muito frequente
13	anonymous	Frequente
14	anonymous	Muito frequente
15	anonymous	Frequente
16	anonymous	Frequente
17	anonymous	Muito frequente
18	anonymous	Muito frequente
19	anonymous	Muito frequente
20	anonymous	Frequente
21	anonymous	Muito frequente
22	anonymous	Muito frequente
23	anonymous	Muito frequente
24	anonymous	Muito frequente
25	anonymous	Frequente
26	anonymous	Muito frequente
27	anonymous	Frequente
28	anonymous	Muito frequente
29	anonymous	Muito frequente
30	anonymous	Muito frequente
31	anonymous	Muito frequente
32	anonymous	Muito frequente
33	anonymous	Muito frequente
34	anonymous	Muito frequente
35	anonymous	Muito frequente
36	anonymous	Muito frequente
37	anonymous	Muito frequente
38	anonymous	Muito frequente
39	anonymous	Muito frequente
40	anonymous	Muito frequente
41	anonymous	Muito frequente
42	anonymous	Muito frequente
43	anonymous	Frequente
44	anonymous	Muito frequente
45	anonymous	Frequente
46	anonymous	Muito frequente
47	anonymous	Muito frequente
48	anonymous	Muito frequente
49	anonymous	Muito frequente
50	anonymous	Muito frequente
51	anonymous	Frequente
52	anonymous	Frequente
53	anonymous	Muito frequente
54	anonymous	Muito frequente
55	anonymous	Muito frequente
56	anonymous	Muito frequente
57	anonymous	Muito frequente
58	anonymous	Frequente
59	anonymous	Muito frequente
60	anonymous	Muito frequente
61	anonymous	Muito frequente
62	anonymous	Muito frequente
63	anonymous	Muito frequente
64	anonymous	Muito frequente
65	anonymous	Frequente
66	anonymous	Frequente
67	anonymous	Muito frequente
68	anonymous	Muito frequente
69	anonymous	Muito frequente
70	anonymous	Frequente
71	anonymous	Muito frequente
72	anonymous	Frequente
73	anonymous	Frequente
74	anonymous	Frequente
75	anonymous	Frequente
76	anonymous	Muito frequente
77	anonymous	Muito frequente
78	anonymous	Muito frequente
79	anonymous	Muito frequente
80	anonymous	Muito frequente
81	anonymous	Muito frequente
82	anonymous	Pouco frequente
83	anonymous	Muito frequente
84	anonymous	Muito frequente
85	anonymous	Frequente
86	anonymous	Muito frequente
87	anonymous	Muito frequente

5. Promove uma Cultura de Cibersegurança?

Mais Detalhes | Insights

Sim	57
Não	13
Não sei responder	17

5. Promove uma Cultura de Cibersegurança?

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Não
2	anonymous	Não
3	anonymous	Sim
4	anonymous	Não
5	anonymous	Sim
6	anonymous	Não sei responder
7	anonymous	Não sei responder
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Não

5. Promove uma Cultura de Cibersegurança?

87 Respostas

13	anonymous	Sim
14	anonymous	Não sei responder
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Não sei responder
19	anonymous	Sim
20	anonymous	Não
21	anonymous	Sim
22	anonymous	Sim
23	anonymous	Não
24	anonymous	Sim
25	anonymous	Não sei responder

5. Promove uma Cultura de Cibersegurança?

87 Respostas

26	anonymous	Não sei responder
27	anonymous	Não sei responder
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Não
32	anonymous	Não sei responder
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim
36	anonymous	Não
37	anonymous	Sim
38	anonymous	Sim

5. Promove uma Cultura de Cibersegurança?

87 Respostas

39	anonymous	Sim
40	anonymous	Não
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Não
44	anonymous	Não sei responder
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Não sei responder
51	anonymous	Sim

5. Promove uma Cultura de Cibersegurança?

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Não
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Sim

5. Promove uma Cultura de Cibersegurança?

87 Respostas

65	anonymous	Não
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Não sei responder
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Não sei responder
77	anonymous	Não sei responder

5. Promove uma Cultura de Cibersegurança?

87 Respostas

75	anonymous	Sim
76	anonymous	Não sei responder
77	anonymous	Não sei responder
78	anonymous	Não sei responder
79	anonymous	Sim

80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Não sei responder
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

6. Divulga as Políticas de Cibersegurança implementadas?

Mais Detalhes | Insights

Sim	29
Não	40
Não sei responder	18

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

ID↑	Nome	Respostas
1	anonymous	Não
2	anonymous	Não
3	anonymous	Sim
4	anonymous	Não
5	anonymous	Não sei responder
6	anonymous	Não
7	anonymous	Não sei responder
8	anonymous	Sim
9	anonymous	Não sei responder
10	anonymous	Não
11	anonymous	Não sei responder
12	anonymous	Não

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

13	anonymous	Sim
14	anonymous	Não sei responder
15	anonymous	Não sei responder
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Não
19	anonymous	Sim
20	anonymous	Não
21	anonymous	Sim
22	anonymous	Não
23	anonymous	Não
24	anonymous	Não
25	anonymous	Não sei responder

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

26	anonymous	Não sei responder
27	anonymous	Não sei responder
28	anonymous	Não
29	anonymous	Não
30	anonymous	Sim
31	anonymous	Não
32	anonymous	Não
33	anonymous	Sim
34	anonymous	Não
35	anonymous	Não sei responder
36	anonymous	Não
37	anonymous	Sim
38	anonymous	Não sei responder

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

39	anonymous	Não
40	anonymous	Não
41	anonymous	Não
42	anonymous	Não sei responder
43	anonymous	Não
44	anonymous	Não
45	anonymous	Sim
46	anonymous	Não
47	anonymous	Não
48	anonymous	Sim
49	anonymous	Não
50	anonymous	Não sei responder
51	anonymous	Sim

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Não
56	anonymous	Não
57	anonymous	Não
58	anonymous	Não sei responder
59	anonymous	Sim
60	anonymous	Não
61	anonymous	Não
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não sei responder

6. Divulga as Políticas de Cibersegurança implementadas?

87 Respostas

65	anonymous	Não
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Não
69	anonymous	Não
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não
73	anonymous	Não
74	anonymous	Não
75	anonymous	Sim
76	anonymous	Não sei responder
77	anonymous	Não

78	anonymous	Não
79	anonymous	Sim
80	anonymous	Não sei responder
81	anonymous	Não
82	anonymous	Não sei responder
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Não

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

Mais Detalhes | Insights

Sim	18
Não	49
Não sei responder	20

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Não
3	anonymous	Não
4	anonymous	Não
5	anonymous	Não sei responder
6	anonymous	Não
7	anonymous	Não sei responder
8	anonymous	Sim
9	anonymous	Não sei responder
10	anonymous	Não
11	anonymous	Não sei responder

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

12	anonymous	Não
13	anonymous	Sim
14	anonymous	Não sei responder
15	anonymous	Sim
16	anonymous	Não sei responder
17	anonymous	Não
18	anonymous	Não
19	anonymous	Sim
20	anonymous	Não
21	anonymous	Não sei responder
22	anonymous	Não
23	anonymous	Não

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

24	anonymous	Não
25	anonymous	Não sei responder
26	anonymous	Não sei responder
27	anonymous	Não
28	anonymous	Não
29	anonymous	Não
30	anonymous	Não sei responder
31	anonymous	Não
32	anonymous	Não
33	anonymous	Não
34	anonymous	Não
35	anonymous	Não sei responder

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

36	anonymous	Não
37	anonymous	Não
38	anonymous	Não
39	anonymous	Não
40	anonymous	Não
41	anonymous	Não
42	anonymous	Não sei responder
43	anonymous	Não
44	anonymous	Não
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

48	anonymous	Não
49	anonymous	Não
50	anonymous	Não sei responder
51	anonymous	Sim
52	anonymous	Sim
53	anonymous	Não
54	anonymous	Sim
55	anonymous	Não
56	anonymous	Não
57	anonymous	Não
58	anonymous	Não sei responder
59	anonymous	Não sei responder
60	anonymous	Não

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

61	anonymous	Não
62	anonymous	Sim
63	anonymous	Não sei responder
64	anonymous	Não
65	anonymous	Não
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Não
69	anonymous	Não
70	anonymous	Sim
71	anonymous	Não
72	anonymous	Não

7. Investe em formação e em ações de sensibilização no âmbito da Cibersegurança?

87 Respostas

73	anonymous	Não sei responder
74	anonymous	Não
75	anonymous	Sim
76	anonymous	Não
77	anonymous	Não sei responder
78	anonymous	Não

79	anonymous	Não
80	anonymous	Não sei responder
81	anonymous	Não
82	anonymous	Sim
83	anonymous	Não
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Não sei responder
87	anonymous	Não

8. Decisores/Gestores/Chefias:

Mais Detalhes | Insights

Sim	44
Não	29
Não sei responder	14

8. Decisores/Gestores/Chefias:

87 Respostas

ID	Nome	Respostas
1	anonymous	Sim
2	anonymous	Não
3	anonymous	Não
4	anonymous	Sim
5	anonymous	Não sei responder
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Sim

8. Decisores/Gestores/Chefias:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Não sei responder
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Não sei responder
22	anonymous	Não sei responder
23	anonymous	Não
24	anonymous	Não
25	anonymous	Não

8. Decisores/Gestores/Chefias:

87 Respostas

26	anonymous	Sim
27	anonymous	Não
28	anonymous	Sim
29	anonymous	Não
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Não
33	anonymous	Não
34	anonymous	Não
35	anonymous	Sim
36	anonymous	Não
37	anonymous	Sim
38	anonymous	Não sei responder

8. Decisores/Gestores/Chefias:

87 Respostas

39	anonymous	Não
40	anonymous	Sim
41	anonymous	Não
42	anonymous	Não
43	anonymous	Não
44	anonymous	Não
45	anonymous	Não
46	anonymous	Não
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Não sei responder
51	anonymous	Sim

8. Decisores/Gestores/Chefias:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Não sei responder
57	anonymous	Não
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Não
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Não sei responder
64	anonymous	Sim

8. Decisores/Gestores/Chefias:

87 Respostas

65	anonymous	Não sei responder
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Não sei responder
71	anonymous	Não
72	anonymous	Não sei responder
73	anonymous	Não
74	anonymous	Não
75	anonymous	Sim
76	anonymous	Não
77	anonymous	Não

78	anonymous	Não
79	anonymous	Sim
80	anonymous	Não sei responder
81	anonymous	Sim
82	anonymous	Não
83	anonymous	Não
84	anonymous	Não
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

9. Equipa de Tecnologias de Informação:

Mais Detalhes | Insights

Sim	70
Não	9
Não sei responder	8

9. Equipa de Tecnologias de Informação:

87 Respostas

ID↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Sim
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Sim

9. Equipa de Tecnologias de Informação:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Sim
23	anonymous	Sim
24	anonymous	Não
25	anonymous	Não sei responder

9. Equipa de Tecnologias de Informação:

87 Respostas

26	anonymous	Sim
27	anonymous	Não
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Sim
34	anonymous	Não
35	anonymous	Sim
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim

9. Equipa de Tecnologias de Informação:

87 Respostas

39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Não
42	anonymous	Sim
43	anonymous	Sim
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Não
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Sim
51	anonymous	Sim

9. Equipa de Tecnologias de Informação:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Não
61	anonymous	Não sei responder
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Sim

9. Equipa de Tecnologias de Informação:

87 Respostas

65	anonymous	Não sei responder
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não sei responder
73	anonymous	Não
74	anonymous	Não
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Sim

78	anonymous	Não sei responder
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Não
83	anonymous	Sim
84	anonymous	Não sei responder
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

10. Área da Formação:

Mais Detalhes | Insights

Sim	37
Não	27
Não sei responder	23

10. Área da Formação:

87 Respostas

ID↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Não
3	anonymous	Não
4	anonymous	Sim
5	anonymous	Não sei responder
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Não sei responder
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Sim

10. Área da Formação:

87 Respostas

13	anonymous	Sim
14	anonymous	Não sei responder
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Não
18	anonymous	Não
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Não sei responder
22	anonymous	Sim
23	anonymous	Não
24	anonymous	Não
25	anonymous	Não sei responder

10. Área da Formação:

87 Respostas

26	anonymous	Sim
27	anonymous	Não
28	anonymous	Sim
29	anonymous	Não
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Não
33	anonymous	Não
34	anonymous	Não
35	anonymous	Sim
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Não sei responder

10. Área da Formação:

87 Respostas

39	anonymous	Não
40	anonymous	Sim
41	anonymous	Não
42	anonymous	Não
43	anonymous	Não sei responder
44	anonymous	Não
45	anonymous	Sim
46	anonymous	Não
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Não sei responder
51	anonymous	Sim

10. Área da Formação:

87 Respostas

52	anonymous	Não sei responder
53	anonymous	Não
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Não
58	anonymous	Não
59	anonymous	Sim
60	anonymous	Não
61	anonymous	Não sei responder
62	anonymous	Não sei responder
63	anonymous	Sim
64	anonymous	Sim

10. Área da Formação:

87 Respostas

65	anonymous	Não sei responder
66	anonymous	Não
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Não sei responder
70	anonymous	Sim
71	anonymous	Não sei responder
72	anonymous	Não sei responder
73	anonymous	Não
74	anonymous	Não
75	anonymous	Não sei responder
76	anonymous	Não sei responder
77	anonymous	Não

78	anonymous	Não
79	anonymous	Não sei responder
80	anonymous	Não sei responder
81	anonymous	Sim
82	anonymous	Não sei responder
83	anonymous	Não
84	anonymous	Não
85	anonymous	Sim
86	anonymous	Não sei responder
87	anonymous	Sim

11. Utilizadores:

Mais Detalhes | Insights

Sim	34
Não	33
Não sei responder	20

11. Utilizadores:

87 Respostas

ID	Nome	Respostas
1	anonymous	Sim
2	anonymous	Não
3	anonymous	Não
4	anonymous	Não
5	anonymous	Não sei responder
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Não sei responder
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Não

11. Utilizadores:

87 Respostas

13	anonymous	Sim
14	anonymous	Não sei responder
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Não
18	anonymous	Não
19	anonymous	Não sei responder
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Não
23	anonymous	Não
24	anonymous	Não
25	anonymous	Não sei responder

11. Utilizadores:

87 Respostas

26	anonymous	Sim
27	anonymous	Não
28	anonymous	Sim
29	anonymous	Não
30	anonymous	Sim
31	anonymous	Não
32	anonymous	Não
33	anonymous	Não sei responder
34	anonymous	Não
35	anonymous	Não sei responder
36	anonymous	Não
37	anonymous	Sim
38	anonymous	Não

11. Utilizadores:

87 Respostas

39	anonymous	Sim
40	anonymous	Não
41	anonymous	Não
42	anonymous	Sim
43	anonymous	Não
44	anonymous	Não
45	anonymous	Sim
46	anonymous	Não
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Não sei responder
51	anonymous	Sim

11. Utilizadores:

87 Respostas

52	anonymous	Sim
53	anonymous	Não sei responder
54	anonymous	Sim
55	anonymous	Não
56	anonymous	Não
57	anonymous	Não
58	anonymous	Sim
59	anonymous	Não sei responder
60	anonymous	Não
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Não sei responder
64	anonymous	Sim

11. Utilizadores:

87 Respostas

65	anonymous	Não sei responder
66	anonymous	Não
67	anonymous	Sim
68	anonymous	Não
69	anonymous	Não sei responder
70	anonymous	Não sei responder
71	anonymous	Não
72	anonymous	Não sei responder
73	anonymous	Não
74	anonymous	Não
75	anonymous	Não sei responder
76	anonymous	Não
77	anonymous	Não

78	anonymous	Não
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Não sei responder
83	anonymous	Não sei responder
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

Mais Detalhes | Insights

Sim	65
Não	22

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Sim
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Não
10	anonymous	Sim
11	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

12	anonymous	Sim
13	anonymous	Sim
14	anonymous	Não
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Não
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Não
22	anonymous	Sim
23	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

24	anonymous	Sim
25	anonymous	Não
26	anonymous	Não
27	anonymous	Não
28	anonymous	Não
29	anonymous	Não
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Não
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

36	anonymous	Sim
37	anonymous	Não
38	anonymous	Sim
39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Não
44	anonymous	Não
45	anonymous	Sim
46	anonymous	Não
47	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

48	anonymous	Sim
49	anonymous	Não
50	anonymous	Não
51	anonymous	Sim
52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não
65	anonymous	Não
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Não
69	anonymous	Não
70	anonymous	Sim
71	anonymous	Sim

12. Sabe quem é a área ou pessoa responsável pela Segurança Informática na Empresa?

87 Respostas

72	anonymous	Não
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Não
76	anonymous	Sim
77	anonymous	Sim

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

13. Utilizar palavras-chave seguras:

Mais Detalhes | Insights

Sim	83
Não	3
Não sei responder	1

13. Utilizar palavras-chave seguras:

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Sim
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Sim
12	anonymous	Sim

13. Utilizar palavras-chave seguras:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Sim
23	anonymous	Sim
24	anonymous	Sim
25	anonymous	Sim

13. Utilizar palavras-chave seguras:

87 Respostas

26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim

13. Utilizar palavras-chave seguras:

87 Respostas

39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Sim
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não
48	anonymous	Sim
49	anonymous	Não sei responder
50	anonymous	Sim
51	anonymous	Sim

13. Utilizar palavras-chave seguras:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Não
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Sim

13. Utilizar palavras-chave seguras:

87 Respostas

65	anonymous	Sim
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Sim

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

Mais Detalhes

Sim	77
Não	5
Não sei responder	5

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

ID	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Sim
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Sim
12	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Sim
23	anonymous	Sim
24	anonymous	Sim
25	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Não sei responder
34	anonymous	Sim
35	anonymous	Não sei responder
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

39	anonymous	Não
40	anonymous	Não
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Não
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Não sei responder
51	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Sim

14. Definir níveis de acesso diferentes para vários tipos de utilizadores:

87 Respostas

65	anonymous	Sim
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Não sei responder
76	anonymous	Sim
77	anonymous	Não

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

15. Utilizar uma firewall:

Mais Detalhes | Insights

Sim	70
Não	1
Não sei responder	16

15. Utilizar uma firewall:

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Não sei responder
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Não sei responder
12	anonymous	Sim

15. Utilizar uma firewall:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Não sei responder
23	anonymous	Não sei responder
24	anonymous	Sim
25	anonymous	Não sei responder

15. Utilizar uma firewall:

87 Respostas

26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Não sei responder
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim
36	anonymous	Não sei responder
37	anonymous	Sim
38	anonymous	Sim

15. Utilizar uma firewall:

87 Respostas

39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Sim
42	anonymous	Não sei responder
43	anonymous	Sim
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não sei responder
48	anonymous	Sim
49	anonymous	Não sei responder
50	anonymous	Sim
51	anonymous	Sim

15. Utilizar uma firewall:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Não
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não sei responder

15. Utilizar uma firewall:

87 Respostas

65	anonymous	Sim
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Não sei responder
72	anonymous	Não sei responder
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Não sei responder

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Não sei responder
84	anonymous	Não sei responder
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

16. Implementar software de antivírus, anti-spam e anti-phishing:

Mais Detalhes | Insights

Sim	82
Não	0
Não sei responder	5

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

ID	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Não sei responder
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Sim
12	anonymous	Sim

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Não sei responder
23	anonymous	Sim
24	anonymous	Sim
25	anonymous	Sim

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Sim
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Sim
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Sim
51	anonymous	Sim

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não sei responder

16. Implementar software de antivírus, anti-spam e anti-phishing:

87 Respostas

65	anonymous	Sim
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não sei responder
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Não sei responder

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

17. Realizar ações de sensibilização sobre cibersegurança:

Mais Detalhes | Insights

Sim	78
Não	4
Não sei responder	5

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Não sei responder
5	anonymous	Sim
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Sim
10	anonymous	Sim
11	anonymous	Sim
12	anonymous	Sim

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

13	anonymous	Sim
14	anonymous	Sim
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Sim
21	anonymous	Sim
22	anonymous	Não
23	anonymous	Sim
24	anonymous	Sim
25	anonymous	Sim

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Sim
34	anonymous	Sim
35	anonymous	Sim
36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

39	anonymous	Sim
40	anonymous	Sim
41	anonymous	Sim
42	anonymous	Não sei responder
43	anonymous	Não sei responder
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Sim
48	anonymous	Sim
49	anonymous	Sim
50	anonymous	Sim
51	anonymous	Sim

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Não
55	anonymous	Sim
56	anonymous	Não
57	anonymous	Sim
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim
61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não sei responder

17. Realizar ações de sensibilização sobre cibersegurança:

87 Respostas

65	anonymous	Sim
66	anonymous	Sim
67	anonymous	Sim
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não sei responder
73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Não

78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Sim
81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Sim
85	anonymous	Sim
86	anonymous	Sim
87	anonymous	Sim

18. Utiliza o seu *e-mail* profissional para efetuar registos em sites e aplicações para fins pessoais?

Mais Detalhes | Insights

Sim	7
Não	80
Não sei responder	0

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Não
2	anonymous	Não
3	anonymous	Não
4	anonymous	Não
5	anonymous	Não
6	anonymous	Não
7	anonymous	Não
8	anonymous	Não
9	anonymous	Não
10	anonymous	Não
11	anonymous	Sim

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

12	anonymous	Não
13	anonymous	Não
14	anonymous	Não
15	anonymous	Não
16	anonymous	Sim
17	anonymous	Não
18	anonymous	Não
19	anonymous	Não
20	anonymous	Não
21	anonymous	Não
22	anonymous	Não
23	anonymous	Não

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

24	anonymous	Não
25	anonymous	Não
26	anonymous	Não
27	anonymous	Não
28	anonymous	Não
29	anonymous	Não
30	anonymous	Não
31	anonymous	Não
32	anonymous	Não
33	anonymous	Não
34	anonymous	Não
35	anonymous	Não

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

36	anonymous	Não
37	anonymous	Não
38	anonymous	Não
39	anonymous	Não
40	anonymous	Sim
41	anonymous	Não
42	anonymous	Não
43	anonymous	Não
44	anonymous	Não
45	anonymous	Não
46	anonymous	Não
47	anonymous	Sim

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

48	anonymous	Não
49	anonymous	Sim
50	anonymous	Não
51	anonymous	Não
52	anonymous	Não
53	anonymous	Não
54	anonymous	Não
55	anonymous	Não
56	anonymous	Não
57	anonymous	Não
58	anonymous	Não
59	anonymous	Não

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

60	anonymous	Não
61	anonymous	Não
62	anonymous	Não
63	anonymous	Não
64	anonymous	Não
65	anonymous	Não
66	anonymous	Não
67	anonymous	Não
68	anonymous	Não
69	anonymous	Não
70	anonymous	Não
71	anonymous	Não

18. Utiliza o seu e-mail profissional para efetuar registos em sites e aplicações para fins pessoais?

87 Respostas

72	anonymous	Não
73	anonymous	Não
74	anonymous	Não
75	anonymous	Não
76	anonymous	Não
77	anonymous	Sim
78	anonymous	Sim
79	anonymous	Não

80	anonymous	Não
81	anonymous	Não
82	anonymous	Não
83	anonymous	Não
84	anonymous	Não
85	anonymous	Não
86	anonymous	Não
87	anonymous	Não

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

Mais Detalhes | Insights

Sim	66
Não	11
Não sei responder	10

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

ID	Nome	Respostas
1	anonymous	Sim
2	anonymous	Sim
3	anonymous	Sim
4	anonymous	Não
5	anonymous	Não sei responder
6	anonymous	Sim
7	anonymous	Sim
8	anonymous	Sim
9	anonymous	Não
10	anonymous	Sim
11	anonymous	Não sei responder

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

12	anonymous	Sim
13	anonymous	Sim
14	anonymous	Não
15	anonymous	Sim
16	anonymous	Sim
17	anonymous	Sim
18	anonymous	Sim
19	anonymous	Sim
20	anonymous	Não sei responder
21	anonymous	Sim
22	anonymous	Sim
23	anonymous	Sim

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

24	anonymous	Sim
25	anonymous	Não sei responder
26	anonymous	Sim
27	anonymous	Sim
28	anonymous	Sim
29	anonymous	Sim
30	anonymous	Sim
31	anonymous	Sim
32	anonymous	Sim
33	anonymous	Não sei responder
34	anonymous	Sim
35	anonymous	Sim

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

36	anonymous	Sim
37	anonymous	Sim
38	anonymous	Sim
39	anonymous	Sim
40	anonymous	Não
41	anonymous	Sim
42	anonymous	Sim
43	anonymous	Sim
44	anonymous	Sim
45	anonymous	Sim
46	anonymous	Sim
47	anonymous	Não
48	anonymous	Sim

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

49	anonymous	Não sei responder
50	anonymous	Não sei responder
51	anonymous	Sim
52	anonymous	Sim
53	anonymous	Sim
54	anonymous	Sim
55	anonymous	Sim
56	anonymous	Sim
57	anonymous	Não
58	anonymous	Sim
59	anonymous	Sim
60	anonymous	Sim

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

61	anonymous	Sim
62	anonymous	Sim
63	anonymous	Sim
64	anonymous	Não sei responder
65	anonymous	Sim
66	anonymous	Não
67	anonymous	Não
68	anonymous	Sim
69	anonymous	Sim
70	anonymous	Sim
71	anonymous	Sim
72	anonymous	Não sei responder

19. Considera que esta utilização apresenta algum risco para a segurança da informação e dos sistemas da Empresa?

87 Respostas

73	anonymous	Sim
74	anonymous	Sim
75	anonymous	Sim
76	anonymous	Sim
77	anonymous	Não
78	anonymous	Sim
79	anonymous	Sim
80	anonymous	Não sei responder

81	anonymous	Sim
82	anonymous	Sim
83	anonymous	Sim
84	anonymous	Não
85	anonymous	Não
86	anonymous	Sim
87	anonymous	Sim

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

Mais Detalhes | Insights

Sim	5
Não	81
Não sei responder	1

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

ID ↑	Nome	Respostas
1	anonymous	Não
2	anonymous	Não
3	anonymous	Não
4	anonymous	Não
5	anonymous	Não
6	anonymous	Não
7	anonymous	Não
8	anonymous	Sim
9	anonymous	Não
10	anonymous	Não
11	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

12	anonymous	Não
13	anonymous	Não
14	anonymous	Não
15	anonymous	Sim
16	anonymous	Não
17	anonymous	Não
18	anonymous	Não
19	anonymous	Não sei responder
20	anonymous	Não
21	anonymous	Não
22	anonymous	Não
23	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

24	anonymous	Não
25	anonymous	Não
26	anonymous	Não
27	anonymous	Não
28	anonymous	Não
29	anonymous	Não
30	anonymous	Não
31	anonymous	Não
32	anonymous	Não
33	anonymous	Não
34	anonymous	Não
35	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

36	anonymous	Não
37	anonymous	Não
38	anonymous	Não
39	anonymous	Não
40	anonymous	Não
41	anonymous	Não
42	anonymous	Não
43	anonymous	Não
44	anonymous	Não
45	anonymous	Não
46	anonymous	Não
47	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

48	anonymous	Não
49	anonymous	Não
50	anonymous	Não
51	anonymous	Sim
52	anonymous	Não
53	anonymous	Não
54	anonymous	Não
55	anonymous	Não
56	anonymous	Não
57	anonymous	Não
58	anonymous	Não
59	anonymous	Sim
60	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

61	anonymous	Não
62	anonymous	Não
63	anonymous	Não
64	anonymous	Não
65	anonymous	Não
66	anonymous	Sim
67	anonymous	Não
68	anonymous	Não
69	anonymous	Não
70	anonymous	Não
71	anonymous	Não
72	anonymous	Não

20. Já realizou alguma formação ou ação de sensibilização, desenvolvida pela Empresa, no âmbito da Cibersegurança?

87 Respostas

73	anonymous	Não
74	anonymous	Não
75	anonymous	Não
76	anonymous	Não
77	anonymous	Não
78	anonymous	Não
79	anonymous	Não
80	anonymous	Não

81	anonymous	Não
82	anonymous	Não
83	anonymous	Não
84	anonymous	Não
85	anonymous	Não
86	anonymous	Não
87	anonymous	Não

21. Se respondeu “Sim” na pergunta anterior, identifique genericamente o tema abordado:

6 Respostas

ID ↑	Nome	Respostas
1	anonymous	fiz formação sobre o tema de ciber segurança por iniciativa propria
2	anonymous	RGPD e implicações nas aplicações e comunicações internas.
3	anonymous	Webinar - Proteção de dados Pessoais
4	anonymous	RGPD, no que respeita a medidas técnicas e organizativas apropriadas a garantir segurança adequada relativamente aos dados pessoais.
5	anonymous	A utilização de PW seguras, não as transmitir a ninguém, não entrar em links diretamente, como este :), espero que seja seguro, não entrar em sites estranhos, etc.
6	anonymous	A informação classificada

ANEXO VI – Divulgação da ação de sensibilização

Formação em Cibersegurança

:Comunicação interna
Para

Responder | Responder a Todos | Reencaminhar | ...
seg 09/08/2021 15:22

Formação em Cibersegurança

Participação e conclusão até 30 de setembro 2021

Internet – Está consciente da sua (in)segurança?

De forma a dotar os Colaboradores de mais conhecimento, sobre esta matéria, a [redacted] está a promover uma ação de formação sobre Cibersegurança, contando com a participação de todos, no curso Cidadão Ciberseguro.

+ Informação sobre o contexto da Formação em Cibersegurança >>

Destinatários
O curso "Cidadão Ciberseguro" foi desenhado para todos os cidadãos, em geral, e tem uma adequada aplicação aos Colaboradores da [redacted], tendo em conta os riscos decorrentes da utilização da Internet e dos equipamentos eletrónicos da empresa.

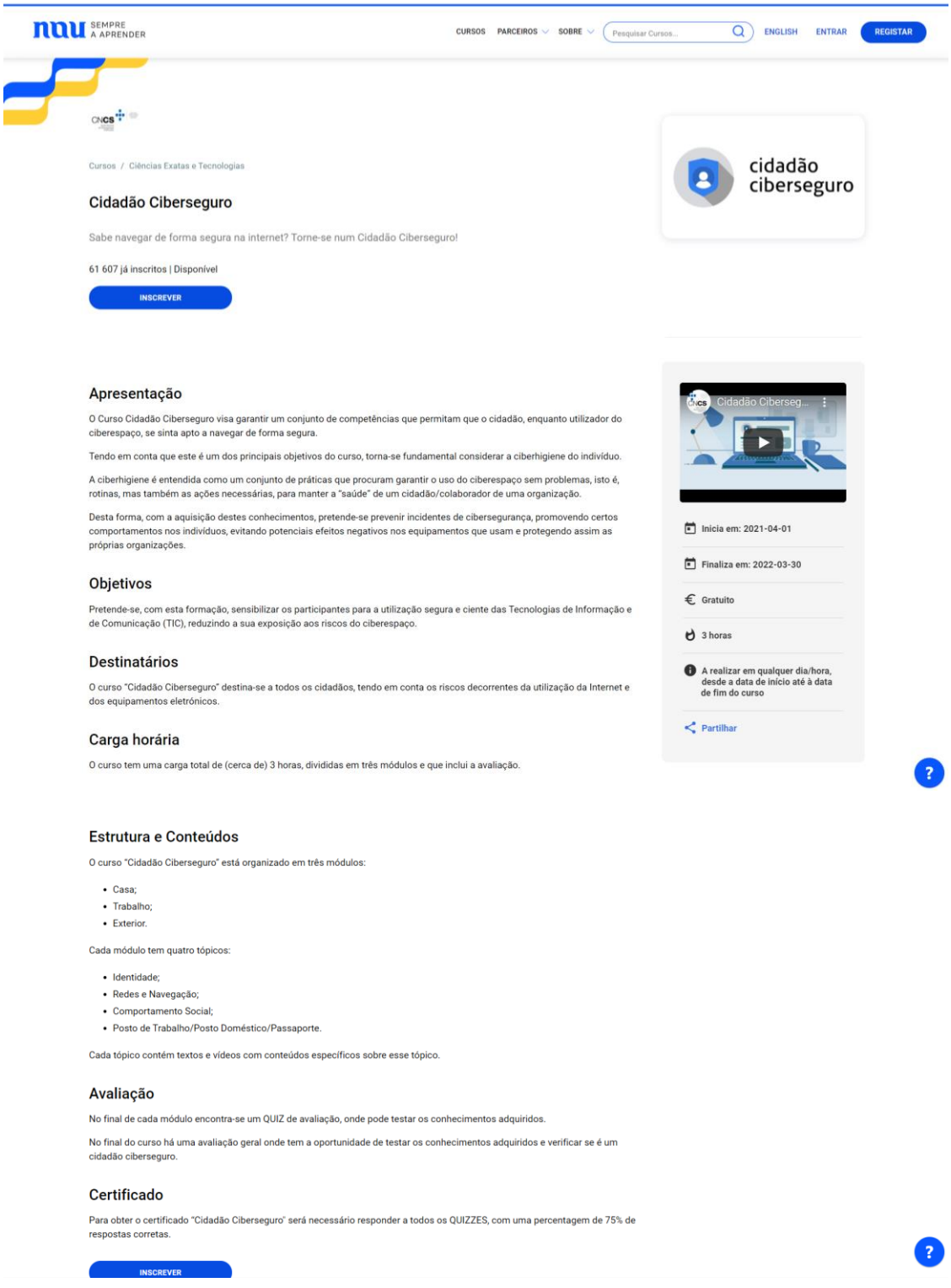
Link de inscrição >>
Para frequência da ação aconselha-se a utilização do browser – Google Chrome.

Programa
O curso tem uma carga total de 3 horas, divididas em três módulos, incluindo a avaliação.

Certificado
Para obter o certificado "Cidadão Ciberseguro" será necessário responder aos quizzes, dos vários módulos, com uma percentagem de 75% de respostas corretas.

Após a conclusão do curso deverá ser descarregado um Certificado digital (PDF) e remetido, via e-mail, para a Direção de Gestão de Pessoas (DGP), através do seguinte endereço de correio eletrónico: [redacted]

ANEXO VII – Programa da Ação de Sensibilização



ANEXO VIII – Proposta de Módulo formativo

Área de formação: Cibersegurança

Curso: Cultura de Cibersegurança e *Phishing*

Descritivo

Este módulo pretende:

- Esclarecer o conceito de Cultura de Cibersegurança;
- Sensibilizar os Colaboradores para o seu papel no desenvolvimento da Cultura de Cibersegurança;
- Esclarecer o conceito de *phishing*;
- Sensibilizar os Colaboradores para o seu papel na prevenção de um ataque de *phishing*.

Objetivos

No final da formação, os Colaboradores deverão ser capazes de:

- Compreender o conceito de Cultura de Cibersegurança;
- Identificar os intervenientes no desenvolvimento da Cultura de Cibersegurança e respetivas responsabilidades;
- Compreender o conceito de *phishing;*
- Compreender o papel do fator humano na prevenção de um ataque de *phishing*.

Target

Sessões parciais com grupos de 20 pessoas (máximo).

Todos os Colaboradores que exerçam funções nas áreas corporativas e de suporte à operação/manutenção (Administrativos/as, Quadros Superiores com e sem funções de Chefia, área Operacional/Manutenção).

Carga horária: 2 horas

Organização da ação: *Online*, via Microsoft Teams.

Metodologia de Avaliação: Exercícios de avaliação a realizar durante a ação.

Recursos pedagógicos

- Computador
- Acesso à Internet
- Apresentação

Desenvolvimento da ação

Fase	Conteúdos Programáticos	Material	Duração
Apresentação formador e formandos		Computador; Ligação à Internet; *Microsoft Teams*	10 min
Aferição de conhecimentos sobre o conceito de Cultura de Cibersegurança		Computador; Ligação à Internet; *Microsoft Teams*	10 min
Parte I – Cultura de Cibersegurança	- O que é a Cultura de Cibersegurança - Qual a importância da Cultura de Cibersegurança - Como tornar a Cultura de Cibersegurança eficaz - Quem desenvolve/influencia a Cultura de Cibersegurança - Qual o papel dos Colaboradores na Cultura de Cibersegurança	Computador; Ligação à Internet; *Microsoft Teams*	20 min
Exercício 1	Sistematização do conceito de Cultura de Cibersegurança	Computador; Ligação à Internet; *Microsoft Teams; Link* com formulário de exercício	15 min
Parte II - *Phishing*	- O que é o *Phishing* - Apresentação de estatísticas globais sobre este tipo de cibercrime - Qual o procedimento neste tipo de ciberataque - Quais os riscos associados ao fator humano - De que forma o comportamento humano pode afetar a organização - Como prevenir um ataque de *Phishing*	Computador; Ligação à Internet; *Microsoft Teams*	40 min
Exercício 2	Sistematização do conceito de *Phishing*	Computador; Ligação à Internet; *Microsoft Teams; Link* com formulário de exercício	15 min
Dúvidas e questões	Espaço aberto para questões dos formandos	Computador; Ligação à Internet; *Microsoft Teams*	10 min

Apresentação do Módulo Formativo

Parte I

Cultura de Cibersegurança

2

Que palavras ou expressões associam à Cultura de Cibersegurança?

3

O que é a Cultura de Cibersegurança?

É o conjunto de "**conhecimento, crenças, perceções, atitudes, suposições, normas e valores das pessoas em relação à segurança cibernética e como eles se manifestam no comportamento das pessoas com as tecnologias da informação**".

ENISA - *The European Union Agency for Cybersecurity* (2018, p. 5)

4

Qual a importância da Cultura de Cibersegurança?

Influencia a forma de pensar de todos os indivíduos;

Promove resiliência contra ciberataques, em particular os que derivam da Engenharia Social;

Evita impor outras medidas de segurança que inibam a eficácia do desempenho de funções de cada Colaborador.

5

Como se torna a Cultura de Cibersegurança eficaz?

Envolvendo TODOS os Colaboradores da organização.

Munindo todos os Colaboradores de ferramentas, conhecimento, competências e compreensão sobre o seu papel e contributo.

Fazendo com que todas as pessoas dentro da empresa ajam no sentido de reduzir o risco.

6

Quem desenvolve a Cultura de Cibersegurança?

Decisores/Gestores/Chefias

Equipa de Tecnologias de Informação

Área da Formação

Colaboradores/Utilizadores

7

E quem tem maior influência?

TODOS por igual, cada um com o seu papel.

8

Qual o papel dos Colaboradores?

Ser atento e crítico.

Estar informado sobre as boas práticas de Cibersegurança.

Alertar sobre atividade suspeita.

Utilizar sistemas de segurança nos equipamentos pessoais e profissionais.

Exercício I

Sistematização | Cultura de Cibersegurança

Exercício I

Módulo Formativo - Cultura de Cibersegurança e Phishing

1. O que é a Cultura de Cibersegurança? *

- ( ) Um conjunto de sistemas de proteção informática
- ( ) Um conjunto de regras de prevenção imposto pela Política de Cibersegurança
- ( ) Um conjunto de conhecimentos, atitudes, normas e valores das pessoas em relação à segurança cibernética

2. Quem influencia a Cultura de Cibersegurança? *

- ( ) Os Decisores
- ( ) A Equipa de Tecnologias de Informação
- ( ) Todos os Colaboradores da Empresa

3. De que forma cada Colaborador contribui para a Cultura de Cibersegurança? *

- ( ) Utilizando os equipamentos profissionais para fins pessoais
- ( ) Estando alerta e informado sobre as boas práticas de Cibersegurança e tendo um papel ativo na prevenção de riscos
- ( ) Delegando a responsabilidade na Equipa de Tecnologias de Informação

Parte II

Phishing

11

O que é o phishing?

É um **ataque de Engenharia Social**, baseado no uso da tecnologia, que **utiliza o indivíduo como um meio para atingir um fim**.

Nos ataques de Engenharia Social, os criminosos manipulam a mente humana, através de falsificação, desorientação e mentiras para atingirem os seus objetivos.

É uma forma de cibercrime, uma tentativa fraudulenta de aceder a informações financeiras, credenciais do sistema ou outros dados sensíveis.

O termo "*phishing*" surgiu na década de 90 associado ao facto dos *hackers* utilizarem *e-mails* fraudulentos para "pescar" informações às vítimas.

12

Algumas estatísticas

Em **2020**, um estudo desenvolvido pela Kaspersky, apresenta **Portugal** como o **2º país do mundo com mais vítimas de *phishing***.

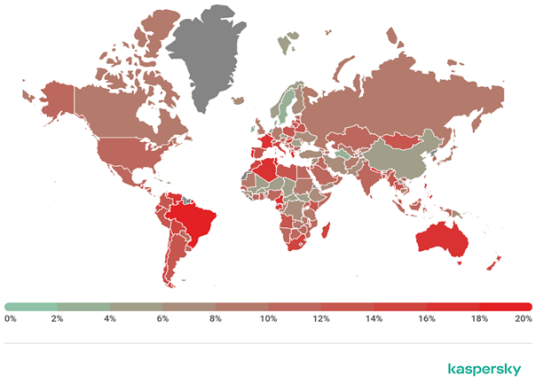


Imagem 1 – a geografia dos ataques de phishing em 2020

Fonte: https://www.computerworld.com.pt/2021/03/15/portugal-e-o-segundo-pais-do-mundo-com-mais-vitimas-de-phishing/

13

Algumas estatísticas

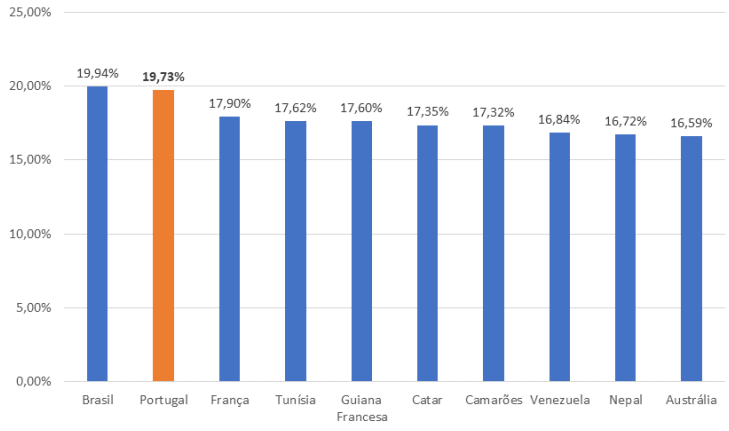


Imagem 2 – Top 10 dos países com mais vítimas de *phishing* em 2020

Fonte: https://www.computerworld.com.pt/2021/03/15/portugal-e-o-segundo-pais-do-mundo-com-mais-vitimas-de-phishing/

14

Qual o procedimento neste tipo de ciberataque?

A vítima pode ser abordada por **e-mail**, **chamada telefónica ou mensagem**.

A comunicação é aparentemente credível e **remete para fontes oficiais**, tais como entidades bancárias, financeiras, ou alguém que represente uma autoridade (organizacional ou outra).

Encoberto pela necessidade de verificação de dados, **o atacante pode solicitar à vítima os dados** que lhe irão permitir aceder ao sistema, tais como o utilizador, *password*, número de cartão ou códigos de acesso, **ou ceder um *link* ou anexo que comporta *software* malicioso**.

15

Riscos associados ao fator humano

Identificam-se alguns **comportamentos de risco** que podem facilitar um ataque de *phishing:*

- Utilização de *e-mails* profissionais para fins pessoais;
- Acesso a *websites* não fidedignos;
- Abertura de anexos ou links de e-mail de spam e/ou de fontes não fidedignas;
- Partilha indevida de *passwords* e de informações privadas ou corporativas;
- Entre outros.

16

Como é que estes comportamentos podem afetar uma organização?

Ao ser alvo de um ataque de *phishing*, o utilizador/colaborador poderá ceder ao atacante um ponto de entrada no Sistema de Informação da empresa.

Já dentro do sistema, o atacante poderá aceder ou bloquear informações críticas para o negócio.

17

Como prevenir um ataque de *phishing*

- **Não abrir quaisquer, *links*, ficheiros ou anexos suspeitos, recebidos de fontes desconhecidas;**
- **Não descarregar e/ou instalar aplicações a partir de fontes não fidedignas;**
- **Utilizar *passwords* únicas com combinação de caracteres pouco óbvia;**
- Utilizar a autenticação de multi fatores;
- Manter os sistemas atualizados;
- Utilizar sistemas de segurança e *software* antivírus adequados aos diversos dispositivos.

18

Exercício II

Sistematização | *Phishing*

19

Exercício II

Módulo Formativo - Cultura de Cibersegurança e Phishing

1. O que é o Phishing? *

- ○ Uma técnica de pesquisa de informação relevante
- ○ Um cibercrime que utiliza a tecnologia para bloquear o computador do utilizador
- ○ Um ataque de Engenharia Social que utiliza a pessoa/vítima para aceder a informação crítica

2. Identifique dois comportamentos de risco dos utilizadores que podem facilitar um ataque de Phishing: *

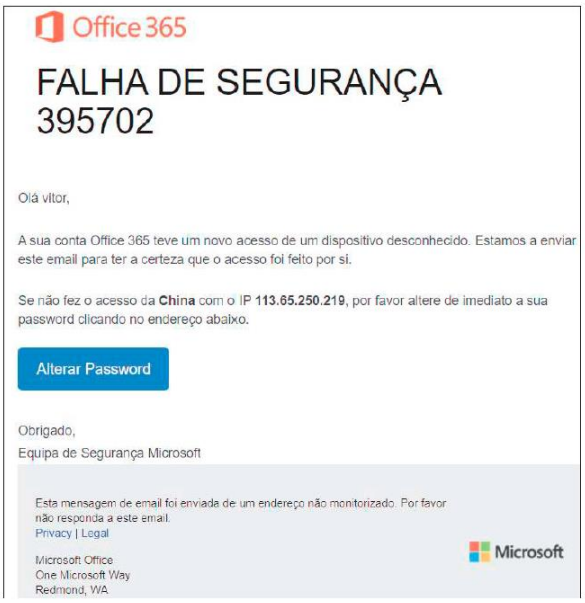
Introduza a sua resposta

3. Identifique duas boas práticas que podem prevenir um ataque de Phishing: *

- [ ] Desligar o computador sempre que se ausenta do local de trabalho
- [ ] Não abrir e-mails, links ou anexos suspeitos
- [ ] Guardar as passwords num ficheiro dentro do computador
- [ ] Utilizar passwords com combinações de caracteres pouco óbvias
- [ ] Adiar as atualizações do sistema sempre que recebe notificações

ANEXO IX – *Templates* do segundo ataque simulado

Template de *e-mail* enviado no segundo ataque simulado



Template da *Landing Page* enviada no segundo ataque simulado