INTERFACE TECNOLÓGICA

A CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA

THE GROWING IMPORTANCE OF INFORMATION SECURITY, ESPECIALLY IN THE PANDEMIC PERIOD

José Henrique Baptista Junior – jhbaptista2016@gmail.com
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo - Brasil

Maurício de Oliveira Dian – mauricio.dian@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga – Taquaritinga – São Paulo - Brasil

DOI: 10.31510/infa.v18i1.1109
Data de submissão: 14/04/2021
Data do aceite: 09/07/2021
Data da publicação: 30/07/2021

RESUMO

Presente na rotina de todas as pessoas, seja na vida particular ou no ambiente corporativo, a tecnologia tem como objetivo auxiliar a vida da sociedade e resolver problemas de forma inteligente, mas seu uso sem as devidas medidas de segurança pode possibilitar brechas para ataques mal-intencionados e causar prejuízos em larga escala. Sendo assim, este trabalho se propõe a realizar uma revisão de conceitos voltados a segurança da informação, ao crescimento do número de ciberataques ao longo dos anos, os tipos de ataques mais evidentes e ainda contextualizar a crescente importância da segurança da informação sobretudo com a chegada e as consequências que a pandemia trouxe no que se refere ao trabalho remoto adotado durante o período e a evidente demanda por profissionais especializados na área de segurança da informação.

Palavras-chave: Segurança da Informação. Ciberataques. Crescente importância da Segurança.

ABSTRACT

Being at routine of all people, be in the particular life or in a corporate ambience, the technology has as purpose helping the society life and solve problems by a smart way, but your use without the appropriate measures of security can enable gaps for malicious attacks and cause large-scale damages. Therefore, this work proposes to perform a review of concepts focused at information security, the increasement in the number of cyber attacks throught the years, the most evident types of attacks and also to contextualize the growing importance of data security, especially with

the pandemic arrival and the consequences that brought with regard to the remote work adopted during the period and the evident demand for professionals specialized in the area of information security.

Keywords: Information Security. Cyberattacks. Growing Importance of Security.

1. INTRODUÇÃO

O início da "Era da Informação" fez com que as empresas, as organizações governamentais e a não governamentais (ONGs) trouxessem a utilização das tecnologias da informação para seus cotidianos e, sendo assim, houve um aumento e propagação exponencial do uso da TI pelo mundo. Consequentemente, surgiram os crimes digitais e, por conta disso, surgiu também a necessidade crescente de manter as informações e os ativos organizacionais de maneira segura e livres de riscos que possam ameaçar sobretudo a integridade, a disponibilidade e a confidencialidade que a segurança da informação tanto presa.

Um problema que pode existir, sobretudo nas pequenas e médias empresas, é a falta de preocupação quanto a segurança da informação. Em muitos casos, os funcionários e gestores não tem a consciência de que as políticas de segurança da informação se fazem necessárias e precisam ser seguidas para melhor proteger os recursos da empresa. A ABNT NBR 27002 (2013), reforça essa ideia dizendo que atualmente a informação pode ser encarada como um importante ativo para as instituições e, sendo assim, é preciso que todos tenham um olhar crítico quando o assunto se trata de segurança de dados.

Durante a pandemia e com o fato de muitas empresas terem de aderir massivamente o *home office*, a necessidade de segurança da informação cresceu ainda mais dentro das empresas. Índices apontam que houve um grande aumento sobretudo nos ataques dos tipos *phishing*, *spam*, *ransomware* e fraudes que estão cada vez mais elaborados e contextualizados com o tema "COVID-19" para aumentar a eficiência dos golpes (SOBERS, 2021).

Este trabalho tem por objetivo realizar uma revisão bibliográfica e de conceitos sobre a informação e sua segurança, contextualizar a crescente de ataques cibernéticos e, como consequência, a crescente importância de se manter seguro e o aumento da demanda por profissionais do setor sobretudo nos últimos anos.

Para alcançar tal objetivo, a metodologia adotada se define pela revisão de livros, artigos, matérias especializadas, levantamento de dados sobre incidentes de segurança e análise de gráficos relacionados. O estudo se justifica para mostrar a importância de se manter seguro visto que o número de ciberataques aumenta cada vez mais e durante a pandemia estes números se tornaram ainda mais expressivos e ocasionaram grandes prejuízos ao redor do mundo.

2. A INFORMAÇÃO E A SUA SEGURANÇA

A informação pode ser definida como um conjunto de dados que, quando organizados devidamente, geram conhecimento útil sobre um determinado assunto (CAIÇARA JUNIOR, 2012).

Dantas (2011) afirma que é possível classificá-la em quatro tipos: as informações públicas, que são aquelas que têm baixo grau de relevância e em geral não necessitam tanta proteção; as informações internas, que são aquelas que o acesso não autorizado deverá ser evitado, apesar de que, se ocorrer, os impactos não serão dos mais sérios; as informações confidenciais, que são aquelas que devem ser restringidas de acesso externo, preservando a confidencialidade e sendo acessadas somente por pessoas autorizadas, uma vez que podem causar grande impacto na organização prejudicando os lucros ou com perda de competitividade da empresa diante das concorrentes; e por fim, as informações secretas, que são as mais críticas, pois são vitais para a existência dos negócios da empresa e, portanto, o acesso deve ser preservado a qualquer custo e restrito a apenas algumas pessoas.

A partir do entendimento de tais classificações fica mais fácil mensurar os impactos com possíveis perdas e incidentes que podem vir a ocorrer na organização e, através disso, desenvolver estratégias de proteção mais adequadas e ajustadas para cada tipo de informação e ativo tecnológico que a empresa possuir.

Com o passar do tempo, a informação foi se tornando cada vez mais um dos principais ativos empresariais, principalmente em nível estratégico e, com isso, as empresas passaram a valorizar mais esse ativo e consequentemente aumentou-se a preocupação com sua proteção (CAIÇARA JUNIOR, 2012).

Uma ameaça às informações e aos ativos empresariais poderá ser qualquer coisa que as prejudique com a finalidade de causar impactos ou perdas consideráveis. Alterações, corrupções, indisponibilidade e vazamentos de informações sigilosas são alguns exemplos. Essas ameaças utilizam as vulnerabilidades existentes no ambiente, sejam elas físicas, naturais, de hardware, de software ou até humanas, para impossibilitar a continuidade dos negócios através da concretização de algum tipo de ataque. (LAUREANO, 2005).

Desta forma é possível afirmar que a segurança da informação é a área da tecnologia que busca garantir as características que dão qualidade à informação e seu principal papel é realizar a preservação dos atributos básicos das informações (ABNT NBR ISO/IEC 27002:2013).

Sendo assim, e segundo Dantas (2011, p.13), se faz necessário a Segurança da Informação, pois através da aplicação dos seus conceitos, métodos e políticas, é possível garantir maior proteção contra os riscos e ameaças à informação e ainda promover maior continuidade e lucratividade dos negócios.

3. CIBERATAQUES E A IMPORTÂNCIA DE SE MANTER SEGURO

Foi em meados década de 90 que as redes e internet se popularizaram e marcaram o crescimento e expansão dos vírus de computador, o "boom da internet" e o surgimento da *World Wide Web.* Com maior acesso às informações e o aumento da conectividade entre vários estudantes de computação e entusiastas pela cultura hacker, houve o início de grandes ataques mal-intencionados, ou como podemos chamar: os ciberataques (MALWAREBYTES, 2021).

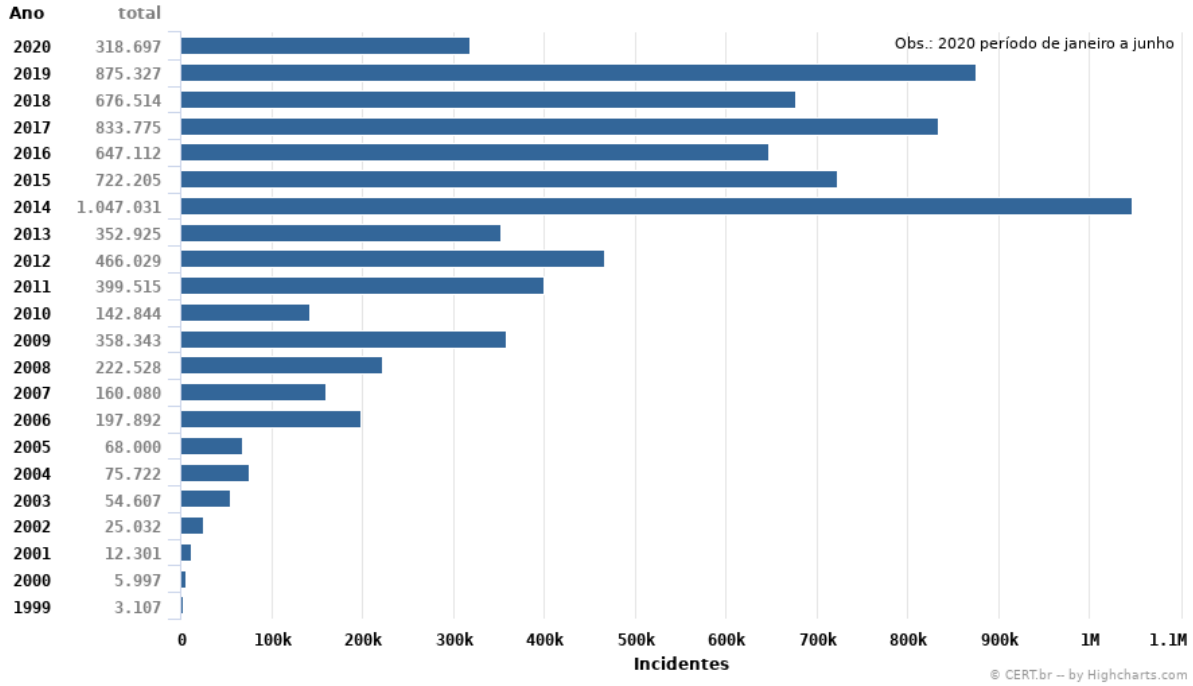
De modo geral, estes ataques cibernéticos são uma tentativa de invadir sistemas e computadores para adquirir, roubar, criptografar ou bloquear o acesso de usuários às informações. Estes ataques cibernéticos podem ser realizados de maneiras diferentes e cada uma dessas maneiras tem suas peculiaridades e formas de ação para atingir o seu objetivo, passando a serem classificados de acordo com o modo como agem e estando entre os principais os *exploits* e os *malwares* (CERT.BR., 2012).

Segundo a Malwarebytes (2021), há várias motivações para estes ataques, porém os que mais chamam atenção são os ciberataques com foco em ganho financeiro e espionagem

corporativa, onde o ataque consiste em criptografar ou roubar informações importantes para uma empresa, obrigando-a pagar para obter acesso novamente as informações perdidas ou em caso de espionagem para manter as informações em sigilo.

Com a crescente utilização da internet e dos meios digitais com o passar dos anos, os ataques cibernéticos foram se tornando cada vez mais rotineiros no uso diário de quem trabalha com algum tipo de tecnologia. Observe no Gráfico 1 o aumento dos ataques cibernéticos documentados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.BR) de Janeiro 1999 até Junho de 2020.

Gráfico 1 - Total de Incidentes Reportados ao CERT.BR por Ano



Fonte: CERT.BR. (2020)

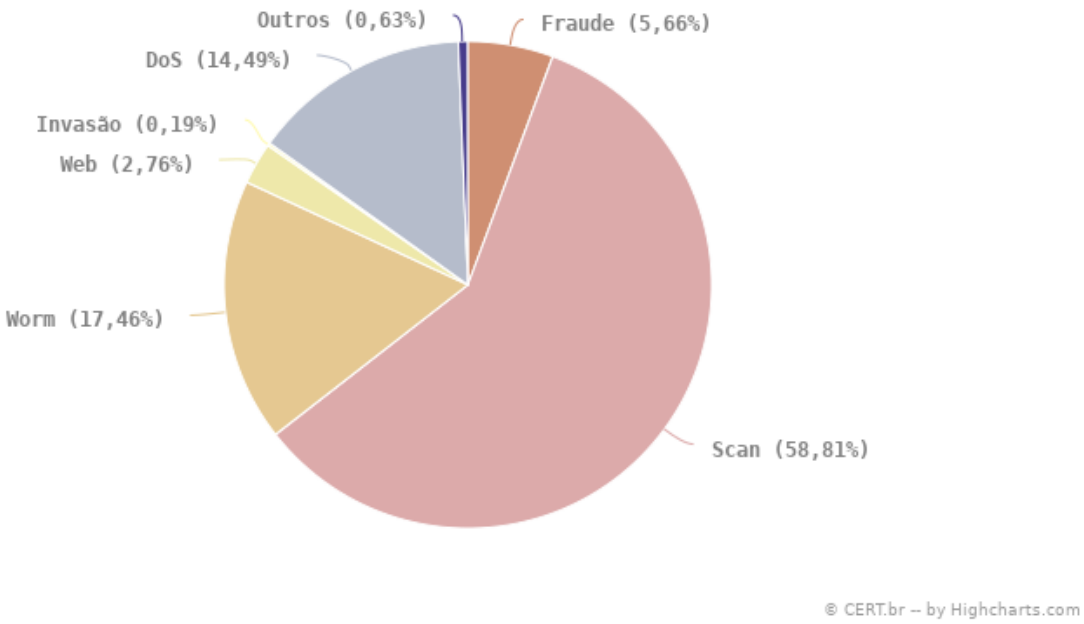
Ao analisar o Gráfico 1, é evidente o crescimento dos incidentes com segurança da informação. Segundo Cert.br (2020) desde que o censo começou a ser realizado até Junho de 2020 houve um aumento de aproximadamente 33600% nos índices de ataques reportados, tendo seu ápice em 2014 com mais de 1 milhão de incidentes naquele ano.

Com o decorrer dos anos, os ataques cibernéticos evoluem e novos tipos acabam surgindo na busca por se tornarem mais eficazes. Como os cibercriminosos buscam contextualizar muitos de seus ataques com base em eventos e assuntos em alta de momento para direcionar melhor e obter maior êxito em seus crimes, é provável que essa crescente em 2014 tenha ocorrido devido ao Brasil ter sido sede da Copa do Mundo da FIFA e ter vivido um momento politicamente conturbado, com protestos e manifestações políticas ao governo da época. Segundo Canaltech (2014), muito disso teve influência inclusive do grupo hacktivista *Anonymous* que cumpriu suas promessas e realizou uma série de ataques a sites de empresas patrocinadoras do evento além de entidades do governo, tudo como forma de manifestação aos altos gastos para a realização do torneio.

E mesmo após o ano de 2014 e uma imaginada queda no total de incidentes em 2015, o Brasil ainda continuou a ser alvo de uma quantidade grande de ataques. Segundo UOL (2018, apud Norton Cyber Security, 2017) em 2017 o Brasil ocupava o segundo lugar entre os países no mundo com maiores números de crimes cibernéticos. Até a data de publicação deste artigo o Brasil ainda figura entre os principais países-alvo.

Segundo o Cert.br (2020), e conforme ilustra o Gráfico 2, de Janeiro à Junho de 2020 em levantamento realizado pelo centro de estudos foi constatado que os ataques do tipo *scan*, *worms* e de negação de serviço (DOS) foram os mais praticados por criminosos virtuais no país.

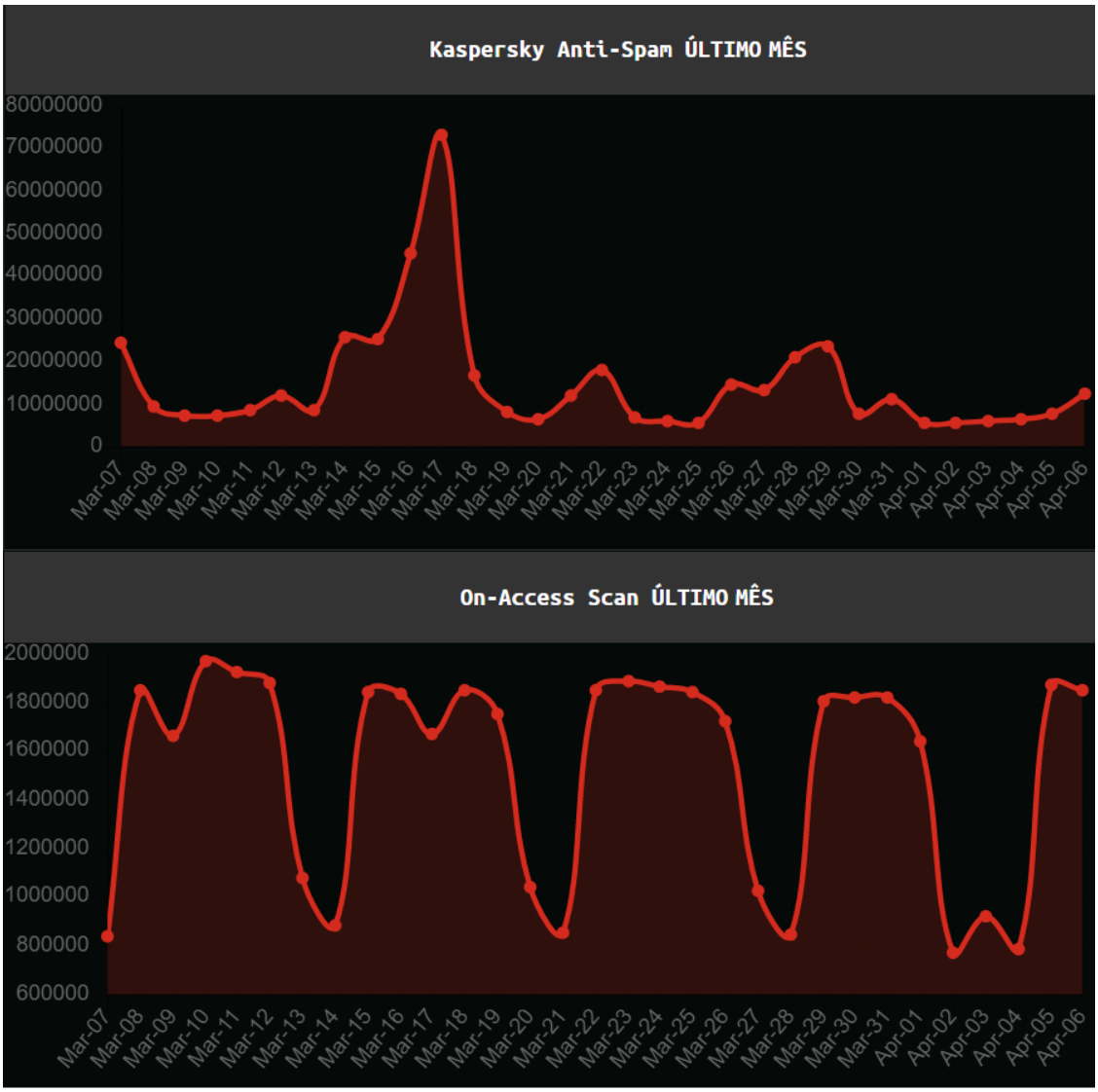
Gráfico 2- Incidentes Reportados ao CERT.br -- Janeiro a Junho de 2020



Fonte: CERT.BR. (2020)

E não parou por aí. Tomando como exemplo dados disponibilizados por uma das maiores fabricantes de software antivírus atualmente e, conforme o Gráfico 3 logo abaixo, no período de 07 de Março de 2021 à 06 de Abril de 2021, foram detectados mais de 460 milhões de *spams* e mais de 47 milhões de ocorrências relacionadas a detecção de práticas de escaneamento de vulnerabilidades (KASPERSKY, 2021).

Gráfico 3 - Ataques detectados pelo Kaspersky o período de 07 de Março de 2021 a 06 de Abril de 2021



Fonte: Adaptado de Kaspersky (2021)

Sobers (2021) afirma ainda que realmente as tendências de segurança da informação para 2021 sejam de que é preciso se proteger sobretudo contra os ataques dos tipos *phishing*, *whaling*, engenharia social, *ransomware* e de negação de serviço distribuída (DDoS). São esses segundo ele os que permanecem em alta ao redor do mundo.

Com esse aumento de preocupações e de incidentes, as empresas estão cada vez mais em busca de profissionais de segurança da informação capacitados. Com base em pesquisa realizada,

em 2019 o mercado de trabalho já empregava 2,8 milhões de profissionais, apesar do déficit global ter chegado a 4 milhões. Só na América Latina haviam aproximadamente 600 mil vagas em aberto ainda segundo a pesquisa (SOPESP, 2020 apud (ISC)², 2019).

Ano após ano no país, a crescente preocupação com segurança da informação foi sendo notada e, em decorrência disso, surgiram novas leis como a Crimes Cibernéticos (Lei 12.737/12), o Marco Civil (Lei 12.965/14) e, mais recentemente, a Lei Geral de Proteção de Dados (Lei 13.709/18) que há pouco entrou em vigor.

Mesmo tendo o país registrado 486 milhões de funcionários de segurança da informação em 2019, o mercado brasileiro continua na busca por profissionais da área plenamente capacitados e com conhecimentos em conexões remotas e VPNs, infraestrutura e segurança, redes e *cloud computing* para atender essa demanda em época de isolamento social (SOPESP, 2020 apud (ISC)², 2019).

Muitas empresas, inclusive, para se adequar às exigências da LGPD começaram a buscar profissionais de segurança da informação capacitados e até mesmo a treinar os que já possuíam diante da necessidade de se adequar à nova lei que, efetivamente, entrou em vigor em Agosto de 2020 (MEUSUCESSO, 2019).

Além disso, levando em consideração o "fator pandemia" que obrigou as pessoas a mudar seu comportamento para novos hábitos e alavancou o uso da tecnologia como principal meio de comunicação, estudos, aulas remotas, entretenimento e até mesmo para trabalhar, como é no caso do *home office*. Com essa mudança toda, novos riscos e vulnerabilidades surgiram e segundo a Computerworld (2021, apud Cybersecurity) a tendência é que tudo isso continuará a crescer durante os próximos meses ou até mesmo anos.

Estatísticas apontaram que devido ao isolamento social provocado pela pandemia os ataques cresceram 50% durante a migração para *home office.* Como agravante, o fato de cada funcionário ter seus próprios dispositivos e rede de internet fez com que o número de ataques crescesse também em 50% no segundo semestre de 2020, ataques estes como roubo de credenciais e instalação de *ransomwares.* Além disso houve aumento de aproximadamente 300% no número de registro de domínios com relação às vacinas do COVID-19, sendo 29% deles suspeitos de envolvimento com algum tipo de golpe. 46% das empresas detectaram pelo menos um de seus funcionários realizando downloads de aplicativos maliciosos e, portanto, colocando

suas credenciais em risco e expondo a rede e os dados da empresa a possíveis ataques. Ainda segundo a pesquisa, a cada 10 segundos uma empresa é alvo de uma tentativa de ataque *ransomware* ao redor do mundo (DEMARTINI, 2021 apud CHECK POINT SOFTWARE TECHNOLOGIES, 2020).

Segundo Brito (2020, apud Enterprise Strategy Group) a necessidade de manter-se seguro cresceu tanto que no mercado mundial falta profissionais qualificados para atender a demanda de vagas abertas. Ainda segundo ele, em 2020 a falta de profissionais da área de segurança para ocupar as vagas em aberto afetou 70% das empresas do mundo inteiro.

Melo (2020) reforça dizendo que a cibersegurança nunca teve tanta importância quanto nos últimos tempos, com a crescente de ataques e ameaças durante a pandemia e as brechas de segurança abertas pelo *home office,* os atacantes veem a situação atual como uma oportunidade e, portanto, a conscientização da necessidade de investir cada vez mais em cibersegurança também aumentou, especialmente no mundo corporativo.

A abordagem das empresas quanto a segurança da informação como um tópico importante, apesar de estar mudando aos poucos, ainda é um desafio a ser superado. Os profissionais da área devem assumir a postura de contextualizar e conscientizar a cibersegurança para os demais colaboradores, facilitando o entendimento sobre o assunto, quebrando conceitos enraizados, demonstrando os riscos e conscientizando sobre a importância de se utilizar soluções inteligentes para garantir segurança da informação (MELO, 2020).

4. CONSIDERAÇÕES FINAIS

O aumento nos números de incidentes demonstra que manter as informações seguras ainda é um desafio a ser superado e, apesar do surgimento de medidas e leis ao longo dos anos para tentar combater os crimes digitais, os ataques ainda se tornaram cada vez mais recorrentes, especialmente durante a pandemia.

Em virtude desses acontecimentos e da migração para o regime *home office* causado pelo COVID-19 as empresas passaram a ter um olhar mais crítico quanto a esse assunto e as consequências disso foi um aumento na procura por profissionais qualificados para a área de

segurança da informação o que afetou diretamente o mercado de trabalho gerando novas vagas e oportunidades na área.

De fato, a segurança da informação vem ganhando notoriedade e importância cada vez mais, porém sempre se faz necessário que medidas de proteção sejam adotadas por parte das empresas como investimentos em profissionais da área caso ainda não tenham, readequação de suas estratégias e medidas de segurança diante das exigências das legislações criadas em prol da segurança e conscientização e treinamento dos colaboradores sobre os riscos e ameaças.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICA. **NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2013. 99 p.

BRITO, Paulo. Falta de pessoal de cibersegurança afeta 70% das organizações. **Ciso Adviser**, 2020. Disponível em: https://www.cisoadvisor.com.br/falta-de-pessoal-em-ciberseguranca-afeta-70-das-organizacoes/. Acesso em: 02/04/2021

CAIÇARA JUNIOR, Cícero. **Sistemas Integrados de Gestão**: uma abordagem gerencial. 4. ed. Curitiba: Editora Ibpex, 2012.

CANALTECH. **Anonymous cumprem promessa e começam ataques contra Copa do Mundo**. Disponível em: https://canaltech.com.br/hacker/Anonymous-cumprem-promessa-e-comecam-ataques-hackers-contra-Copa-do-Mundo/. Acesso em: 06 de abr. 2021.

CERT.br. **Cartilha da Segurança para Internet**, versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 25 mar. 2021.

CERT.br. **Estatísticas dos Incidentes Reportados ao CERT.br**. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 25 de mar. 2021.

COMPUTERWORLD. **Ciberataques estão em alta na pandemia – e não devem diminuir tão cedo**, 2021. Disponível em: https://computerworld.com.br/seguranca/ciberataques-estao-em-alta-na-pandemia-e-nao-devem-diminuir-tao-cedo/. Acesso em: 24 de mar. 2021.

DANTAS, Marcus Leal. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 155 p.

DEMARTINI, Felipe. Ciberataques crescem 50% durante a migração para home office na pandemia. **Canaltech**, 2021. Disponível em: https://canalte.ch/T7UIP. Acesso em: 26 de mar. 2021.

KASPERSKY. **CIBERAMEAÇA MAPA EM TEMPO REAL**, 2021. Disponível em: https://cybermap.kaspersky.com/pt/stats. Acesso em: 28 de mar. 2021.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. [S. l.: s. n.], 2005. 131 p. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 25 mar. 2021.

MALWAREBYTES. **Tudo sobre hacking**. Disponível em: https://br.malwarebytes.com/hacker/. Acesso em 25 de mar. 2021.

MELO, Ueric. Cibersegurança aplicada à segurança física. **Ciso Adviser**. 2020. Disponível em: https://www.cisoadvisor.com.br/security-room-posts/ciberseguranca-aplicada-a-seguranca-fisica/. Acesso em: 09 de abr. 2021.

MEUSUCESSO. **LGPD abre um novo mercado um ano antes de entrar em vigor**. Disponível em: https://meusucesso.com/noticias/lgpd-abre-novo-mercado-6616/. Acesso em: 03 de abr. 2021.

SOBERS, Rob. 134 Cybersecurity Statistics and Trends for 2021. **Varonis**, 2021. Disponível em: https://www.varonis.com/blog/cybersecurity-statistics/. Acesso em 26 de mar. 2021.

SOPESP. **Cresce a busca por profissionais da área de cibersegurança**, 2020. Disponível em: https://www.sopesp.com.br/2020/05/11/cresce-a-busca-por-profissionais-da-area-de-ciberseguranca/. Acesso em: 26 de mar. 2021.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**, 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 25 de mar. 2021.