Edição 2021: Volume 3, Número 1

"Diálogos interdisciplinares"

Artigo 3: RODRIGUES Jr., Ed Wilson et ali. **Home office e a segurança da informação em tempos de pandemia.**

ED WILSON RODRIGUES Jr.

EDSON RODRIGO LUCIANO NOGUEIRA

GABRIEL FONSECA MENDES

LUCAS AFONSO DA SILVA CAMPOS

HOME OFFICE E A SEGURANÇA DA INFORMAÇÃO EM TEMPOS DE PANDEMIA

Cuiabá/MT

2021

Resumo:

Estamos vivendo em uma época de grandes mudanças, tanto o Brasil como outros países ao redor do mundo todo estão enfrentando a pandemia de coronavírus (COVID-19). Neste cenário, são diversos os desafios, e uma das áreas que mais requerem atenção é a da segurança da informação em home office, pois muitas empresas tiveram que adotar este modelo de trabalho devido ao isolamento social necessário. Portanto, o presente artigo tem como objetivo informar e apresentar práticas que possam auxiliar na manutenção da segurança cibernética no home office, utilizando como metodologia a revisão de literatura.

Palavras-chave: Home office, pandemia, segurança, tecnologia da informação.

ABSTRACT

We are living in a time of great changes, both Brazil and other countries around the world are facing the coronavirus pandemic (COVID-19). In this scenario, there are several challenges, and one of the areas that most require attention is information security in the home office, as many companies have had to adopt this work model due to the necessary social isolation. Therefore, this article aims to inform and present practices that can assist in maintaining cybersecurity in the home office, using the literature review as methodology.

Keywords: Home office, pandemic, security, information technology.

Em suma o home office, trata-se de uma estação de trabalho, na qual os indivíduos realizam suas atividades em casa, mantendo o vínculo empregatício formal com a organização. Sendo assim, com os avanços da tecnologia da informação e comunicação, bem como as modificações da sociedade e novos meios e maneiras de flexibilizar a relação de trabalho, o home office, surge a partir da década de 70. (RAFALSKI e ANDRADE, 2015) e (BARROS e SILVA, 2010)

> Percebe-se, na atualidade, muito em parte pelo advento da globalização, novas configurações sociais, econômicas e tecnológicas, as quais fazem emergir profundas modificações no mundo trabalho. São exemplos dessas modificações a flexibilização da produção, a terceirização da mão de obra, a produção just-in-time, modelos de carreiras com características mais individuais e a maior valorização do capital humano e psicológico no trabalho. (RAFALSKI e ANDRADE, 2015, p. 1)

Desse modo, com a abertura de mercado em países em desenvolvimento para organizações multinacionais e formas de trabalho como o home office, abriram-se oportunidades de internacionalizar e descentralizar as empresas, criando um cenário com diferentes maneiras de trabalhar e se apresentarem como uma realidade do fenômeno trabalho. (RAFALSKI e ANDRADE, 2015).

A melhor definição de informação é um conjunto ou reunião de dados acerca de alguém ou de algo. (MICHAELIS, 2015). Estendendo esse conceito, temos que a informação é a interpretação desses dados.

ISO/IEC 27002 (2013, p. 10) menciona que "organizações de todos os tipos e tamanhos coletam, processam armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal". Tendo em vista esse fato, ao longo dos anos foi tornando-se premente a necessidade de proteger esse ativo.

Segundo a norma ISO/IEC13335-1 (2004), um ativo é "qualquer coisa que tenha valor para a organização". E tudo que detém valor para a organização precisa ser protegido. Ainda segundo a ISO/IEC 27002 (2013, p. 10) "num mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos. "

Um dos significados de segurança é "conjunto das ações e dos recursos utilizados para proteger algo ou alguém. " (PRIBERAM, 2018) ou "condição ou estado do que está livre de danos ou riscos. " (MICHAELIS, 2018).

Segundo ISO/IEC 27002(2013, p. 10) "a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos. "

Antes de explorar a criação e divulgação da política de segurança da informação, é necessário conhecer a tríade tradicional da segurança da informação, seus três pilares CID: Confidencialidade, Integridade e Disponibilidade. (DHILLON E BACKHOUSE, 2001) argumentam que o sigilo das informações depende muito das pessoas que as utilizam.

Para compreender o conceito e necessidade de elaborar uma política de segurança da informação condizente com a organização, é preciso esclarecer alguns conceitos,

Sêmola (2013), destaca que a segurança da informação não é uma ciência exata, ela estaria classificada como gestão de riscos. E para gerir riscos é preciso conjurar vários verbos: conhecer, planejar, agir, auditar, educar, monitorar, aprender e gerenciar são alguns deles.

Neste sentido, com base em Brown e Stallings (2017) segurança da informação é a proteção oferecida para atingir os objetivos apropriados de preservação dos pilares, integridade, disponibilidade e confidencialidade.

A ISO/IEC 27002 (2013, p.14) trata das políticas de segurança da informação e versa sobre o seu objetivo: “prover orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”.

Convém que, no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação. (ISO/IEC 27002, 2013)

Quando construir as políticas de segurança da informação, estas precisam contemplar diversos requisitos, como a estratégia do negócio, as regulamentações, legislação e contratos, ambiente de ameaça da segurança da informação, atual e futuro. (ISO/IEC 27002, 2013)

Todos os termos e conceitos abordados na política devem estar muito bem redigidos e de fácil entendimento, bem como as funções e seus respectivos responsáveis. Controles de segurança precisam ser empregados na organização e viabilizar o atendimento das necessidades de algumas áreas.

A própria ISO/IEC 27002 explana sobre a necessidade de ampla divulgação das políticas de segurança da Informação, tanto para os colaboradores quanto para as partes externas relevantes, visando o amplo entendimento, acessibilidade e relevância a todos que dela depender. A preocupação quanto a divulgação das políticas de segurança para parceiros, fornecedores ou pessoas externas, ocorre, pois, “convém que cuidados sejam tomados para não divulgar informações confidenciais. ” (ISO/IEC 27002, 2013, p.16)

Ao aceitar que é necessário criar e divulgar a política da segurança da informação adequada aos padrões e necessidades da organização o próximo passo é utilizar esta política para reduzir os riscos e as vulnerabilidades do ambiente

O MERCADO BRASILEIRO DA CIBERSEGURANÇA

Segundo um levantamento realizado pela Tempest Security Intelligence, no Brasil, em matéria publicada no site cryptoid.com.br , em mais de 15 segmentos do mercado brasileiro.

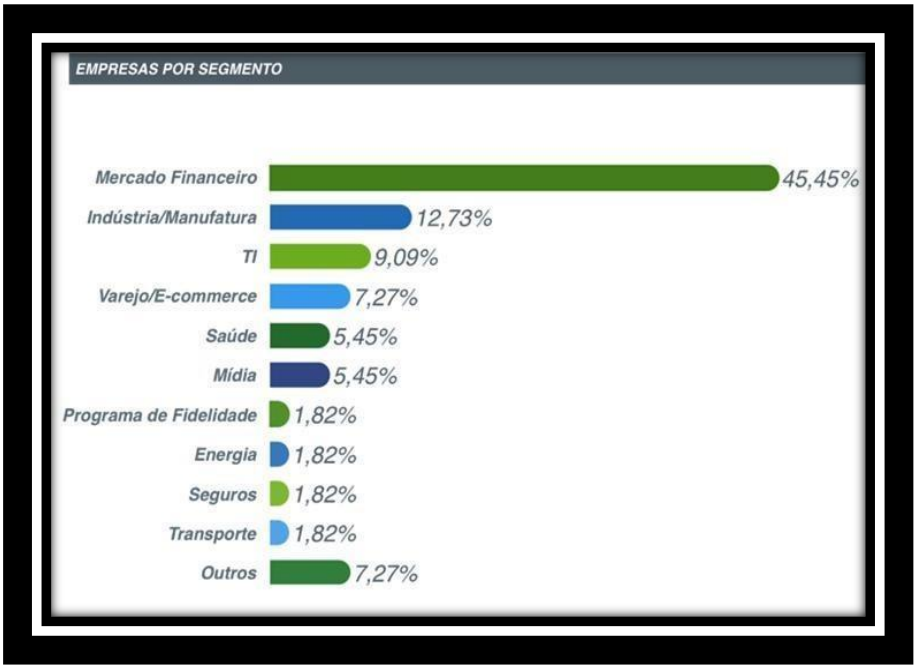

Figura 1 Empresas por segmento

Com as novas regulamentações Lei Geral de Proteção de Dados (LGPD) e General Data Protection Regulation (GDPR – regulamentada pela União Europeia) as empresas têm se importado cada vez mais com a questão da segurança cibernética, mas ainda temos um bom trecho desse caminho a ser percorrido.

Cerca de 3,64% das empresas não possuem recursos/processos de segurança formalizados, 21,82% possuem algum destes, mas sem efetividade real, 30,91% se consideram seguras mesmo estando abaixo das exigências do mercado, 20% possuem processos maduros e investimentos na área e 23,64% seguem o padrão internacional. Assim, cerca de 56,37% das empresas estariam mais ou menos vulneráveis em termos de segurança da informação com níveis de maturidade baixos.

Segundo a pesquisa, mais da metade das empresas declaram que o orçamento anual para segurança da informação representa até 2% do faturamento anual. Destas, 34.5% afirmam que o investimento não ultrapassa 1%. Porém, em 2019, 38,8% das

empresas ouvidas afirmaram a expectativa no incremento dos investimentos em até 20%. Por outro lado, 30,9% afirmam que a variação positiva não deve passar dos 5%.

A Gestão de Riscos está no topo das prioridades de investimentos entre os participantes do estudo. Seguido da Arquitetura de Segurança e Prevenção de Ameaças.

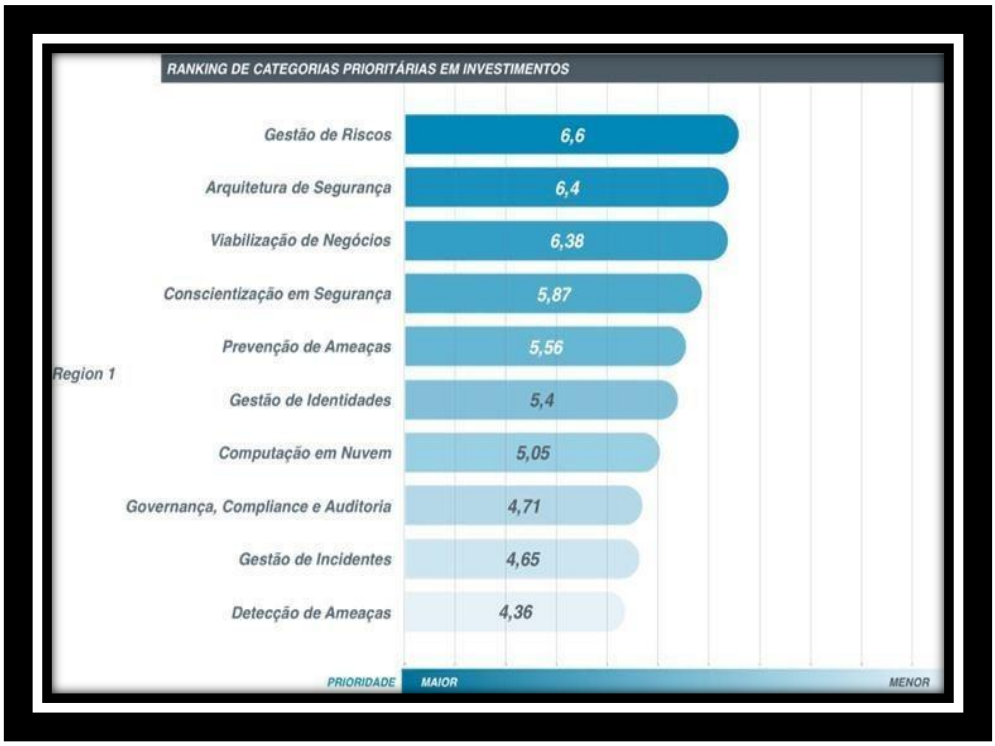

Figura 2 Ranking de categorias prioritárias em investimentos

PRINCIPAIS TENDÊNCIAS PARA SEGURANÇA DA INFORMAÇÃO

Segundo um levantamento realizado pela UPX Technologies, no Brasil, em matéria publicada no site www.securityreport.com.br , com as leis General Data Protection Regulation – GDPR e a Lei Geral de Proteção de Dados Pessoais – LGDP, surge uma nova e urgente demanda no mercado por profissionais especializados: os Chief Information Security Officer – CISOs e os Chief Information Officer – CIOs. Estes deverão planejar e implementar processos e estratégias de segurança de acordo com as normas determinadas pelas leis de proteção de dados. Tecnologias como Machine Learning/IA e Blockchain estão ganhando espaço e se tornando comuns na TI.

De uma forma geral, a questão da segurança da informação abrange um leque amplo de “ofícios” dentro da TI. Processos, requisitos e métodos são considerados, projetados e implementados desde a infraestrutura (redes, servidores, certificados,

firewalls, etc) até a arquitetura de sistemas e os próprios sistemas/aplicativos, do nível da comunicação dos dados até a programação do código-fonte.

Segundo dados da Fortinet - empresa de segurança digital - apresentou que o Brasil sofreu quase 1,7 bilhões de ataques em todo o país, os dados foram catalogados até o fim do primeiro semestre deste ano. A pesquisa aponta que só no início do ano, houve um acréscimo de 18,2% em comparação com o resultado do último semestre de 2019 (1,361,958,857, bilhões de ataque catalogados), após o surto de Covid-19, contabilizando um total de 1,610,527,908 bilhões de ataques subsequentes. Dentre eles, os que levaram título de destaque foram:

- Ataques de Backdoor.DoublePulsar: 420,840,269 de ataques.
- SSL.Anonymous.Ciphers.Negotiation: 260,991,120 de ataques.
- MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure: 218,696,701 de ataques.
- Andromeda.Botnet: 6,986,586 de ataques.
- Zeroaccess.Botnet: 1,532,692 de ataques.
- Conficker.Botnet: 1,127,941 de ataques.

Esses dados podem ser comparados com os gráficos logo abaixo:

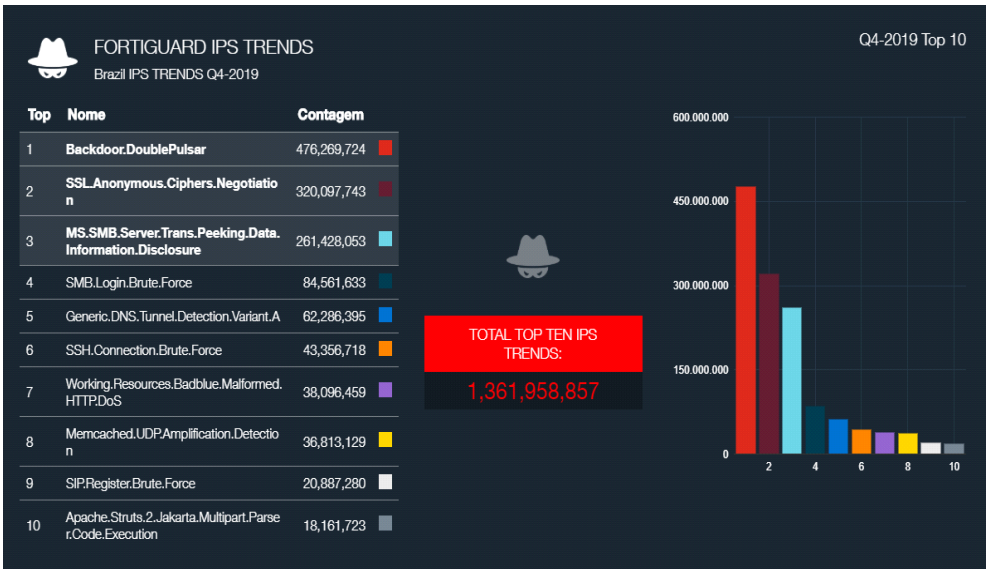

Figura 3 Fortnet 2019

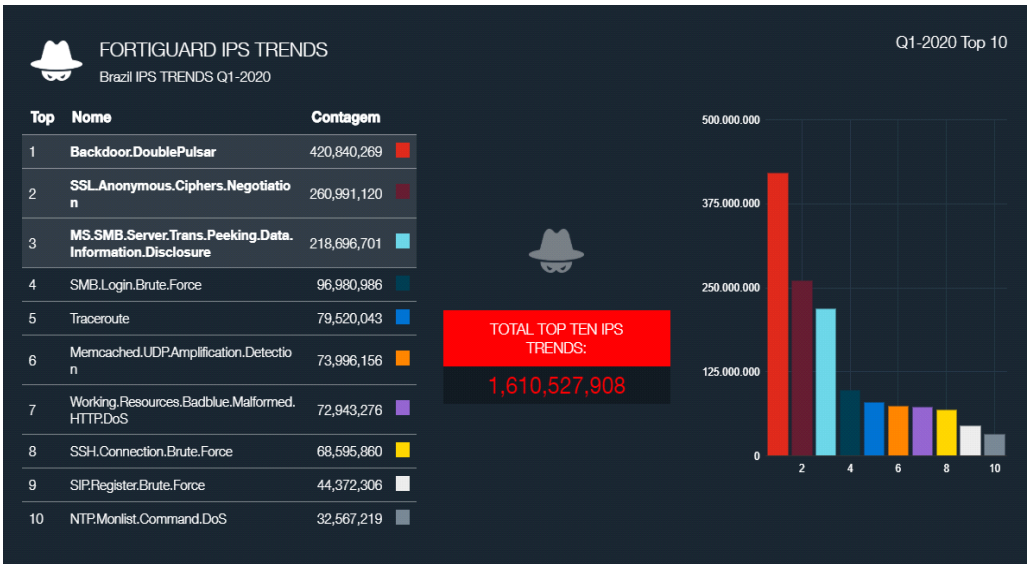

Figura 4 Fortnet 2020

Em contrapartida, o site senado.leg.br aponta que o país ocupou a 70º colocação no índice de segurança cibernética da União Internacional de Telecomunicações (ITU), órgão pertencente a Organização das Nações Unidas (ONU) até o fim do ano de 2019. Segundo o site, o resultado apontou que os prejuízos ultrapassaram mais de R$ 80 bilhões. Os dados apresentam a fragilidade e carência em segurança digital como um todo no País. (Agência Senado, 2019).

Compreendendo estas questões, Jerussalmy (2020) destaca que mesmo com as empresas adotando métricas e medidas de proteção, o ambiente de rede caseira, bem como o uso de notebooks deixa informações das organizações mais vulneráveis, por diversos motivos como necessidade de bloqueio do dispositivo que é utilizado, não utilização de impressões de dados da empresa, entre outros.

Rodrigues (2020), destaca que com a pandemia COVID-19 empresas de vários segmentos de diversas partes do mundo têm adotado o home office como modelo de trabalho, porém é necessário realizar este processo de maneira segura para o ponto de vista empresarial.

Compreendendo isto, muitas empresas têm suas primeiras experiências neste modo de trabalho agora, em um cenário cheio de desafios e modelos diferentes, um fato deste são dados expressos por Rodrigues (2020), que demonstram a falta de computadores para aluguel, bem como inexperiência por parte das empresas de sistemas práticos para criação de políticas de segurança digital para a aplicação de modo remoto.

Desse modo, estão sendo tomadas várias medidas, dentre elas, a essencial é a utilização de VPN (Virtual Private Network) a qual é uma das medidas fundamentais para as operações da empresa neste novo cenário. Pelo fato de impactar e influenciar em questões relacionadas com a segurança e disponibilidade segura das informações. (RODRIGUES, 2020)

Além deste fator é essencial uma equipe de TI (tecnologia da Informação), com foco de executar um trabalho para garantir toda a funcionalidade e efetividade destes sistemas, sendo assim sua preparação para utilização do mais diversos recursos e ferramentas que são oferecidas pelas plataformas. (RODRIGUES, 2020).

Outros fatores que estão ligados à segurança da informação e previnem invasões ou vulnerabilidades que um trabalho em home office são:

O uso de diferentes credenciais que vem com a utilização de laptops para finalidades diferentes (pessoal e trabalho), deve ser observado com atenção sendo necessário logins distintos com o objetivo de proporcionar maior segurança às informações da empresa e divisão do trabalho e aspectos pessoais.

A utilização de um antivírus, é extremamente necessária, principalmente em computadores aos quais são de uso pessoal e são utilizados para trabalho a fim de proteger as informações contidas nele.

Evitar o uso de pendrives e HD´s externos, sendo um meio de proteger o meio utilizado de trabalho, uma vez que os mesmos podem ser porta de entrada de infecções e devem ser evitados. A precaução é a mesma adotada normalmente dentro de empresas: mesmo que a rede esteja segura, é difícil se proteger de um malware que tem acesso direto ao computador da vítima por meio da entrada USB. Antivírus com monitoramento ativo podem ajudar a bloquear eventuais ameaças, mas não usar esse tipo de disco é sempre mais adequado para se manter mais seguro. (ALVES, 2020).

Indubitavelmente, vale informar que é de grande relevância a atualização de programas, utilização de softwares originais, bem como, definição de um perfil de admirador e cuidados com a manutenção, são de suma importância para evitar e prevenir possíveis invasões nos computadores. Nesse sentido, vale ressaltar a importância de um conceito de segurança cibernética que cada vez mais vem sendo difundido, o Zero Trust.

A definição de Zero Trust ou uma arquitetura deste tipo, parte do princípio de que ninguém é considerado confiável, adotando assim uma postura de sempre estar fazendo verificações com o intuito de encontrar possíveis ameaças. George (2019), destaca 3 pilares que compõem a base de uma arquitetura Zero Trust, são eles:

- ✓ Garantir o acesso de forma segura aos recursos da empresa, independentemente da localização.
- ✓ Aplicar medidas de segurança nas quais existam menos privilégios e um maior controle de acesso.
- ✓ Inspecionar e registrar todo o tráfego, até quando o mesmo for de origem de uma rede local de computadores (LAN).

Em síntese, é de deveras importância precavermos mantendo o sistema operacional atualizado e os softwares que o compõem serem baixados diretamente do site oficial, evitando abrir e-mails desconhecidos e acessar páginas que não possuem o prefixo do código "https://", que além de sinalizar que o site é protegido contra a ataques de Spoofing – falsificação de identidade na rede – e Cross-site Scripting – ataque de injeção de código malicioso -, serve de grande auxílio para manter os dados de navegação segura contra outros tipos de códigos maliciosos e ataques subsequentes com o uso de criptografia que é implementado no protocolo do mesmo.

Entretanto todo o cuidado é pouco e o uso de filtro de spams e precaução em acesso à redes públicas são ferramentas essenciais. Além disso, vale ressaltar que é de grande valia manter o uso constante de backups do sistema em dia mantendo-o seguro de ataques de criptografia de dados, trojans, rootkits e derivados, certificar-se de que as portas do firewall do computador estão devidamente fechadas e as senhas dos e-mails e demais redes sociais estão atualizadas.

Por conseguinte, como consequência ou efeito do que foi anteriormente mencionado, além de precavermos de possíveis vetores, todo o cuidado se torna pouco para que seja mantido com eficiência a segurança em casa durante jornadas de trabalho home office em tempos caóticos de pandemia.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. – **NBR ISO/IEC 27002: Tecnologia da informação –Técnicas de segurança – Código de prática para controles de segurança da informação**. Rio de Janeiro:2013. 2ª Edição.

ABNT-ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro: 2013.2ª Edição.

AGÊNCIA SENADO - **Brasil é 2º no mundo em perdas por ataques cibernéticos, aponta audiência**. Disponível em: <

https://www12.senado.leg.br/noticias/materias/2019/09/05/brasil-e-2o-no-mundo-em-perdas-por-ataques-ciberneticos-aponta-audiencia>. Acesso em: 28 de maio de 2020.

ALVES, P. **Dicas para trabalhar em home office: saiba proteger informações importantes.** techtudo, 2020. Disponível em: <https://www.techtudo.com.br/listas/2020/03/dicas-para-home-office-saiba-proteger-informacoes-importantes-do-trabalho.ghtml>. Acesso em: 25 de maio de 2020.

BARROS, A. M.; SILVA, J. R. G. D. **Percepções dos indivíduos sobre as consequências do teletrabalho na configuração home-office: estudo de caso na Shell Brasil.** scielo, 2010. Disponível em: <https://www.scielo.br/pdf/cebape/v8n1/a05v8n1.pdf>. Acesso em: 25 de maio de 2020.

BROWN, Lawrie e STARLLINGS, Willia. **Segurança de Computadores: Princípios e Práticas.** Rio de Janeiro: Elsevier, 2017. 2ª Edição.

Cryptoid. **Cibersegurança destaques notícias pesquisas e estudos proteção de dados.** Disponível em: <https://cryptoid.com.br/pesquisas-seguranca-da-informacao-e-ciberseguranca/tempest-apresenta-primeiro-estudo-do-mercado-brasileiro-de-ciberseguranca/>. Acesso em 27 de maio de 2020.

DHILLON, GURPREET & BACKHOUSE, James. (2001). **Current directions in IS security research: Towards socioorganizational perspectives. Information Systems Journal.** 11. 10.1046/j.1365-2575.2001.00099.x.

FORTINET. **THREAT INTELLIGENCE INSIDER 2019**. Disponível em:<https://www.fortinetthreatinsiderlat.com/pt/Q4-2019/BR/html/trends?fbclid=IwAR2uQztnfgMn3lnAPGfEokPQX8FEnGX1Lf6hfmIe9JFb5yjT2qSZ9m6OoBQ#trends_position>. Acesso em: 28 de maio de 2020

FORTINET. **THREAT INTELLIGENCE INSIDER 2020**. Disponível em: https://www.fortinetthreatinsiderlat.com/pt/Q1-2020/BR/html/trends?fbclid=IwAR2uQztnfgMn3lnAPGfEokPQX8FEnGX1Lf6hfmIe9JFb5yjT2qSZ9m6OoBQ#trends_position. Acesso em: 28 de maio de 2020.

GEORGE, T. **The (Re-)Emergence of Zero Trust. security week,** 2019. Disponível em: <https://www.securityweek.com/re-emergence-zero-trust>. Acesso em: 27 de maio de 2020.

ISO/IEC 13335-1:2004. **Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management.**

JERUSSALMY, E. **Confira cuidados no home office com a segurança da informação. revista Brasil**, 2020. Disponível em: <https://radios.ebc.com.br/revista-brasil/2020/03/confira-cuidados-no-home-office-com-seguranca-da-informacao>. Acesso em: 26 de maio de 2020.

MICHAELIS. **Michaelis Dicionário Brasileiro da Língua Portuguesa.** 2015. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/seguran%C3%A7a/ - Consultado em 27 de maio de 2020.

PRIBERAM. **Dicionário Priberam da Língua Portuguesa.** 2008-2013. Disponível em: http://www.priberam.pt/dlpo/chave - Consultado em 27 de maio de 2020.

RAFALSKI, J. C.; ANDRADE, A. L. D. **Home-Office: Aspectos Exploratórios do Trabalho a partir de Casa**. **pepsic**, 2015. Disponível em: <http://pepsic.bvsalud.org/pdf/tp/v23n2/v23n2a13.pdf>. Acesso em: 26 de maio de 2020.

RODRIGUES, A. Home office e a segurança de rede das empresas. **securityinformationnews**, 2020. Disponível em: <https://securityinformationnews.com/2020/04/21/home-office-e-a-seguranca-de-rede-das-empresas/>. Acesso em: 26 de maio de 2020.

SecurityReport. **Principais tendências para Segurança da Informação em 2019**. Disponível em: <http://www.securityreport.com.br/overview/principais-tendencias-para-seguranca-da-informacao-em-2019/#.XS23NPxRdhE>. Acesso em 27 de maio de 2020.

SÊMOLA, Marcos. **Gestão da Segurança da Informação. Uma Visão Executiva**. Rio de Janeiro: Elsevier, 2014 . 2ª Edição.

TELTEC SOLUTIONS. **O que é uma arquitetura Zero Trust? Entenda o modelo de cibersegurança. teltec solutions,** 2019. Disponível em: <https://teltecsolutions.com.br/mundo/arquitetura-zero-trust>. Acesso em: 27 de maio de 2020.