**Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"**

**Curso Superior de Tecnologia em Segurança da Informação**

# Impactos da Pandemia de COVID-19 na Segurança da Informação para as empresas e pessoas

**Martinelli Junior, Walter Luiz; Lahr Giraldi, Marcus Vinícius.**

wmartinelli95@gmail.com, marcus.lahr@fatec.sp.gov.br

***Abstract.*** *This paper discusses the Covid-19 pandemic, under the cyber-security approach, for both enterprises and people. It briefly addresses statistics about the ongoing pandemic during 2020, explores the definition and ambience of digital transformation and how both phenomena are related. It analyzes the impacts caused by the pandemic towards information security in corporate environments, listing some threats that have become evident and countermeasures that can be adopted aiming to maintain the privacy, integrity, and confidentiality of personal and corporate data. Finally, the study exposes a real scenario of technological- and business-level changes made by a retailer company in São Paulo state.*

***Resumo.*** *Este artigo aborda a pandemia de Covid-19 a partir do ponto de vista da segurança da informação, tanto para empresas como para pessoas. Aborda brevemente estatísticas sobre a pandemia em curso durante 2020, explora a definição e ambientação da transformação digital e como ambos os fenômenos se relacionam. Analisa os impactos que a pandemia trouxe para a segurança da informação em ambientes corporativos, enumerando algumas ameaças que se evidenciaram e contramedidas que podem ser adotadas visando a privacidade, integridade e confidencialidade dos dados pessoais e corporativos. Por fim, analisa um cenário real de adaptações realizadas a níveis tecnológicos e de negócios em uma companhia de varejo no interior do estado de São Paulo.*

## 1. Introdução

A transformação digital pela qual a sociedade atualmente está passando é, em grande parte, um processo natural do amadurecimento das empresas e da forma como estas fazem negócios, tendo em vista o uso cada vez mais amplo de equipamentos digitais para processamento de informações. Entretanto, eventos externos podem ser fatores motivadores de mudança, incluindo mudanças profundas, na forma como as empresas

desempenham suas atividades e se relacionam com seus clientes. Indubitavelmente, o fator motivador mais evidente no ano de 2020 é a pandemia de Covid-19.

Covid-19 é, conforme declara a Organização Mundial da Saúde (do inglês *World Health Organization*, ou WHO), a doença causada pelo vírus denominado SARS-CoV-2, sendo identificada pela primeira vez na cidade de Wuhan, na China, em dezembro de 2019. Seus principais sintomas incluem febre, tosse seca, fadiga, inflamações em vias respiratórias e dificuldade para respirar. Em casos mais graves, as complicações respiratórias podem levar a óbito.

Ainda segundo a WHO (2020), cerca de 80% das pessoas que contraem a doença se recuperam sem a necessidade de tratamento hospitalar. Os 20% restantes podem requerer oxigenação artificial em decorrência da apresentação de sintomas mais graves, sendo que aproximadamente 5% do total podem ficar "severamente doentes"[1] e precisar de cuidados intensivos. Até a data de 23 de novembro de 2020, os números oficiais da WHO indicam aproximadamente 58 milhões de infectados no mundo todo, com um total de 1,38 milhão de vidas perdidas em decorrência da doença. Conforme a Organização relata ainda, o contágio ocorre por contato de mucosas (olhos, nariz, boca) com o vírus, de modo que se torna fundamental, como uma das formas mais eficientes de controlar sua disseminação, adotar medidas de distanciamento social e evitar locais com aglomerações. Outras medidas preventivas incluem o uso de máscaras cobrindo nariz e boca, higienização efetiva e regular das mãos com água e sabão e uso de álcool para higienização de mãos, objetos e superfícies.

É a partir desta recomendação de distanciamento social e do cenário de incerteza impostos pela pandemia em curso que este artigo foi elaborado. Seu principal objetivo é demonstrar de que formas a pandemia de COVID-19 impactou empresas no que diz respeito à aceleração da transformação digital e do ponto de vista da Segurança da Informação. Tal objetivo é motivado pelas mudanças sociais profundas causadas pelo cenário pandêmico e suas implicações na TI, hoje parte fundamental das operações de empresas de praticamente qualquer setor econômico.

Posto isso então, o artigo está estruturado conforme segue. A seção 2 explana o que é transformação digital e como a pandemia se relaciona com isso. A seção 3 analisa impactos corporativos no que tange à Segurança da Informação. A seção 4 faz recomendações de melhores práticas e contramedidas sobre como prevenir, detectar e responder a ameaças cibernéticas que se aproveitam do atual momento de fragilidade humana. A seção 5 traz um breve estudo de caso de uma rede de varejo, que precisou revisitar alguns de seus processos frente à pandemia. E a 6ª e última seção sumariza os pontos abordados.

## 2. O que é transformação digital

Com o cenário de distanciamento social imposto pela pandemia de Covid-19, a transformação digital que já estava em curso na sociedade foi acelerada profundamente. Para entender este processo, entretanto, cabe ressaltar primeiramente o que é a transformação digital e, principalmente, o que não é transformação digital. Após isso, pode-se estabelecer uma relação entre este conceito e a forma como empresas estão estabelecendo novos processos e fluxos de trabalho (ou mesmo revisitando e aprimorando

[1] "*Critically ill"*, traduzido pelo autor.

processos existentes) e o impacto disso na relação com seus funcionários, parceiros de negócios clientes.

Para começar a definir o que é transformação digital, deve-se primeiro definir o que *não é* transformação digital. Apesar de parecer contraintuitivo, essa abordagem é segura porque analisa a forma como, normalmente, as empresas lidam com seus dois ativos mais preciosos: clientes e informações. Partindo deste pressuposto, não há ninguém melhor para fornecer uma visão ampla e profunda deste assunto do que uma das maiores empresas de softwares voltados para Gerenciamento de Relacionamento com Clientes (CRM[2]). Conforme destaca a Salesforce (2020) as empresas até pouco tempo atrás armazenavam as informações relativas a suas operações e seus contatos com clientes e parceiros de negócios em papel. Tecnologia relativamente eficiente, barata e simples, o papel manteve-se como principal forma de arquivar informações, porém apresentava uma limitação grande, quando se tratava de compartilhamento destas informações. Desta forma, eram usadas copiadoras, faxes e outros meios de transmissão destes dados.

Os computadores, no entanto, se popularizaram e, com o passar do tempo, as empresas começaram a armazenar nestes mesmos computadores os dados que antes eram armazenados em papel. Basicamente, este foi um processo de *digitização*[3], que é, conforme continua a Salesforce, "o processo de converter informação analógica em digital". Este processo, apesar de trazer um aumento de produtividade, tinha um problema: as informações digitais eram usadas, basicamente, de uma forma extremamente similar (ou até da mesma forma) que suas contrapartes analógicas. Pior, como continua a companhia, "sistemas e processos corporativos ainda eram predominantemente desenhados em torno de ideias analógicas sobre como encontrar, compartilhar e usar informações" (2020).

A necessidade de simplificação destes processos de trabalho levou as empresas a uma outra etapa de sua caminhada evolutiva, desta vez, utilizando informações já em sua forma digital para tornar seu trabalho mais simples e eficiente. A este processo, dá-se o nome de *digitalização*[4]. Desta forma, não existe uma revolução nos negócios, ou mesmo a criação de novos tipos de negócios; ao invés disso, apenas usa-se a tecnologia para fazer as coisas do jeito antigo, porém de forma mais rápida. Um exemplo dado pela própria Salesforce consiste no uso de um CRM para atendimento a requisições de clientes. Em vez de pesquisar em pilhas de papeis procurando por informações relevantes ou preenchendo formulários, pode-se fazer isso inserindo e consultando informações em um sistema informatizado. Neste cenário, o processo básico de atendimento ao cliente (onde o cliente reporta um problema a um agente da empresa prestadora do produto ou serviço e a empresa analisa as informações necessárias para atender à reclamação do cliente) permanece o mesmo de como sempre foi, com a diferença de ser mais rápido unicamente devido à plataforma onde as informações são registradas e consultadas.

Conforme destaca Marc Benioff, CEO[5] da Salesforce, "toda transformação digital começa e termina com o cliente" (2020). E, a partir deste ponto, as empresas começaram a perceber que muitas vezes é possível (e até mesmo necessário) oferecer serviços melhores e cada vez mais personalizados para seus clientes, de modo a se manter relevantes para estes. Assim, a transformação digital não é o processo de usar tecnologias

[2] Do original "*Customer Relationship Management*", traduzido pelo autor.
[3] Do original "*digitization*", traduzido pelo autor.
[4] Do original "*digitalization*", traduzido pelo autor.
[5] *Chief Executive Officer*, ou Diretor Executivo de uma empresa

novas para acelerar processos velhos, e sim, usar tecnologias (muitas vezes) já existentes (e, onde necessário, desenvolver novas tecnologias) para entregar *valor* para o cliente, por meio de produtos e serviços novos e que os clientes realmente *queiram* ou dos quais *precisem*. Conforme um estudo realizado em 2012 pela Accenture, empresa que desenvolve tecnologias de inteligência artificial para análises mercadológicas, 73% dos consumidores preferem comprar de marcas que usam informações pessoais, como hábitos de consumo, para oferecer experiências de compras mais relevantes.

Um exemplo utilizado pela Salesforce nesse ponto é o de que muitas empresas estão usando redes sociais (tecnologia existente) como plataformas de atendimento ao cliente (finalidade nova). Redes sociais não foram criadas para atendimento ao cliente, mas é lá que eles estão e, em muitos casos, é onde é mais fácil *para os clientes* buscarem informações sobre problemas que estão enfrentando com algum produto ou serviço. Pode-se citar, neste caso, a KLM, companha aérea holandesa. Durante uma erupção vulcânica na Islândia que impactou o espaço aéreo europeu, em 2011, a empresa começou a usar o Twitter como forma de relacionamento com os clientes, tendo em vista o fluxo anormalmente alto de demanda de suas plataformas de *call-center*. Após a normalização do problema, a empresa abandonou esta forma de relacionamento com o cliente por aproximadamente 6 meses, até que o CEO da companhia questionou o motivo de tal abandono, uma vez que tal experiência agregou tanto valor à companhia. Desde então, o Twitter tem feito parte de uma estrutura ainda maior de atendimento ao cliente na KLM, que conta ainda com equipes multidisciplinares e multilinguísticas com atendimento 24/7. Isso permitiu, segundo Viktor van der Wijk, Diretor de Marketing Digital da companhia, que a empresa "responda mais rapidamente às requisições dos clientes, redirecione-os para outros meios de viajar e proteja a imagem corporativa da KLM" (2020)[6].

### 2.1. Rupturas Agudas e Crônicas e suas semelhanças

De acordo com a consultoria Deloitte, transformações digitais podem ser comparadas a situações médicas, podendo ser agudas ou crônicas. Da mesma forma que procedimentos médicos para soluções rápidas de problemas agudos (como uma dose cavalar epinefrina ministrada durante uma parada cardíaca) podem ajudar a estabilizar um paciente e reduzir a severidade de sua condição imediata mas não são indicados para tratamentos a longo prazo, algumas medidas adotadas de maneira emergencial pelas empresas durante o começo da pandemia de Covid-19 ajudaram a estabilizar sua situação em um primeiro momento, porém devem ser revistas e ajustadas conforme este cenário, inicialmente agudo, se transforma em um cenário mais permanente e crônico.

Alguns fatores, entretanto, são comuns a ambos os cenários de ruptura, independentemente de serem agudos ou crônicos. O primeiro deles é a agilidade e o trabalho em equipes multidisciplinares, que é muito mais evidente em companhias com maior grau de maturidade digital (KANE, et al; 2020). Kane ressalta ainda que, em companhias com este perfil, "é mais provável de se ver equipes multidisciplinares e [...] é menos provável que processos e estruturas de gerenciamento interfiram na sua capacidade de trabalhar digitalmente". Adicionalmente, organizações com este perfil normalmente concedem a seus funcionários uma maior autonomia na tomada de decisão. Um benefício disso é que empregados de níveis hierárquicos mais baixos estão assumindo

[6] "*[...] respond more quickly to customer inquiries, re-direct them to other means of travel, and protect the KLM brand image*", traduzido pelo autor.

responsabilidades que, de outra forma, não assumiriam; em última análise, isso permite que a companhia como um todo seja mais ágil.

Kane et al (2020) destaca uma segunda característica importante: aprendizado contínuo. Isso pode ser dividido em duas frentes: como funcionários e como companhias. Como funcionários, o aprendizado normalmente se dá pela necessidade de adaptação a novos desafios e circunstâncias, fazendo com que muitos aprendam no trabalho. Já no caso de companhias, o cenário de reinvenção (ainda que forçada) de partes de seus negócios faz com que muitas empresas aprendam através de experimentação em novos cenários. Em alguns casos, conforme destaca Mark Onisk, CCO da Skillsoft (empresa de capacitação online), o "aprendizado corporativo está se tornando parte da cola que mantém juntos os elementos sociais da companhia enquanto os empregados trabalham remotamente" (2020).

Por fim, Kane et al (2020) enumeram um terceiro ponto de semelhança como sendo a habilidade dos líderes em comunicar claramente uma visão estratégica para a companhia. Este ponto relaciona-se com o primeiro no sentido de que, conforme a consultoria Deloitte (2020) destaca em seu relatório *The kinetic leader: Boldly reinventing the enterprise*, em uma entrevista com mais de 1300 líderes executivos ao redor do mundo, 69% dos entrevistados afirmaram acreditar que o líder tecnológico do futuro "precisa ser orientado a mudanças, ter visão (de negócios), ser ágil e instigar inovação"[7]. Cabe ressaltar que ter e comunicar claramente uma forte visão estratégica para a companhia como um todo no meio de qualquer mudança, aguda ou crônica, ajuda os funcionários a saberem como reagir quando rupturas tecnológicas causam mudanças no ambiente.

### 2.2. Rupturas Agudas e Crônicas e suas diferenças

Apesar das similaridades apontadas por Kane et al (2020), os autores afirmam ainda que existem diferenças entre os dois tipos de cenários. Conforme será abordado mais adiante neste artigo, apesar de todos os impactos financeiramente negativos e da perda de vidas, a pandemia de Covid-19 tem causado a aceleração de mudanças digitais que, em alguns casos, estavam atrasadas a um bom tempo. A seguir, serão analisadas 3 diferenças citadas por Kane et al.

A primeira destas diferenças é o que Jeffrey Pfeffer e Robbert Sutton chamaram, em seu livro homônimo, de espaço entre saber e fazer (2000).[8] Conforme um estudo conduzido pela Deloitte (2020) durante a elaboração do livro *The Technology Fallacy* (publicado inicialmente a menos de 2 anos, em março de 2019), 87% dos entrevistados sabem que, em algum momento, seu segmento econômico será impactado em nível moderado a profundo por tecnologias digitais. Entretanto, apenas 44% dos entrevistados sentem que suas companhias estão fazendo o que consideram como suficiente para acompanhar tal ruptura. Um exemplo de como mudanças precisaram ser feitas rapidamente foi a emissão de toques de recolher por parte de alguns governos. Neste cenário onde as pessoas não poderiam mais sair na rua, organizações que já tinham uma cultura de trabalho remoto estabelecida tiveram uma vantagem competitiva tanto em termos tecnológicos (por já terem uma infraestrutura preparada para tal modalidade) como a nível de processos de negócio (por já terem processos bem definidos e políticas

[7] "*[...] future tech leaders need to be change-oriented, have a vision, be agile and be innovative*", traduzido pelo autor.
[8] *The Knowing-Doing Gap*, traduzido pelo autor.

de segurança para o teletrabalho). Já empresas que apenas flertavam com a ideia de implementar novos métodos de trabalho, como o *home office*, na teoria *sabiam* o que precisava ser feito, porém não haviam tido a *iniciativa* de colocar tal ideia em prática.

O segundo ponto abordado pelos autores é que cenários de ruptura aguda fazem com que empresas estejam mais dispostas a assumir riscos que, de outras formas, não o fariam. Conforme uma pesquisa realizada em junho de 2020 (LAMBERT, 2020) pela revista Fortune em parceria com a consultoria Deloitte, que contou com a participação de mais de 220 CEOs, 77% dos entrevistados disseram que "a transformação digital de suas companhias foi *significativamente acelerada* durante a crise"[9]. Adicionalmente, 40% dos entrevistados disseram que já estão gastando mais com infraestrutura e plataformas de TI, motivado em grande parte pela adoção de teletrabalho e outras modalidades de interação totalmente digital com clientes e parceiros de negócios. Desta forma, percebe-se que o cenário de ruptura aguda, trazido pela pandemia em curso, fez com que muitas empresas se mostrassem dispostas a tentar coisas novas sem necessariamente estarem certas do resultado. Esta capacidade de adaptação serve como um indicativo de saúde organizacional e, durante tempos de mudanças rápidas, pode ajudar a construir um ambiente corporativo de sucesso.

Por fim, a terceira e última faceta abordada por Kane et al (2020) diz respeito ao planejamento estratégico de longo prazo, bem como a liderança em tempos de incerteza. Ressalta-se que no que tange ao planejamento estratégico de longo prazo, deve-se considerar não apenas um cenário, mas, conforme a consultoria Deloitte (2020) ressalta, fazer planos para o que for possível dentre um número de cenários futuros possíveis. Certamente não seria possível imaginar um cenário exato de tantas incertezas como uma pandemia, porém, exercícios de treinamento referente ao planejamento que tenham sido realizados podem ajudar a enfrentar este tipo de desafio. Em um cenário de incerteza, gerentes e executivos devem desenvolver planos que englobem múltiplos futuros possíveis, e, quando for necessário decidir as iniciativas a ser usadas, escolher aquelas que serão mais relevantes para múltiplos cenários futuros.

É neste cenário de incerteza que as empresas (e, consequentemente seus clientes e seus funcionários, ou seja, *pessoas*) estão hoje inseridas, com impactos diretos relativos à Segurança da Informação. Estes impactos serão abordados na próxima seção.

## 3. COVID-19 e a Segurança da Informação nas empresas

Com a disseminação da Covid-19 pelo mundo e um cenário onde a maioria das empresas se viu forçada a mudar as operações para um modelo de teletrabalho, novos desafios surgiram quase que da noite para o dia. O principal destes pode ser resumido em uma pergunta: como migrar toda ou a maioria das operações para fora da empresa com segurança e de maneira transparente para o cliente e os funcionários?

Dito de maneira simples, não existe uma resposta direta e objetiva para a pergunta acima. O primeiro passo foi realocar os trabalhadores de forma remota. Para tanto, recursos financeiros destinados a outros fins foram realocados para garantir que a infraestrutura necessária fosse instalada ou ampliada (ANAT; CASO; SCHWARZ, 2020). Um dos principais recursos tecnológicos empregados para este fim foi o uso de

[9] "*[...] 77% of the CEOs say their company's digital transformation was* significantly accelerated *during the crisis*", traduzido pelo autor.

redes virtuais privadas (VPNs), que permitem que trabalhadores em qualquer localidade do mundo acessem a rede corporativa. Isso apresenta riscos, especialmente se for usado um computador pessoal em vez de um dispositivo corporativo para esta tarefa. Adicionalmente, concentradores de VPN experimentaram uma carga de trabalho nunca imaginada, com empresas beirando os 100% do seu contingente de operações trabalhando de forma remota. O segundo desafio que pode ser enumerado é sobre como manter todo o ambiente operando de forma eficiente sem torná-lo indisponível devido à demanda elevada.

Para empresas que já possuíam, antes da pandemia, políticas de teletrabalho, o chamado *home office*, os desafios foram superados de forma mais suave, sendo necessário alguns ajustes finos e adaptações de processos muitas vezes já existentes. Para empresas sem estrutura para tanto ou sem a cultura desta modalidade, os desafios foram maiores. Foi necessário mapear processos corporativos e fluxos de informação, planejar, adquirir e implementar toda a infraestrutura necessária para trabalho remoto e treinar os usuários para esta nova modalidade de trabalho. Como se não bastasse, esse é o cenário ideal, onde nenhum detalhe operacional foi deixado de lado ou esquecido devido ao pouco tempo, pressão e criticidade das alterações realizadas; em qualquer cenário diferente do ideal, tem-se tempo perdido, funcionários parados, processos interrompidos ou até mesmo retrabalho.

A partir do ponto em que toda a infraestrutura foi adequada para trabalho, começam a surgir outros desafios. O primeiro deles é que, em muitos casos, os Planos de Resposta a Incidentes (PRI) ou de Continuidade de Negócios (PCN) da maioria das empresas simplesmente não incluem um cenário de pandemia, de forma que precisaram ser revistos. E, mesmo nos casos em que um cenário similar era considerado, pode ser que, conforme salienta Tope Aladenusi (2020), tais planos não envolvessem corretamente a dimensão do impacto de um evento deste porte, e, consequentemente, precisem ser revisitados para incluir cenários de pandemia, que afetam vários países e elementos críticos de cadeias de suprimento ao mesmo tempo (2020).

Algo digno de nota também no decorrer da pandemia é um cenário global de incerteza econômica. Diante deste cenário, buscas por termos como *coronavirus*, *vaccine*, *Wuhan*, *SARS* e *pandemics*, tiveram sua popularidade absurdamente elevada em motores de busca, como o Google desde janeiro de 2020, alcançando o pico entre os meses de março a maio deste ano. Tal comportamento é um forte indicativo de que, conforme ressaltam os pesquisadores Olajide Adebola e Kenneth Okereafor (2020), o mundo está ansioso por informações sobre esta nova doença, formas de impedir sua disseminação e até mesmo por uma vacina. Ainda segundo os pesquisadores, durante este momento, cyber-criminosos estão "se aproveitando do desespero e medo das pessoas para vender produtos inexistentes, disseminar rumores sem embasamentos e notícias falsas e, no processo, roubar valiosas informações confidenciais usando, para tanto, vários softwares maliciosos" (ADEBOLA, Olajide; OKEREAFOR, Kennet, 2020 p. 3)[10].

Sumarizando, conforme destacam Adebola e Okereafor (2020), bem como Aladenusi (da Deloitte) (2020) e Steve Bates (da KPMG) (2020), algumas das formas que os criminosos virtuais encontraram para agir durante este período são as seguintes:

[10] "*[...] cybercriminals are taking advantage of people's desperation and fear to sell non-existing products, disseminate unsubstantiated claims and fake news and in the process steal valuable confidential data using various malicious software (*malware*) to package their arsenal*", traduzido pelo autor.

1. E-mails falsos ou forjados (*spam*) com informações desencontradas ou ilegítimas sobre Covid-19, usados para gerar pânico. Usando o Google Trends, que mede a popularidade de termos pesquisados no buscador da companhia, o termo teve um aumento de popularidade, não ficando abaixo de 75 (numa escala de 0 a 100) desde a primeira quinzena de janeiro.
2. Ataques conhecidos como Fraude do CEO, que consiste em uma tentativa de golpe onde o atacante se passa por algum executivo ou funcionário de alto escalão de uma companhia querendo transferir fundos corporativos para outras contas bancárias. Este tipo de ataque lida com o senso de urgência que solicitações de pessoas em posições de liderança normalmente possuem, e o atual cenário de distanciamento social pode aumentar a fragilidade que ele explora.
3. Aumento no número de criminosos cibernéticos, devido à maior quantidade de pessoas desempregadas, ou que estão procurando alguma forma de ganhar dinheiro com o cenário adverso imposto pela pandemia.
4. E-mails com links que direcionam para sites maliciosos, forjados para parecerem fontes de informação legítima sobre o Covid-19 (como órgãos nacionais ou mundiais de saúde), no intuito de roubar credenciais de acesso de plataformas corporativas de trabalho, como Office365. Esta técnica é conhecida como *phishing*, e o termo teve sua popularidade nos motores de busca do Google elevada durante este ano.
5. Em alguns casos, links suspeitos contidos em e-mails ou outras mensagens direcionam para o download de arquivos contendo softwares maliciosos (*malwares*), muitas vezes disfarçados de documentos do Word ou PDF ou outros tipos de arquivos legítimos, normalmente usados em ambientes corporativos. Em alguns casos, estes *malwares* eram *ransomwares*, um tipo de *malware* que criptografa informações de modo que fiquem inacessíveis, normalmente pedindo algum resgate em dinheiro ou moedas virtuais para devolução ou restauração dos dados. Vale ressaltar também que a busca pelo termo *ransomware* também teve sua popularidade aumentada no decorrer da pandemia.
6. Ataques de negação de serviço (DoS) a plataformas corporativas ou a sites de empresas. Em alguns casos, tal comportamento é facilitado por uma resposta lenta de certas organizações ao cenário de mudança para o teletrabalho, fragilizando ambientes já existentes e os tornando mais vulneráveis a este tipo de ataque. Outra estatística referente a isso, é o aumento da popularidade do termo VPN, especialmente entre fevereiro e abril desse ano.

Os problemas relatados acima, apesar de possuírem um alto potencial destrutivo, são todos originados fora do ambiente corporativo, podendo ser considerados ameaças. Entretanto, existem algumas dificuldades originadas dentro das empresas, e que, portanto, podem ser consideradas como fraquezas ou fragilidades, que se tornaram ainda mais evidentes neste período de pandemia. Citando novamente os autores, pode-se enumerá-las da seguinte forma:

7. Aumento do uso de dispositivos corporativos para finalidades pessoais, como utilização para redes sociais ou troca de mensagens. Os principais dispositivos sujeitos a este tipo de utilização indevida são notebooks e celulares.
8. Funcionários podem ser potenciais ameaças internas às companhias, tendo em vista as dificuldades econômicas e sociais oriundas do período de pandemia. Entre as principais dificuldades identificadas pelas consultorias Deloitte e KPMG, podem-se destacar a perda de emprego, redução salarial e incerteza sobre empregabilidade

nos próximos 12 a 18 meses. Em alguns casos, ofensores externos se valem destas incertezas de funcionários ou ex-funcionários para conseguir informações corporativas e/ou privilegiadas, como dados do ambiente interno ou informações de clientes e fornecedores.

9. Funcionários atuam também como outra forte ameaça interna no sentido de que muitos não estão habituados ao teletrabalho. Dificuldades incluem pouco ou nenhum contato com tecnologias como VPN e softwares de teleconferência ou ferramentas de colaboração conjunta (como Cisco Webex, Microsoft Teams ou Slack), falta de clareza no entendimento de alguns processos corporativos (sejam eles novos ou adaptados à nova realidade), além de muitas vezes não terem um espaço dedicado para isso em casa.
10. Com o aumento acentuado na adoção do *home office*, em alguns casos é difícil manter a confidencialidade de informações, especialmente quando mais de uma pessoa na residência está nesta modalidade de trabalho. Isso se agrava nos casos em que não se possui uma estrutura doméstica apropriada para tanto, como um escritório ou ambiente mais reservado para o teletrabalho.
11. Atrasos na resposta a ataques e incidentes de segurança. Com times trabalhando de maneira remota e, em muitos casos, sem interação direta, o gerenciamento de equipes de resposta a incidentes pode não ser tão eficiente como em um cenário pré-pandemia.
12. Infraestrutura (como concentradores de VPN, portais de acesso e/ou corporativos, gateways de voz e vídeo) insuficiente ou não redimensionada corretamente para atender ao aumento repentino de demanda. Em alguns casos a infraestrutura pode ter sido redimensionada, mas não foi testada para verificar se consegue operar eficientemente sob a nova carga de trabalho.
13. Conexões inseguras com o ambiente corporativo. Em alguns casos, funcionários utilizam redes sem fio compartilhadas com vizinhos (cenário muitas vezes comum em apartamentos) ou até mesmo redes públicas, como em cafeterias ou bibliotecas, para acesso ao ambiente corporativo. Além disso, existem casos em que funcionários trabalham usando seus próprios dispositivos computacionais ou celulares, seja por insuficiência de recursos corporativos ou porque a cultura da empresa permite/incentiva tal prática (BYOD[11]).
14. Cortes de custos ou diminuição de investimentos relativos à segurança digital após o término da pandemia. Vários fatores podem causar tal redução, como a redução de faturamento das empresas, remanejamento da distribuição de orçamentos para os próximos anos fiscais e diminuição da percepção de cyber-segurança como sendo algo crítico ou fundamental para a companhia.

Uma vez expostos alguns dos principais desafios para as companhias, a próxima seção analisará algumas contramedidas recomendadas por especialistas na área.

## 4. Contramedidas

Uma vez que se enumera os desafios causados pela pandemia de Covid-19, é possível começar a elaborar medidas para sua resolução, ou mesmo para a diminuição ou mitigação de riscos operacionais e de TI. Neste ponto, é importante destacar que, devido

[11] "*Bring Your Own Device*", ou "Traga seu próprio dispositivo", em tradução livre.

às naturezas diversas de riscos apresentados na seção anterior, as contramedidas serão separadas em tópicos, para melhor entendimento e catalogação.

### 4.1. Plataformas digitais de compra e venda

- Procurar por referências externas de confiabilidade (plataformas como o Reclame Aqui, por exemplo).
- Procurar por erros ortográficos, que podem indicar sites fraudulentos.
- Verificar se os dados fornecidos pela empresa em seu site (como CNPJ, telefone e endereço) realmente existem.
- Nunca fornecer detalhes bancários para efetuar pagamentos.
- Desconfiar e verificar a autenticidade quanto ao recebimento de ofertas com preços muito abaixo da média de mercado.

### 4.2 *Spams*, *scams* e *phishing*

- Desconfiar de e-mails em nome de instituições importantes, como bancos, órgãos de saúde ou órgãos governamentais.
- Desconfiar de e-mails cujo remetente seja desconhecido ou pertença a um domínio que não condiz com quem afirma ser, bem como e-mails com o(s) destinatário(s) em cópia oculta (BCC/CCO).
- Desconfiar de e-mails cujo assunto /ou conteúdo seja alarmista ou busque despertar ações imediatas ou urgentes.
- Não abrir e-mails suspeitos.
- Nunca fazer download de arquivos anexos em e-mails, a não ser que sejam esperados e as verificações acima tenham sido feitas.

### 4.3 Medidas defensivas em dispositivos computacionais pessoais e corporativos

- Instalar um programa *anti-malware* eficiente e de confiança em todos os dispositivos computacionais conectados à internet, como computadores, *tablets* e celulares. Onde possível, instalar também um software de filtragem de pacotes de rede (*firewall*).
- Manter o sistema operacional, antivírus, *firewall* e demais aplicações sempre atualizadas. Na maioria dos casos, eles possuem um sistema de atualizações automáticas que costuma vir ativado por padrão.
- Somente instalar programas de fontes conhecidas.

### 4.4 Técnicas de engenharia social

- Desconfiar de ligações, e-mails ou mensagens solicitando informações pessoais (como endereço, CPF ou data de nascimento) ou bancárias (como *tokens* de autenticação, número de cartões e códigos de segurança).
- Evitar clicar em links desconhecidos. Em alguns navegadores existe um recurso muito útil que mostra o destino de um link apenas passando o mouse sobre ele, sem que seja necessário clicar.
- Desconfiar de anexos não solicitados que forem recebidos em qualquer plataforma. Sempre verificar se a extensão do arquivo corresponde ao suposto arquivo.
- Verificar a fonte de qualquer informação recebida, especialmente antes de tomar qualquer decisão sobre ela (incluindo a decisão de repassar a informação).

### 4.5 Medidas corporativas estruturais

- Escalar concentradores de VPN, *gateways* de voz e dados, portais de acesso e outros componentes de infraestrutura de acesso para acomodar o teletrabalho.
- Testar a infraestrutura para determinar se ela consegue aguentar a carga de trabalho esperada e demandada.
- Identificar pontos únicos de falha na infraestrutura e criar resiliência adicional ou redundâncias para estes. Um ponto único de falha é, conforme a Oracle Corporation (2010), "um componente de um sistema que, em caso de falha, faz com que todo o sistema fique indisponível ou não seja confiável".[12]
- Manter um backup funcional de dados importantes (esse método vale também para informações pessoais). Sempre que possível, manter mais de um backup e em mais de um tipo de mídia diferente.
- Redimensionar, se necessário, a capacidade de *help desk* para atender a novas demandas de usuários trabalhando remotamente.
- Garantir que haja disponibilidade de equipamentos computacionais suficiente para atender a novas demandas de funcionários trabalhando remotamente, visando eliminar a necessidade de trabalhar com o próprio dispositivo.
- Reduzir ou eliminar a dependência de indivíduos-chave, sejam eles funcionários ou parceiros de negócio. Onde, no caso de indivíduos, isso não for possível, garantir que estes indivíduos estejam praticando forte e efetivamente o distanciamento social.
- Adicionar um portal, menu de *service desk* ou linha telefônica dedicada para que os funcionários reportem qualquer aparente irregularidade ou incidente. Este tipo de informação deve ser facilmente acessível.
- Usar criptografia de disco (se possível a nível de hardware ou sistema operacional) para dados em repouso.
- Investir em métodos de autenticação mais robustos para acesso ao ambiente corporativo e e-mails, como *tokens* e autenticação multifatorial.

### 4.6 Medidas corporativas procedurais

- Treinamento efetivo e prático sobre como utilizar as ferramentas de acesso corporativo em teletrabalho.
- Treinamento e conscientização sobre a importância de se estar atento a ameaças provenientes de ataques que se utilizem de *phishing*, engenharia social e fraudes baseadas na Covid-19.
- Enfatizar os protocolos de segurança existentes e encorajar que os funcionários se manifestem sem receios caso algo aparente estar errado.
- Capacitação adicional para os times de suporte, *help desk* e resposta a incidentes, visando a atuação remota de maneira efetiva e eficaz.
- Alterar, onde for necessário, mecanismos de monitoramento, controle e resposta a incidentes relativos à segurança da informação, para que, caso um incidente ocorra, o gerenciamento desde e da equipe que o tratará possa ser feito de maneira efetiva, mesmo à distância. Os times de auditoria (tanto internos como externos, se houver) podem ser de extrema ajuda neste ponto.

---

[12] "*A single point of failure (SPOF) is a system component which, upon failure, renders an entire system unavailable or unreliable"*, traduzido pelo autor.

- Através de uma comunicação clara, passar aos funcionários uma sensação de segurança sobre como a empresa está lidando com a pandemia, especialmente no que tange à permanência de funcionários na empresa.
- Uso de fones de ouvido, gavetas com tranca, filtros de privacidade para telas e trituradores de papel quando se estiver trabalhando fora das dependências da empresa. Se possível, ter um local reservado em casa para tal finalidade.

Estes são os pontos apresentados pelos autores anteriormente e que podem ser considerados de alta relevância na forma como as empresas podem se adaptar à realidade imposta pela pandemia de Covid-19. Convém salientar que as medidas e processos devem ser ajustados à realidade de cada empresa, e que não há uma trilha específica ou cenário ideal, mas que a adoção de qualquer medida deve ser objeto de estudo pela empresa antes de sua implantação (visando analisar sua viabilidade) e depois desta (visando mensurar seus impactos), devendo ser feitos quaisquer ajustes necessários.

## 5. Estudo de caso em uma rede supermercadista

Após a apresentação de dados catalogados por pesquisadores e empresas de consultoria sobre o impacto da pandemia em curso para a segurança da informação em ambientes corporativos, é válido demonstrar um exemplo prático de algumas alterações. Para isso, será exposto o caso de uma rede supermercadista, atuante no interior do estado de São Paulo, na microrregião de Campinas, e como a empresa se adaptou tecnológica e processualmente ao cenário de pandemia.

A empresa, fundada há mais de 50 anos e com sede no município de Americana, é uma rede de supermercados que opera, atualmente, com duas bandeiras. Uma delas, com 17 lojas presentes em 10 cidades, é a rede que opera exclusivamente com varejo, enquanto a segunda bandeira, que atua como varejo e atacado, está presente em 3 municípios, por meio de 4 lojas. A rede, com aproximadamente 3800 funcionários, possui ainda um centro logístico próprio, bem com uma sede administrativa (onde ficam aproximadamente 200 funcionários). Serão analisadas algumas alterações que precisaram ser feitas, tanto do ponto de vista tecnológico como do ponto de vista operacional, visando a adequação ao cenário de pandemia. Posto isso, pode-se destacar as seguintes mudanças realizadas pela empresa:

- Todos os links MPLS que interligam os diferentes *sites* da empresa foram migrados para a tecnologia SD-WAN (o que incluiu a substituição de vários equipamentos de rede em todos os sites) permitindo melhor gerenciamento, maior segurança e a possibilidade de melhor definir políticas de priorização de tráfego de rede conforme seu tipo (*traffic-shaping*).
- Uma vez que todo tráfego interno e externo passa pelo *data center* antes de chegar ao seu destino, foi necessário aumentar a largura de banda dos links de internet em mais de 300%, de modo a comportar o aumento de demanda. Segundo a estimativa da empresa, até 70% do quadro operacional da sede administrativa (que possui o maior consumo de banda) pode trabalhar à distância simultaneamente sem prejuízos às atividades.
- Aumento da largura de banda dedicada ao gateway de voz, visando uma melhor qualidade de ligações realizadas usando-se a plataforma de VoIP da empresa.

- Foram providenciados notebooks e celulares corporativos para todos os colaboradores do departamento de TI, com o objetivo de suportar as operações da empresa da melhor forma possível, em qualquer horário.
- Foram providenciados notebooks para todos os gerentes, além de outros funcionários-chave, que dependam de alta mobilidade para desempenho de suas funções ou que prestem algum tipo de plantão para suporte às operações.
- Implementação da plataforma Microsoft Office365 para todos os funcionários com usuários baseados em AD (*Active Directory*). Inclui-se nisso a migração de e-mail baseado em IMAP para Exchange, o controle de licenças do Microsoft Office centralizado e vinculado ao usuário do AD e disponibilização da plataforma Microsoft Teams para todos os funcionários, visando garantir o distanciamento social, mesmo para os que estão trabalhando no escritório administrativo.
- A reunião mensal com os gerentes regionais e das lojas foi migrada totalmente para modalidade remota, sendo realizada agora via Microsoft Teams. Em todas as lojas foi providenciada uma rede sem fio dedicada para uso gerencial.
- Para todos os funcionários da sede administrativa foi disponibilizado o acesso para teletrabalho, sendo autenticado com certificado digital e senha. Para cada usuário, o acesso a cada concentrador de VPN é realizado com um certificado digital diferente, tudo gerenciado por um *appliance* de segurança *open-source*.
- Foi fornecido treinamento para todos os funcionários (onde aplicável) sobre a utilização da VPN para acesso à rede corporativa quando da realização de teletrabalho, abordando funcionalidades da aplicação e medidas de segurança e cuidados a serem tomados (como Políticas de Mesa Limpa e de Tela Limpa, por exemplo), bem como treinamento sobre como se proteger de *spam* e *phishing*.
- Disponibilização de um número telefônico exclusivo para atendimento a funcionários que estivessem enfrentando problemas no trabalho remoto, além de suporte via WhatsApp, quando necessário.
- Reorganização do horário de funcionamento da equipe de suporte de TI, de modo a ter uma maior porcentagem da equipe durante o horário administrativo (das 9h às 18h durante a semana e das 9h às 15h aos sábados). Para os demais dias e horários, foi instituído o plantão na modalidade de sobreaviso, onde o agente de suporte é acionado apenas quando há necessidade.
- Alinhamento do processo de acionamento do time de suporte por parte das lojas em um único número telefônico, que direciona a ligação para uma aplicação VoIP com clientes instalados nos celulares corporativos da equipe. Cada agente possui seu próprio ramal na aplicação, e a configuração de disponibilidade de cada agente é centralizada, direcionando as ligações para o agente correto em função do horário pré-definido.
- Automatização de processos sistêmicos que antes dependiam de intervenção humana, como exportação e conferência de informações sobre vendas e programação de preços de produtos.
- Expansão do sistema de monitoramento de rede para abranger informações resultantes de processamentos automatizados e acionar a equipe responsável (atuando em sobreaviso), se necessário.

Apesar de não serem abordadas acima todas as alterações realizadas na empresa, pode-se perceber que foram feitas mudanças significativas na parte de operações e

suporte. A modernização de processos se deu em decorrência da necessidade de maior agilidade na resposta às mudanças mercadológicas existentes, bem como na busca para proporcionar uma maior qualidade de vida para os colaboradores e uma melhor experiência para o cliente.

Ainda no que tange à experiência do cliente, a empresa iniciou em 2020 as operações de sua plataforma de *e-commerce*, inicialmente apenas para sua bandeira de varejo, abrangendo 10 cidades do interior paulista. As compras podem ser feitas pelo site ou aplicativo da empresa, e o cliente tem a opção de retirar as compras na loja mais próxima de sua residência (pela modalidade *drive-thru*) ou recebê-las em casa. O pagamento pode ser feito no site, via cartão de crédito, ou no momento da retirada ou entrega, por cartão de débito ou crédito.

Percebe-se, então, que mesmo para empresas com uma cultura não tão direcionada à tecnologia, principalmente em decorrência da natureza de seu Negócio, o cenário de pandemia trouxe a necessidade e oportunidade de analisar processos internos e reestruturá-los, visando maior dinamicidade e agilidade. Em última análise, os benefícios sentidos na empresa, como uma maior facilidade de adequação às necessidades mercadológicas, se traduzem em mais facilidade e segurança: no geral, uma melhor experiência para o cliente.

## 6. Considerações Finais

A capacidade de infecção e propagação do SARS-CoV-2 fez com que mudanças profundas ocorressem na sociedade, no modo como as pessoas trabalham, estudam, se locomovem, buscam informações sobre temas de preocupação geral, ofertam e consomem produtos ou serviços. Diferentemente de episódios pandêmicos anteriores, desta vez a humanidade tem a *internet* como uma importante aliada, como é evidenciado pelo massivo aumento da dependência de serviços baseados na *internet* ao longo de 2020.

Até o momento da redação deste artigo, não existe uma vacina disponível contra a Covid-19, e muitos países que enfrentaram a primeira onda de propagação da doença no primeiro semestre de 2020 com restrições à circulação (e até mesmo *lockdown* em casos mais críticos) e medidas sanitárias intensificadas viram seu número de infecções e mortes serem reduzidos durante este período em decorrências das ações adotadas. Entretanto, nestes mesmos países, uma vez que alguns setores da economia estão retomando suas atividades, é sensível a tendência oposta, com o aumento diário de novos casos, internações e óbitos. Tais fatores, em conjunto, levam a crer que, este cenário cíclico, de imposição e afrouxamento alternados de medidas preventivas, especialmente o distanciamento social, será realidade nos próximos meses ou anos, até que se tenha uma imunização populacional eficiente e massiva. Posto isto, e à luz das informações abordadas, identifica-se uma tendência de aceleração ainda maior da transformação digital pela qual a sociedade passa. Como consequência, é necessária a manutenção de medidas de segurança cibernética já existentes, bem como a elaboração de novas medidas em resposta ao cenário hostil que foi identificado no artigo.

Adicionalmente, o estudo ressalta que novos métodos de interação com clientes podem ser a chave para se manter relevante frente às mudanças impostas e aceleradas pela pandemia. Serviços de aquisição e entrega de bens de consumo não-duráveis, como

víveres perecíveis, por exemplo, são uma nova realidade e tendência mercadológica. Apenas a título de exemplo, as empresas podem começar a analisar hábitos de consumo identificados a partir dos dados coletados por tal modalidade comercial visando refinar e direcionar ainda mais suas campanhas publicitárias e se tornar mais relevantes para seus clientes, ofertando produtos que os clientes *queiram* ou dos quais *precisem*, e, mais importante ainda, *quando* os clientes precisam.

Além disso, ficam orientações relativas à segurança em ambientes corporativos, como uso de métodos cada vez mais robustos de criptografia e mecanismos de autenticação, bem como outras técnicas objetivando garantir a privacidade e integridade de informações corporativas, sejam elas confidenciais ou não, e a alta disponibilidade de ambientes, sistemas e plataformas. Paralelamente a isso, a adoção de boas práticas como políticas de backup eficientes, atualização constante de sistemas operacionais e *softwares*, mecanismos de identificação e bloqueio de atividades suspeitas em ambientes corporativos é, mais do que nunca, primordial. E, entre tais boas práticas, pode-se destacar o treinamento constante a usuários, uma vez que por mais seguros que sejam os sistemas computacionais modernos, eles ainda são operados por seres humanos. E, como também salientado no artigo, é neste fator humano, imprevisível, sensível e, em muitos casos, o elo mais fraco da corrente de segurança cibernética, que criminosos vêm concentrando seus esforços, muitas vezes com resultados positivos para si próprios e prejudiciais para instituições e pessoas.

Finalmente, cabe indicar que estudos futuros concernentes a este tema podem incluir a coleta e análise de dados relativos à satisfação de clientes e colaboradores frente às mudanças operacionais e procedurais nas empresas, aplicadas em decorrência da Pandemia. Podem ser estudados também impactos financeiros positivos e negativos em decorrência do remanejamento orçamentário das empresas para investimentos em infraestrutura de TI e soluções de segurança cibernética. Um terceiro objeto de estudo pode ser o impacto positivo ou negativo da adoção extensiva de teletrabalho nos níveis de produtividade dos funcionários.

## Referências


Aladenusi, Tope. “COVID-19’s Impact on Cybersecurity”, 2020. Disponível em <https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf>. Acesso em 08 nov 2020.

Anant, Venky; Caso, Jeffrey and Schwarz, Andreas. “COVID-19 crisis shifts cybersecurity priorities and budgets”, 2020. Disponível em <https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets#>. Acesso em 08 nov 2020.

Bates, Steve. “IT operating model impacts of COVID-19 – Navigating the multi-dimensional aspects of a new reality”, 2020. Disponível em <https://home.kpmg/xx/en/home/insights/2020/05/it-operating-model-impacts-of-covid-19.html>. Acesso em 21 nov 2020.

Bates, Steve. “Managing the information security impact of COVID-19 – Risk and security threats related to remote working”, 2020. Disponível em <https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html>. Acesso em 08 nov 2020.

Google, Inc. “Google Trends – Pesquisar - coronavirus”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=coronavirus >. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - pandemics”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=pandemics>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - phishing”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=phishing>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - ransomware”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=ransomware>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - SARS”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=SARS>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - spam”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=spam>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - VPN”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=VPN>. Acesso em 09 nov 2020.

Google, Inc. “Google Trends – Pesquisar - Wuhan”, 2020. Disponível em: <https://trends.google.com/trends/explore?q=Wuhan>. Acesso em 09 nov 2020.

Kane, Gerald C. et al. “A case of acute disruption - Digital transformation though the lens of COVID-19”, 2020. Disponível em: <https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-transformation-COVID-19.html>. Acesso em 31 out 2020.

Khalid, Kark. “The kinetic leader: Boldly reinventing the enterprise – Findings from the 2020 Global Technology Leadership Study”, 2020. Disponível em <https://www2.deloitte.com/us/en/insights/topics/leadership/global-technology-leadership-study.html>. Acesso em 08 nov 2020.

KPMG International Cooperative. “Risk and security in the wake of COVID-19 – Steps CISOs can take now to keep businesses operating”, 2020. Disponível em <https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/04/risk-and-security-in-the-wake-of-covid-19-concern.pdf>. Acesso em 08 nov 2020.

KPMG International Cooperative. “Understand the implications of COVID-19 on your IT operating model – Thriving in the new reality”, 2020. Disponível em <https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/05/understand-the-implications-of-covi-19-on-your-it-operating-model.pdf>. Acesso em 21 nov 2020.

Lambert, Lance. “Fortune survey: 62% of CEOs plan policy changes in response to current calls for racial justice”, 2020. Disponível em <https://fortune.com/2020/06/17/fortune-survey-62-of-ceos-plan-policy-changes-in-response-to-current-calls-for-racial-justice/>. Acesso em 08 nov 2020.

Nasri, Grace. “Why consumers are increasingly willing to trade data for personalization”, 2012. Disponível em: <https://www.digitaltrends.com/social-media/why-consumers-are-increasingly-willing-to-trade-data-for-personalization/#ixzz2g8dgrqko>. Acesso em 31 out 2020.

Okereafor, Kenneth and Adebola, Olajide. “Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety”, 2020. Disponível em: <https://www.researchgate.net/publication/339727143_TACKLING_THE_CYBERS

ECURITY_IMPACTS_OF_THE_CORONAVIRUS_OUTBREAK_AS_A_CHALLENGE_TO_INTERNET_SAFETY>. Acesso em 31 out 2020.

Oracle Corporation. “Availability and Single Points of Failure”, In: Sun Directory Server Enterprise Edition 7.0 Deployment Planning Guide, 2010. Disponível em: <https://docs.oracle.com/cd/E19424-01/820-4806/fjdch/index.html>. Acesso em 21 nov 2020.

Salesforce.com, Inc. “Examples of Digital Transformation?”, In: Getting Started With Digital Transformation. Disponível em: <https://www.salesforce.com/products/platform/examples-of-digital-transformation/?d=cta-right-nav-2>. Acesso em 31 out 2020.

Salesforce.com, Inc. “How to Digitally Transform Your Business?”, In: Getting Started With Digital Transformation. Disponível em: <https://www.salesforce.com/products/platform/how-to-transform-your-business-for-digital/>. Acesso em 31 out 2020.

Salesforce.com, Inc. “KLM’s social media team can now respond to thousands of user posts every day”, 2020. Disponível em: <https://www.salesforce.com/customer-success-stories/klm/>. Acesso em 21 nov 2020.

Salesforce.com, Inc. “What is Digital Transformation?”, In: Getting Started With Digital Transformation. Disponível em: <https://www.salesforce.com/products/platform/what-is-digital-transformation/>. Acesso em 31 out 2020.

Salesforce.com, Inc. “Why are Businesses Going Through Digital Transformations?”, In: Getting Started With Digital Transformation. Disponível em: < https://www.salesforce.com/products/platform/why-business-need-transformation-innovation/?d=cta-right-nav-1>. Acesso em 31 out 2020.

Westerman, George; Bonnet, Didier and McAfee, Andrew. “The Nine Elements of Digital Transformation”, 2014. Disponível em: <https://sloanreview.mit.edu/article/the-nine-elements-of-digital-transformation/>. Acesso em 31 out 2020.

World Health Organization. “Coronavirus disease (COVID-19)”, 2020. Disponível em: <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/coronavirus-disease-covid-19>. Acesso em 31 out 2020.

World Health Organization. “WHO Coronavirus Disease (COVID-19) Dashboard”, 2020. Disponível em: <https://covid19.who.int/>. Acesso em 8 nov 2020 e 23 nov 2020.

Walter Luiz Martinelli Junior

# Impactos da Pandemia de COVID-19 na Segurança da Informação para as empresas e pessoas

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.

Área de concentração: Tecnologia da Informação.

Americana, 02 de dezembro de 2020.

**Banca Examinadora:**

_____

Marcus Vinícius Lahr Giraldi (Presidente)

Especialista

Fatec Americana Ministro Ralph Biasi

_____

Francisco Carlos Mancin (Membro)

Mestre

Fatec Americana Ministro Ralph Biasi

_____

Armando Vulcano Júnior (Membro)

Especialista

Fatec Americana Ministro Ralph Biasi