SEVEN publicações acadêmicas
EM PARCERIA COM: IEMS UNIASSELVI

# Uma análise conceitual dos riscos e dos desafios da segurança da informação na computação em nuvem

**David Kadab Chaves**
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ – Rio de Janeiro-RJ

**Gláucya Daú**
Universidade do Estado do Rio de Janeiro - UERJ – Rio de Janeiro-RJ
Universidade Federal Fluminense - UFF – Niterói-RJ

**Annibal Scavarda**
Universidade Federal do Estado do Rio de Janeiro - Unirio – Rio de Janeiro-RJ
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca - CEFET/RJ – Rio de Janeiro-RJ
Universidade Federal Fluminense - UFF – Niterói-RJ

**RESUMO**
Este presente artigo esclarecerá temas relevantes relacionados à evolução tecnológica e como obter excelência no quesito segurança em computação nas nuvens. O objetivo é demonstrar a real importância da Segurança Computacional nas empresas que utilizam este recurso e que exige a cada dia que dados não sejam apenas armazenados, mas também preservados. A metodologia utilizada neste trabalho foi baseada em um estudo de caso exploratório, de natureza qualitativa, integrando a revisão da literatura. Será que estamos protegidos a todo tempo? Como fazer para evitar vulnerabilidades? Como mitigar os riscos? Como saber identificar uma ameaça? Perguntas que são mais complexas de serem respondidas do que aparentam. Concluiu-se que as empresas não sabem classificar as informações, tão pouco distinguir quais são os verdadeiros ativos que devem ser resguardados, sendo muitas vezes ignorado o quesito segurança.

**Palavras-chave**: Ameaças, *Cloud Computing*, *Malware*, Segurança da informação, Vulnerabilidade.

## 1 INTRODUÇÃO

O cenário atual mostra um momento em que o desenvolvimento tecnológico evolui assustadoramente e que em muitas vezes não é tarefa simples conciliar a segurança das informações com todo este avanço tecnológico, porém é de extrema importância refletir sobre como preservar os três principais pilares da segurança da informação, são eles: confidencialidade – garante que a informação seja acessível somente por pessoas autorizadas; disponibilidade – garante que a informação esteja acessível sempre que necessário e integridade – garante que a informação esteja integra desde sua origem até o destino. A evolução tecnológica teve como marco histórico, o momento em que o homem conseguiu armazenar dados para utilizá-los posteriormente. Observa-se como os computadores já se solidificam na forma de dispositivos móveis, usados até mesmo como suporte ao trabalho; surgem servidores mais potentes a cada dia e o *Cloud Computing* também vem ganhando espaço na sociedade.

Quando o assunto é segurança da informação, podemos relacionar custo e benefício. O custo nem sempre é acessível conforme desejado, porém evitará futuros problemas que podem causar impactos significativamente superior ao custo de implementar uma política de segurança eficiente. Será que os gestores estão cientes deste cenário? Será que estariam dispostos a investir na segurança?

## 2 OBJETIVO

O objetivo deste artigo científico é demonstrar a importância da Segurança Computacional nas empresas que utilizam a tecnologia de computação nas nuvens, onde a evolução tecnológica exige que a cada dia dados não sejam apenas armazenados, mas também preservados. Para isto, este trabalho fará uma breve introdução aos tipos de infrações virtuais e as pessoas que as praticam, para que o entendimento seja completo. E para finalizar, abordará as principais tendências tecnológicas.

## 3 METODOLOGIA

A proposta metodológica foi baseada em um estudo de caso exploratório, de natureza qualitativa, integrando a revisão da literatura. Aplicar-se-á as seguintes perguntas norteadoras: Será que estamos protegidos a todo tempo? Como fazer para evitar vulnerabilidades? Como mitigar os riscos? Como saber identificar uma ameaça?

Para a revisão da literatura foram construídas equações de busca com base em palavras-chave e conectadas com a temática. O Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) foi a base de dados para a busca dos artigos. Essa metodologia de pesquisa foi escolhida com a intenção de facilitar a identificação das tecnologias utilizadas e o que pode ser melhorado, gerando informações que possam nortear a implementação de novos recursos tecnológicos.

## 4 DESENVOLVIMENTO

A informação é o principal ativo de uma empresa, portanto necessita ser bem protegido. Este trabalho contém pesquisas e estudos realizados abordando o assunto custo e benefício ao investir em segurança, para que a empresa consiga acompanhar a evolução tecnológica sem grandes percas.

Este artigo foi baseado em diversas pesquisas que envolvem a importância da segurança dos ativos no meio empresarial. Mais de 70% das empresas brasileiras ainda não contam com um sistema de segurança adaptado. Um breve estudo sobre infrações virtuais e os tipos de infratores para nivelar o entendimento e será apresentado estudos relacionados a uma tecnologia que está em ascensão, o *Cloud Computing*.

## 4.1 *CLOUD COMPUTING*

Indiscutivelmente que a computação em nuvem veio para ficar, essa crescente e exponencial evolução (MATHER, 2009), que já está deixando de ser tendência e está se tornando realidade. Seus apelos (facilidade de acessar serviços de dados e aplicações de qualquer dispositivo e de qualquer lugar; e sem a necessidade de ter um HD para realizar o armazenamento) são atrativos. Entretanto, nos traz novos desafios em termos de segurança, privacidade e resiliência. Um provedor de nuvem pública, por questões estratégicas, não abre sua tecnologia, organização e processos.

A questão da segurança é de fundamental importância. A aceleração da computação em nuvem está diretamente relacionada com o grau de confiança no modelo e nas tecnologias envolvidas. Sem sentir confortáveis com o nível de segurança obtido, os gestores das empresas não tomarão decisões favoráveis. Assim, conhecer os múltiplos aspectos que envolvem segurança em *Cloud Computing* é obrigação de todo gestor ou profissional de tecnologia. O relatório começa com um nivelamento dos aspectos conceituais da computação em nuvem, seus modelos de serviço (Infraestrutura como Serviço, Plataforma como Serviço e Software como Serviço) e de entrega (Nuvens Públicas e Privadas). A partir daí descreve os aspectos críticos que se relacionam com segurança, divididos basicamente em dois domínios: o domínio da governança (incluindo fatores como riscos, auditoria, avaliação e relatórios); e operacional, que inclui variáveis como operação do data center em nuvem, continuidade do negócio, gerenciamento de identidades de acesso, virtualização etc.

A segurança é indiscutivelmente o que leva a refletir se realmente deve-se investir em *Cloud Computing*. Existem vários quesitos que geram uma desconfiança, não se sabe onde está localizado o servidor em nuvem, não é claro o que os provedores deste serviço realizam para prover excelência na segurança, não se sabe sobre a segurança física desse local e também sobre a segurança relacionada à confiabilidade, porém existe uma fatia da segurança que oferece um grande conforto para quem contrata serviços em *Cloud Computing*, pois a empresa que fornece esse tipo de serviço garante em contrato que é responsável por todos os dados hospedados, podendo constar em contrato inclusive multas por não cumprimento.

Atualmente, além do *Cloud Computing*, a questão da virtualização está também em ascensão. Os servidores físicos estão ficando obsoletos, devido a uma grande procura por servidores virtuais (TULLOCH, 2014).

Na medida em que mais experiências práticas são obtidas com a computação nas nuvens, o relatório será expandido e acrescido de mais detalhamentos. De acordo com várias pesquisas realizadas, ainda é comum ver muitas pessoas pensando que essa tecnologia vai demorar a disseminar, principalmente porque muitos analistas de indústrias fazem estimativas conservadoras de sua adoção pelo mercado. É verdade que

os relatórios de analistas de indústrias com estimativas em relação às tendências e perspectivas de *Cloud Computing* tendem a serem bem conservadoras.

Pesquisas a respeito deste assunto, realizadas com especialistas, mostram que os resultados são unanimes, onde exploram fatores que mostram que a computação nas nuvens cresce cada vez de forma mais exponencial e é uma realidade que está sendo incorporada nas instituições de uma maneira que propicia resultados significativos.

Quando é dito que ela cresce de forma exponencial, deve ser lembrado o lendário "criador da computação", Von Neumann. Ele fez duas observações importantes: uma que o progresso humano é exponencial e não linear. A outra é que este crescimento exponencial começa devagar e muitas vezes passando despercebido, até que atinge um ponto crítico, quando se transforma em algo explosivo e profundamente transformador.

Geralmente as previsões são baseadas na perspectiva de um crescimento linear e não exponencial. Mas o ritmo de mudanças está acelerando. Por exemplo, os últimos 20 anos de progresso do século XX seriam conseguidos hoje em 14 anos. Em breve em apenas 7 anos e assim sucessivamente. Em termos práticos, o século XXI terá um ritmo de progresso tecnológico pelo menos 1000 vezes maior que o que vimos no século que acabou recentemente.

Novas tecnologias trazem muitos benefícios, mas não é aconselhável desprezar as questões de segurança. Computação em nuvem é uma mudança no modelo computacional como um todo, mas o uso de nuvens públicas deve ser visto com atenção. Não que elas sejam inerentemente inseguras, geralmente não são, mas nossos hábitos muitas vezes facilitam os acessos indevidos. Uma alternativa é usar nuvens privadas (nuvens computacionais internas ao "firewall", quando é mais fácil ter o acesso ao controle das normas e procedimentos de segurança) ou mesmo usar nuvens híbridas, onde é formada por nuvens privadas para aplicações e dados críticos, mas também usando alguns serviços providos por nuvens externas, constituídos de determinados tipos de serviços.

## 4.2 PRINCIPAIS TIPOS DE *MALWARES*

Quando um equipamento é conectado a uma rede, automaticamente ele deixa de estar 100% seguro. Existem vários tipos de malwares que podem causar impactos significativos para o meio corporativo, assim como para o uso pessoal. Abaixo, os principais tipos de malwares da atualidade (ULBRICH, 2004).

- **Vírus:** Vírus é um programa de computador malicioso que se propaga infectando, ou seja, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução dos arquivos hospedeiros para que possa se tornar ativo e continuar o processo infecção.

- ***Worm*:** *Worm* é um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores.
- ***Trojan*:** *Trojan* é um programa que se passa por um "presente" (por exemplo, cartões virtuais, álbum de fotos, protetor de tela, jogos) que além de executar funções para as quais foi aparentemente projetado, também executam outras funções normalmente maliciosas e sem o conhecimento do usuário. O *Trojan* geralmente é responsável por abertura de portas, deixando assim, brechas para outros ataques provenientes de outros tipos de *malwares.*
- ***Keylogger*:** *Keylogger* é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, como, por exemplo, após o acesso a um site de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.
- ***Screenlogger*:** *Screenlogger* é a forma avançada de *keylogger*, onde é capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou armazenar a região que circunda a posição onde o mouse é clicado.
- ***Spyware*:** *Spyware* é a palavra usada para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Podem ser usadas de forma legítima, mas, geralmente são usadas de forma dissimulada, não autorizada e maliciosa; tem como principal ferramenta URL falso.
- ***Backdoor*:** *Backdoor* é um programa que permite a um invasor retornar a um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.
- ***Exploits*:** *Exploits* são programas maliciosos projetados para explorar uma vulnerabilidade existente em um software de computador.
- ***Sniffers*:** *Sniffers* são usados para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos que estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia. Deixa a placa de rede do computador em modo promíscuo, ou seja, a placa de rede passa a processar todos os pacotes que viajam pela rede conectada e não apenas os pacotes que eram de destinos específicos.
- **Ataque DoS (*Denial of Service*):** Ataques de DoS, também conhecidos como "Ataques de Negação de Serviços", consistem em tentativas de fazer com que computadores - servidores *Web*, por exemplo

- tenham dificuldade ou mesmo sejam impedidos de executar suas tarefas. Para isso, em vez de "invadir" o computador ou mesmo infectá-lo com malwares, o autor do ataque faz com que a máquina receba tantas requisições que chega ao ponto de não conseguir interpretar todas delas. Em outras palavras, o computador fica tão sobrecarregado que nega serviço, deixando todo o acesso indisponível. Dependendo do serviço atingido, pode haver um prejuízo enorme para a vítima, impactando vários pilares da instituição, principalmente financeiramente. Quando o ataque DoS tem como origem diversas máquinas, dizemos que é um ataque DDoS (*Distributed Denial of Service*), com isso, o ataque pode se tornar muito mais abrangente, prejudicial e com potencial de causar graves danos.

## 4.3 PRINCIPAIS TIPOS DE INFRATORES VIRTUAIS

Existe a concepção de que o infrator virtual é chamado "*Hacker*", porém é um termo dado erroneamente, o certo para o que o indivíduo tentou dizer, deve ser "*Cracker*" (ULBRICH, 2004). Abaixo estão listados os principais tipos de infratores virtuais e suas nomenclaturas, que os classificam e definem, bem como *hackers*, *crackers*, *script kiddies*, *lammers*, *carders*, *cyberpunks* e *newbies*, dentre outros (CARMONA, 2002).

*Hacker* é um indivíduo que se dedica com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores. Graças a esses conhecimentos, um *hacker* frequentemente consegue obter soluções e efeitos extraordinários, que extrapolam os limites do funcionamento "normal" dos sistemas como previsto pelos seus criadores; incluindo, por exemplo, contornar as barreiras que supostamente deveriam impedir o controle de certos sistemas e acesso a certos dados. Muitos compartilham informações e colaboram em projetos comuns, incluindo congressos, ativismo e criação de software livre, constituindo uma comunidade hacker com cultura, ideologia e motivações específicas. Outros trabalham para empresas ou agências governamentais, ou por conta própria. *Hackers* foram responsáveis por muitas e importantes inovações na computação, incluindo a linguagem de programação C e o sistema operacional Unix (Kernighan e Ritchie), o editor de texto emacs (Stallman), o sistema GNU/Linux (Stallman e Torvalds) e o indexador Google (Page e Brin). *Hackers* também revelaram muitas fragilidades em sistemas de criptografia e segurança, como, por exemplo, urnas digitais (Gonggrijp, Haldeman), cédula de identidade com chip, bloqueio de telefones celulares etc.

Normalmente se considera como "*Hacker*", uma pessoa ou um grupo que ataca para causar danos ou ofensas a qualquer empresa, órgão do governo ou mesmo um computador pessoal. Embora a maneira de operar seja parecida, os objetivos desses gênios computacionais são distintos, cada qual com suas idealizações. Por isso, eles são divididos em categorias, sendo as principais:

- ***White Hat Hackers:*** Esses são considerados os *hackers* do bem. São especialistas em segurança, agindo para expor e resolver possíveis brechas e falhas nos sistemas das empresas que os contratam;
- ***Black Hat Hackers:*** Esses são os mal-intencionados, que invadem redes e computadores, criam vírus e *malwares* sempre com intenções não lícitas, como roubar senhas de bancos, dados confidenciais e outros;
- ***Hacktivists:*** Agem por motivos ideológicos. Eles são os principais responsáveis por quedas em sites de governos, órgãos e empresas multinacionais. Seu método principal de invasão é por meio de ataques DDoS.
- ***Crackers:*** *Cracker* é um termo usado para designar o indivíduo que pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por hackers em defesa contra o uso jornalístico do termo *hacker*. O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo *cracking*, pois havia certa confusão entre algumas pessoas, que se referiam pessoas que agiam de má fé, como sendo os *hackers*, sendo que o correto deveria ser *cracker*. Assim como os *hackers*, os *crackers* também possuem grande conhecimento voltado ao ramo da tecnologia. Crackers com bastante conhecimento, dificilmente serão encontrados, pois conseguem eliminar todos seus rastros, vestígios, tornando-se assim, "invisíveis". O ato de quebrar a segurança de um sistema, muitas vezes exige brilhantismo para se realizar e capacidade para explorar as vulnerabilidades conhecidas do sistema alvo com criatividade. Porém alguns, "erroneamente" definidos como crackers, utilizam-se de soluções conhecidas para problemas recorrentes em sistemas vulneráveis, copiando assim ou explorando falhas descobertas por outros sem qualquer esforço.
- ***Script Kiddies:*** Subcategoria de crackers. Não têm um alvo certo, vão tentando invadir tudo que vêm na frente e usam ferramentas encontradas na Internet. Tem um conhecimento digital bem acima dos usuários comuns, mas não sabem nem o básico de linguagens de programação, apenas pegam programas prontos e os utilizam para infectar determinados computadores.
- ***Lammers:*** Dificilmente aprendem a usar algum programa, não sabem e não tem condição de aprender como as coisas funcionam. Aqueles que chegam aos chats anunciando "vou te invadir, sou o melhor", mas desistem, pois não conseguem realizar nenhuma ação prejudicial, nem o básico do básico, ou seja, são aqueles que só ameaçam e sentem-se frustrados por não entenderem do assunto.
- ***Carders:*** É o especialista em fraudes com cartões de crédito. Sabem como conseguir listas de cartões válidos em sites que os utilizam (sites de compras, chat pago, qualquer site que tenha funcionalidades que sejam pagas de alguma forma etc.), geram números falsos que passam pela verificação e mesmo roubar e clonar cartões verdadeiros. Quando um cartão é clonado, o usuário do cartão não sai no

prejuízo, porém, até que descubra e tome as atitudes necessárias, várias compras já teriam sido realizadas, deixando sempre alguém com o prejuízo.

- ***Cyberpunks:*** São tecno-anarquistas que lutam pela manutenção da privacidade no ciberespaço através da difusão de programas de criptografia de massa. Tentam proteger o cidadão comum contra as tentativas governamentais e empresariais de esquadrinhar suas vidas a partir das pistas deixadas quando utiliza qualquer sistema eletrônico. O programa PGP (*Pretty Good Privacy*) criado por P. Zimmermann é um dos principais instrumentos utilizados pelos *cyberpunks*.
- ***Newbies:*** *Newbie* é o novato na rede. Ele se mete em lugares que não deve, faz perguntas que não deve. Neste nível encontram-se os primeiros usuários que utilizam programas desenvolvidos por *experts*, sem muito conhecimento sobre qualquer ética *hacker*, mas com conhecimento básico sobre o que é ser um, e só por diversão e/ou tentativa de reconhecimento social. É o segundo passo dado para seguir para a área *hacker*.

## 5 CONSIDERAÇÕES FINAIS

De forma geral, muitas empresas não sabem classificar as informações, tão pouco distinguir quais são os verdadeiros ativos que devem ser resguardados. Muitas organizações até os dias de hoje, investem bastante em máquinas, equipamentos de hardware, o que é importante, porém muitas vezes o ponto focal é ignorado, que é a parte lógica de todo o sistema, principalmente no quesito segurança.

Este artigo mostrou evidências dos principais tipos de *softwares* maliciosos (*Malware*), detalhando suas características e realçando a importância da prevenção.

Classificamos também, os principais tipos de infratores virtuais, pois ainda existem muitas pessoas que não sabem defini-los, ou definem generalizando todos como sendo *hackers*, como foi dito, esta nomenclatura vem sendo usada de forma incorreta na maioria dos casos.

Este artigo abordou a tecnologia que está em evidência no mercado tecnológico, tendência que é realidade e está presente em quase todos os setores de muitas empresas. Todavia, o fator de segurança computacional é primordial para que o *Cloud Computing* continue crescendo.

## REFERÊNCIAS


ULBRICH, Henrique Cesar. Universidade H4CK3R. São Paulo: Universo dos Livros, 2004.

CARMONA, Tadeu. Universo H4CK3R. São Paulo: Digerati Books, 2002.

SOSINSKY, Barrie. Cloud Computing Bible. 1 ed. Wiley, 2011.

HUGOS, Michael. HULITZKY, Derek. Business in the Cloud. 1 ed. Wiley, 2010.

RHODES-OUSLEY, Mark. Information Security the Complete Reference. 2 ed. MacGraw-Hill, 2013.

BOSWORTH, Seymour. Computer Security Handbook. 6 ed. Wiley, 2014.

MATHER, Tim. Cloud Computing and Privacy. 1 ed. O´Reilly Media, 2009.

TULLOCH, Mitch. Network Virtualization and Cloud Computing. 1 ed. Microsoft Press, 2014.

DAÚ, Gláucya Lima; SCAVARDA, Annibal; SCAVARDA, Luiz Felipe; PORTUGAL, Vivianne Julianelli Taveira (2019). *The Healthcare Sustainable Supply Chain 4.0: The Circular Economy Transition Conceptual Framework with the Corporate Social Responsibility Mirror*. Disponível em https://www.mdpi.com/2071-1050/11/12/3259. Acessado em 05/06/2024.

MAGRANI, Eduardo. A Internet das Coisas. 1. ed. Rio de Janeiro: Editora FGV, 2018.

MARQUESONE, Rosangela. *Big Data*: Técnicas e tecnologias para extração de valor dos dados. 1. ed. São Paulo: Editora Casa do Código, 2016.

MATARIC, Maja J. Introdução à Robótica. 1. ed. São Paulo: Editora Blucher, 2014.

NETTO, Antonio Valerio; BERTON, Lilian; TAKAHATA, André Kazuo. Ciência de dados e a inteligência artificial na área da saúde. 1. ed. São Paulo: Editora dos Editores, 2022.

NETTO, Antonio Valerio; NOVOA, Cláudia. Fundamentos em gestão e informática em saúde. 1. ed. São Paulo: UNIFESP, 2019.

SCAVARDA, Annibal; DAÚ, Gláucya Lima; SCAVARDA, Luiz Felipe; KORZENOWSKI, André Luís (2019a). *A proposed healthcare supply chain management framework in the emerging economies with the sustainable lenses: The theory, the practice, and the policy. Resour. Conserv. Recycl*. 141, 418–430. Disponível em https://doi.org/10.1016/j.resconrec.2018.10.027. Acessado em 11/06/2024.

SCAVARDA, Annibal; DAÚ, Gláucya Lima; SCAVARDA, Luiz Felipe; CAIADO, Rodrigo Goyannes Gusmão (2019b). *An Analysis of the Corporate Social Responsibility and the Industry 4.0 with Focus on the Youth Generation: A Sustainable Human Resource Management Framework*. Disponível em https://www.mdpi.com/2071-1050/11/18/5130. Acessado em 11/06/2024.

SCHWAB, Klaus. A Quarta Revolução Industrial. 1. ed. São Paulo: Edipro, 2018.

SOUZA, Thiago Antonio (2015). *Lean Healthcare*: Aplicação dos Conceitos de Gestão de Operações em Centros Cirúrgicos. Disponível em http://www.repositorio.jesuita.org.br/handle/UNISINOS/5157. Acessado em 06/06/2024.

STENDER, Gustavo Henrique Cordeiro (2016). *Lean Healthcare*: Modelo de Implantação da Ferramenta Kanban a um Almoxarifado de um Hospital Federal no Rio de Janeiro. Disponível em pppro.cefet-rj.br/T/376_Gustavo Henrique Cordeiro Stender.pdf. Acessado em 14/06/2024.

VILELA JUNIOR, Guanis de Barros; PASSOS, Ricardo Pablo. Inteligência Artificial nas Ciências da Saúde. 2. ed. Campinas: CPAQV, 2021.