Revista a EVOLUÇÃO

Ano IV n. 41 Jun. 2023
ISSN 2675-2573

FESTA JUNINA

Revista a E

A COMBATE AO RACISMO NAS UNIDADES EDUCACIONAIS DA REDE MUNICIPAL DE ENSINO DE SÃO PAULO: ESTRATÉGIAS E POSSIBILIDADES

Rafael Fernando da Silva Santos Fitipaldi

Filiada à: ABEC BRASIL Associação Brasileira de Editores Científicos

doi

Platform & workflow by OJS / PKP

CiteFactor Academic Scientific Journals

www.primeiraevolucao.com.br

Revista Primeira EVOLUÇÃO

Ano IV - nº 41 - Junho de 2023

ISSN 2675-2573

Uma publicação mensal da Edições Livro Alternativo

AUTORES(AS) DESTA EDIÇÃO

Andréa Godoy Miyashiro
Anildo Joaquim Da Silva
Célia Maria Batista
Diego Daniel Duarte dos Santos
Herbert Madeira Mendes
Joseneide dos Santos Gomes
Luís Filipe Narciso
Miriam Ferreira
Nayane Brito Veras Godinho Hermisdorf
Priscila Paula da Costa da Silva
Rafael Fernando da Silva Santos Fitipaldi
Viviane de Cássia Araujo

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Primeira Evolução [recurso eletrônico] / [Editor] Antonio Raimundo Pereira Medrado. – ano 4, n. 41 (jun. 2023). – São Paulo : Edições Livro Alternativo, 2023.
134 p. : il. color

Bibliografia
Mensal
ISSN 2675-2573 (on-line)
Modo de acesso: https://primeiraevolucao.com.br
DOI 10.52078/issn2673-2573.rpe.41

1. Educação – Periódicos. 2. Pedagogia – Periódicos. I. Medrado, Antonio Raimundo Pereira, editor. II. Título.

CDD 22. ed. 370.5

Patrícia Martins da Silva Rede – Bibliotecária – CRB-8/5877

ACESSOS: https://primeiraevolucao.com.br https://doi.org/10.52078/issn2673-2573.rpe.41

São Paulo | 2023

Revista PRIMEIRA EVOLUÇÃO

ISSN: 2675-2573
Publicação Mensal

Contatos
Tel. 55(11) 99543-5703
Whatsapp: 55(11) 99543-5703
primeiraevolucao@gmail.com (S. Paulo)
netomanuelfrancisco@gmail.com (Luanda)
https://primeiraevolucao.com.br

Publicada no Brasil por:
Edições Livro Alternativo
CNPJ: 28.657. 494/0001-09
Colaboradores voluntários em:

A revista PRIMEIRA EVOLUÇÃO é um projeto editorial criado pela **Edições Livro Alternativo** para ajudar e incentivar professores(as) a publicarem suas pesquisas, estudos, vivências ou relatos de experiências.

Seu corpo editorial é formado por professores/as especialistas, mestres/as e doutores/as que atuam na rede pública de ensino, e por profissionais do livro e da tecnologia da informação.

Uma de suas principais características é o fato de ser **independente e totalmente financiada por professoras e professores**, e de distribuição gratuita.

PROPÓSITOS:

Rediscutir, repensar e refletir sobre os mais diversos aspectos educacionais com base nas experiências, pesquisas, estudos e vivências dos profissionais da educação;

Proporcionar a publicação de livros, artigos e ensaios que contribuam para a evolução da educação e dos educadores(as);

Possibilitar a publicação de livros de autores(as) independentes;

Promover o acesso, informação, uso, estudo e compartilhamento de sofwares livres;

Incentivar a produção de livros escritos por professores/as e autores independentes;

Financiar (total ou parcialmente,) livros de professoras/es e estudantes da rede pública.

PRINCÍPIOS:

Os trabalhos voltados para a **educação, cultura** e produções independentes;

O uso exclusivo de **softwares livres** na produção dos livros, revistas, divulgação etc;

A ênfase na produção de **obras coletivas** de profissionais da educação;

Publicar e divulgar **livros de professores(as)** e autores(as) independentes;

O respeito à **liberdade e autonomia** dos autores(as);

O combate ao despotismo, ao preconceito e à superstição;

O respeito à **diversidade**.

Esta revista é mantida e financiada por professoras e professores.
Sua distribuição é, e sempre será, livre e gratuita.

Produzida com utilização de softwares livres

FREE SOFTWARE FOUNDATION

debian LibreOffice OJS OPEN JOURNAL SYSTEMS

Filiada à:

ABEC BRASIL Associação Brasileira de Editores Científicos

doi

Platform & workflow by OJS / PKP

Google Acadêmico

CiteFactor Academic Scientific Journals

www.primeiraevolucao.com.br

A educação evolui quanto mais evoluem seus profissionais

SUMÁRIO

ARTIGOS

ARTIGOS

* *Destaque*

PRINCIPAIS AMEAÇAS DE SEGURANÇA DE INFORMAÇÃO E FORMAS DE MITIGAÇÃO

Anildo Joaquim Da Silva

RESUMO

A Computação em Nuvem ou Cloud Computing, é um modelo para virtualização de recursos, gestão de negócios e venda de serviços pela internet. Este artigo tem como objectivo analisar as principais ameaças e as possíveis formas de mitigação, mas antes, porém, descreve-se os pilares básicos da segurança de informação, nomeadamente: Confidencialidade, Integridade, Disponibilidade, Autenticidade, Irretratabilidade, Conformidade e Segurança Física. Estudar a nuvem hoje, um dos maiores desafios do século na área de tecnologia, pela sua complexidade, no ponto de vista de infraestrutura e da sua segurança. Toda organização que optar na computação das nuvens, a segurança deve ser vista como o elemento fulcral ou ponto de partida para o sucesso do seu negócio, por se tratar de um modelo que cuida de dados sensíveis e compartilhados entre terceiros, para que possam ter uma gestão de recursos segura e eficiente.

Palavras-chave: Autenticidade; Computação em Nuvem; Confidencialidade; Infraestrutura; Organização.

INTRODUÇÃO

Hoje, conectar-se a internet, passa a ser uma condição obrigatória para as organizações, e estar na nuvem é imprescindível para maior visibilidade, facilidade e disponibilidade dos recursos e serviços pela internet. Segundo (TOTVS, 2022), a computação em nuvemé um modelo de entrega de serviços digitais pela internet. Eles podem ser tanto infraestruturas inteiras, plataformas de desenvolvimento ou aplicações de softwares. Outrossim, não se pode falar de nuvem, sem pensar na sua segurança. Segurança da computação em Nuvem, tem a ver com a protecção dos recursos e serviços disponibilizados em online.

Segundo (Barbieri, 2019), a segurança da informação na nuvem são segredos comerciais, know-how técnico ou informações sobre clientes e preços são a base de muitas organizações. A protecção dessas informações é uma tarefa importante, sendo a principal preocupação a protecção contra perda e uso indevido de dados. Por essas razões, a protecção de informações confidenciais é de grande importância para proteger as corporações de danos económicos, sendo o objecto da segurança da informação.

Segundo Kinsta, a segurança na nuvem é uma complexa interação de tecnologias, controles, processos e políticas. Uma prática altamente personalizada de acordo com os requisitos únicos de sua organização. Todas as organizações devem ter um sistema de Gestão de Indenidade e Acesso (IAM) para controlar o acesso à informação. O seu fornecedor da nuvem irá integrar-se directamente com o seu IAM ou oferecer o seu próprio sistema integrado. Um IAM combina autenticação multi-factor e políticas de acesso de utilizador, ajudando-o a controlar quem tem acesso às suas aplicações e dados, o que podem aceder e o que podem fazer aos seus dados (Kinsta, 2022).

Segundo a Microsoft, a segurança da nuvem é uma disciplina da segurança cibernética que foca em proteger dados e sistemas em nuvem de ameaças internas e externas, incluindo melhores práticas, políticas e tecnologias que ajudam organizações a evitar acesso não autorizado e vazamento de dados (Microsoft, 2023).

CONCEITOS DE AMEAÇAS, ATAQUES, RISCOS E VULNERABILIDADE

AMEAÇAS

Ameaças são a causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização. Um Script Kiddie por exemplo é um agente ameaçador que geralmente representa um risco muito baixo para organizações que possuem o mínimo de maturidade em Segurança da informação. Script Kiddies são indivíduos que não têm o conhecimento técnico para desenvolver scripts ou descobrir novas vulnerabilidades em software, mas que têm conhecimento suficiente dos sistemas de computação para ser capaz de baixar e executar scripts que outros desenvolveram e a partir desse ponto tentar explorar vulnerabilidades conhecidas (Paula, 2022). As ameaças exploram vulnerabilidades que por consequência aumentam os Riscos e a exposição não desejada da informação.

Ameaças é qualquer coisa que possa explorar uma vulnerabilidade, intencional ou acidental, para obter, danificar ou destruir um activo.

ATAQUES

Ataques são tentativas de destruir, expor, alterar, inutilizar, roubar ou obter acesso não autorizado, ou fazer uso não autorizado de um activo ou sistema (Paula, 2022). Para exemplificar esse conceito: ataque DDoS (que significa Negação Distribuída de Serviço (denial of service – DoS e distributed denial of service)) é um ataque distribuído de negação de serviços. Sendo bem breve ele se utiliza de vários dispositivos que foram anteriormente infectados e que agora podem ser utilizados como bots (robôs) para gerar uma grande quantidade de requisições em um alvo determinado e sobrecarrega-lo até o esgotamento dos seus recursos de memória e processamento fazendo o mesmo ficar indisponível para acesso.

RISCOS

De acordo com a ISO 27001: Riscos de Segurança da Informação podem ser expressos como o efeito da incerteza sobre os objectivos de Segurança da Informação. Risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade (Paula, 2022).

Risco: o potencial de perda, dano ou destruição de um activo como resultado de uma ameaça que explora uma vulnerabilidade. Risco é uma possibilidade de corromper um activo, através de ameaças e vulnerabilidades.

VULNERABILIDADE

Vulnerabilidadeé uma Fragilidade em um activo ou grupo de activos, que pode ser explorado por uma ou mais ameaças. Ameaças e agentes ameaçadores estão constantemente tentando explorar essas fragilidades em busca de adquirir algum tipo de acesso não autorizado (Paula, 2022). Um exemplo de vulnerabilidade bem actual é o **Log4j**. O Log4j é uma biblioteca do Apache que ajuda desenvolvedores a fazer o que é chamado de "logging", um processo que permite guardar registos de interações, envio de informações, processamento de dados e resultados de uma determinada acção. A falha na Log4j permite que um hacker insira código activo no processo de registo. Esse código, então, diz para o servidor que armazena o software executar um comando que o hacker deseja, que pode variar de acordo com as intenções de quem ataca. Segundo a Tenable, empresa especialista em Cyber Exposure, o problema com o Log4j é considerado crítico porque explorá-lo é relativamente simples. A brecha permite que o invasor remoto não autenticado realize um ataque à popular biblioteca de logApache Log4j, utilizada por vários serviços muito populares como iCloud, Amazon e Tesla.

Vulnerabilidades: fraquezas ou buraco em um programa de segurança que podem ser exploradas por ameaças para obter acesso não autorizado a um activo. Ou seja, uma vulnerabilidade é uma fraqueza ou falha em nossos esforços de protecção.

PILARES DA SEGURANÇA DA INFORMAÇÃO

Segundo a (Netsupport, 2022), os pilares são seis (6), e para (Gatinfosec), os pilares são cinco (5), e pra nós, os pilares são sete (7). Portanto a segurança da informação moderna se apoia, basicamente, em sete pilares fundamentais, abaixo mencionados:

1. CONFIDENCIALIDADE

O conceito se relaciona com o ideal de privacidade das informações, isto é, da restrição do acesso. A segurança da informação, nesse ponto, é pensada e implantada para garantir o total sigilo de dados sensíveis, evitando que acções maliciosas possam expor o seu conteúdo e causar prejuízos para a organização.

2. INTEGRIDADE

A integridade está associada à confiabilidade dos dados, ou seja, por esse viés, o foco maior está em garantir que as informações se mantenham exactas, livre de alterações e possam ser empregadas de maneira eficiente pela organização.

3. DISPONIBILIDADE

Para que um sistema de informação seja útil, é fundamental que seus dados estejam disponíveis sempre que necessário. Logo, a disponibilidade é mais um pilar da segurança da informação, que garante o acesso em tempo integral (24/7) pelos usuários finais.

Para cumprir esse requisito, é precisa garantir aestabilidade e acesso permanente às informações dos sistemas, por meio de processos de manutenção rápidos, eliminação de falhas de software, actualizações constantes e planos para administração de crises.

Vale lembrar que os sistemas são vulneráveis a desastres naturais, ataques de negação de serviço, blecautes, incêndios e diversas outras ameaças que prejudicam sua disponibilidade.

Actualmente, como as organizações estão se valendo cada dia mais de sistemas de informação, qualquer ruptura na disponibilidade deles pode inviabilizar decisões, contratos, vendas e outras acções necessárias, além de prejudicar a relação com o cliente.

4. AUTENTICIDADE

A fim de garantir que as informações sejam provenientes de uma fonte confiável foi estabelecido o pilar de autenticidade. Para isso, é preciso manter um registo do autor de determinada informação, a fim de atestar sua veracidade. Ou seja, A autenticidade é o pilar que valida a autorização do usuário para acessar, transmitir e receber determinadas informações. Seus mecanismos básicos são logins e senhas, mas também podem ser utilizados recursos como a autenticação biométrica, por exemplo. Esse pilar confirma a identidade dos usuários antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por terceiros.

5. IRRETRATABILIDADE

Também chamado de “não repúdio”, do inglês non-repudiation, esse pilar é inspirado no princípio jurídico da irretratabilidade. Esse pilar garante que uma pessoa ou entidade não possa negara autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrónicos. Na gestão da segurança da informação, isso significa ser capaz de provaro que foi feito, quem fez e quando fez em um sistema, impossibilitando a negação das acções dos usuários.

6. CONFORMIDADE

A segurança da informação também deve assegurar que seus processos obedeçam as leis e normas regulamentadas. Por conta disso, foi também estabelecido o pilar da conformidade, garantindo que sejam seguidos os devidos protocolos, dentro do sector

Para além dos seis pilares já frisados e bem conhecidos, é necessário incorporal a segurança física, (nosso ponto de vista), como sendo o sétimo pilar base da segurança de informações, atendendo as características que este apresenta, razão pela qual, o realçamos. Sugerimos as organizações que padronizam as normas de segurança (**ISO/IEC 17799:2005 e ABNT NBR ISO/IEC 27002:2013**), no sentido de incorporarem este, como sendo um dos pilares fundamentais também.

7. SEGURANÇA FÍSICA

Segundo Kinsta, a Segurança Física é outro pilar da segurança nas nuvens. É uma combinação de medidas para evitar o acesso directo e a interrupção do hardware alojado no datacenter do seu provedor de cloud computing. A segurança física inclui o controle do

acesso directo com portas de segurança, fontes de alimentação ininterruptas, Circuito Fechado de Televisão (CCTV ou CFTV), alarmes, filtragem de ar e partículas, protecção contra incêndios, e muito mais (Kinsta, 2022).

Segundo Silva e Schimiguel, a segurança física surgiu da necessidade do ser humano em proteger o acesso aos seus bens. Esse tipo de segurança evoluiu ao ponto de ser aplicado na área de tecnologia da informação devido a necessidade em se guardar os dados contidos nos equipamentos de hardware com o objectivo de proteger as informações salvas nesses equipamentos. Além de proteger os equipamentos e as informações contra acesso não autorizado, limitando o acesso a esses recursos de forma que somente pessoal treinado, capacitado e autorizado possa manuseá-los, a segurança física também tem como propósito evitar danos materiais, pois com a limitação de acesso, a confiabilidade da guarda da informação se torna bem maior (Silva & Schimiguel, 2017).

A Segurança Física deve constar na lista dos pilares de segurança de informação já existentes, por tratar-se da base de todo equipamento que permite o armazenamento de dados, interligação do hardware e as condições para a comunicação entre dispositivos. Se por ventura, existir alguma falha nos equipamentos, a probabilidade de quebra de comunicação ou perda de dados é maior. Por isso, devemos assegurar todo e qualquer equipamento informático, existente na organização.

PRINCIPAIS AMEAÇAS DE SEGURANÇA NA COMPUTAÇÃO DAS NUVENS

Segundo a Microsoft, para se manterem competitivas, as organizações devem continuar usando a nuvem para iterar rapidamente e facilitar o acesso a serviços para funcionários e clientes, além de, ao mesmo tempo, proteger dados e sistemas das ameaças (Microsoft, 2023).

De acordo com o estudo feito por nós e segundo a (Kaspersky, 2023) e a (Microsoft, 2023), as principais ameaças da segurança na computação das nuvens, estão classificadas da seguinte forma:

1. AMEAÇAS INTERNAS

O erro humano é um grande responsável por violações de segurança. Configurações incorretas podem criar abertura para infractores e, muitas vezes, os funcionários clicam em links inválidos ou movem dados acidentalmente para locais com menos segurança.

As ameaças de usuários confiáveis são tão sérias na nuvem quando nos sistemas locais. Essas pessoas podem ser funcionários actuais ou antigos, contratados ou um parceiro de negócios confiável: qualquer pessoa que não precise romper as defesas da organização para acessar os seus sistemas.

Um usuário não precisa ter intenção maliciosa para causar danos. Todos os incidentes relatados são causados por negligência de colaboradores ou contratados. Essa negligência pode incluir servidores mal configurados, armazenamento de dados confidenciais em dispositivos pessoais ou phishing.

2. AMEAÇAS EXTERNAS

Causadas quase que exclusivamente por agentes maliciosos, muitas vezes, os invasores usam campanhas de phishing para roubar senhas de funcionários e obter acesso a sistemas e activos corporativos de valor, como também malware e ataques de DDoS (que significa Negação Distribuída de Serviço (denial of service – DoS e distributed denial of service)).

As ameaças externas, sempre são provenientes de agentes ou invasores externos (Hackers ou Crakers), que o seu objectivo principal, é somente, tirar proveito nas organizações que apresentem vulnerabilidades, ou seja, invadir e corromper o sistema, extrair dados, vazar informações ou roubar senhas dos usuários do sistema para comprometer a organização.

3. VIOLAÇÃO DE DADOS

As violações de dados continuam sendo uma das principais preocupações de segurança em nuvem, já que essas ameaças podem causar grandes danos financeiros e à reputação das orgainizações. Podem, ainda, resultar em perda da propriedade intelectual e responsabilidades legais significativas.

4. CONFIGURAÇÕES INCORRETAS

Essa é uma ameaça nova, mas não surpreendente, já que há diversos exemplos de organizações que expõem dados acidentalmente através da nuvem. Um deles é a Exactis, que deixou um banco de dados contendo informações pessoais de 230 milhões de consumidores norte-americanos por configurações incorretas.

5. FALTA DE ARQUITECTURA E ESTRATÉGIA DE SEGURANÇA

Esse problema é tão antigo quanto a nuvem. O desejo de minimizar o tempo necessário para migrar sistemas e dados para a nuvem geralmente tem precedência sobre a segurança. Como resultado, a organização acaba utilizando infraestrutura e estratégias de segurança que não foram projectadas para a nuvem.

6. INTERFACES E APIS INSEGURAS

As Interfaces de Programação e Aplicação (APIs) inseguras são um vector de ataque comum, como o Facebook bem sabe. Em 2018, a rede social sofreu uma violação que afectou mais de 50 milhões de contas. Especialmente quando associadas a interfaces de usuário, as vulnerabilidades das APIs podem fornecer aos invasores um caminho simples para o roubo de credenciais de usuários ou funcionários.

7. PLANO DE CONTROLE FRACO

Um plano de controle abrange processos de duplicação, migração e armazenamento de dados. As partes interessadas no controle precisam entender as configurações de segurança, como os dados fluem e os seus pontos fracos. Não ter essa prática pode resultar em vazamentos de informações, indisponibilidade se dados ou corrupção das informações.

8. FALHAS NA ESTRUTURA

A meta-estrutura de um provedor de serviços de nuvem mantém as informações de segurança sobre como protege os seus sistemas – e divulga essas informações por meio de chamadas de Interface de Programação e Aplicação (API). As APIs ajudam os clientes a detectar acessos não autorizados, mas também contêm informações altamente confidenciais, como logs ou dados do sistema de auditoria.

Essa linha também é um ponto de falha em potencial, podendo permitir que os invasores acessem os dados. A má implementação da Interface de Programação e Aplicação (API) geralmente é a causa das vulnerabilidades.

Os clientes, por outro lado, podem não atender como implementar os aplicativos na nuvem. Essa questão é particularmente verdadeira quando conectam aplicações que não foram projectadas para ambientes de nuvem.

9. VISIBILIDADE LIMITADA

Uma reclamação comum entre os profissionais de segurança é que um ambiente em nuvem os torna cegos para a maioria dos dados necessários para detectar e impedir actividades suspeitas. Os especialistas dividem esse desafio em duas categorias: uso não autorizado de aplicativos e uso indevido de aplicativos sancionados.

Qualquer aplicativo que não atenda às diretrizes corporativas de segurança representa um risco desconhecido pela equipa. Já o uso indevido envolve a utilização de aplicativos aprovados por pessoas autorizadas ou cibercriminosos com credenciais roubadas. Nesse cenário, as equipas de segurança devem saber a diferença entre usuários, detectando comportamentos anormais.

10. INVASÕES DE CONTA

O sequestro ou invasão de contas continua sendo uma das principais ameaças à nuvem. Conforme as tentativas de phishing se tornam mais eficazes e direcionadas, os riscos de um invasor obter acesso a contas privilegiadas é significativo. Vale destacar que o phishing não é a única maneira de um cibercriminoso obter credenciais. Eles também podem adquiri-las comprometendo o próprio serviço de nuvem.

11. ABUSO

Os cibercriminosos estão cada vez mais usando serviços de nuvem legítimos para apoiar as suas actividades. Por exemplo, eles podem usar um serviço de nuvem para hospedar malwares disfarçados, lançar ataques DDoS, disparar emails de phishing, minerar moedas virtuais ou realizar ataques para roubar credenciais.

Para os especialistas, os provedores de serviços de nuvem devem adoptar medidas para mitigar os riscos e detectar abusos, como fraudes em ferramentas de pagamento ou uso indevido dos serviços. Também é importante que os provedores tenham uma estrutura de resposta a incidentes para permitir que os clientes façam denúncias.

13. ATAQUES A SOFTWARES E APLICAÇÕES POR MEIO DE VÍRUS, MALWARES, WORMS, RANSOMWARES E CAVALOS DE TROIA;

Os softwares e aplicativos são muitas vezes os visados de ataques com facilidades, por serem usados por qualquer pessoa, mesmo não experiente em Tecnologia de Informação e Comunicação (TIC) ou Tecnologia de Informação (TI). Por exemplo temos Ransomware é um malware que criptografa os arquivos da vítima, seja uma pessoa física ou uma organização. Assim, o titular dos dados e arquivos não consegue mais acessar essas informações, apenas mediante pagamento ao hacker. É um tipo de ameaça que, literalmente, sequestra dados. Uma vez que a organização caia no golpe, ela recebe instruções para realizar o resgate — que normalmente deve ser feito em alguma criptomoeda.

14. ATAQUES DOS E DDOS

Os ataques DDoS (que significa Negação Distribuída de Serviço (denial of service – DoS e distributed denial of service)), são uma ameaça comum que ocorre quando um hacker inunda sua rede, serviço ou servidor com tráfego (diversos computadores simultâneos) para interromper suas operações. Essas ameaças são lançadas com pacotes de dados, solicitações de conexões ou mensagens falsas. Tudo isso afecta sua conexão, que fica muito lenta. À princípio, esse tipo de ataque parece não representar muitos riscos.

FORMAS DE MITIGAÇÃO DAS PRINCIPAIS AMEAÇAS

Segundo a Aiqon, a cloud computing é um modelo complexo, principalmente quando se fala de segurança, por isso, precisa de um gerenciamento apropriado do acesso e é essencial para minimizar o risco de perda de dados por conta de ataques externos, infiltradores e erros como compartilhamento acidental de dados sensíveis (Aiqon, 2020). Por estes e outros motivos, o Aiqon, descreve (abaixo) uma série de formas para mitigação das principais ameaças de segurança na nuvem:

1. Treinamento de funcionários na navegação segura, hábitos de download e invasão de contas;
2. Desenvolva políticas de permissão e uso da nuvem em toda a organização;
3. Desprovisionar acesso a recursos imediatamente sempre que tiver alteração de funcionários;
4. Implemente a governança de acesso aos dados;
5. Assegurar a infraestrutura de rede com um web application firewall;
6. Implementar filtro de conteúdo;
7. Usar o balanceamento de carga para identificar possíveis inconsistências no tráfego;
8. Soluções avançadas de antivírus, deve-se instalar antivírus actualizados e pagos (não se recomenda o gratuito);
9. Backups de dados feitos de forma regular e compreensiva;
10. Implemente a análise de comportamento do usuário. Crie um baseline de perfil comportamental para cada usuário e procure por acções atípicas para esse usuário e outros da mesma função. Remova contas e credencias inutilizadas e rastreie tentativas

de acesso a contas desabilitadas, junto com outras tentativas suspeitas de acesso a dados ou ganho de permissões elevadas;

11. Monitore usuários privilegiados. Rastreie as contas de serviço e privilegiadas separadamente das outras contas de usuário. Essas contas devem ser usadas para tarefas especificas que outras contas não têm permissão o suficiente para realizar;

12. Use o monitoramento de alterações continuamente para detectar alterações suspeita e investiga-las de imediato. Tenha certeza de que as quais configurações foram modificadas, quem as fez e quando e onde isso aconteceu;

13. Implemente controle de acesso e identidade;

14. Permita apenas senhas fortes, devem ter números, letras e caracteres;

15. Identifique e revogue acessos excessivos a informação sensível;

16. Habilite logs centralizados para tornar fácil para os investigadores o acesso a logs durante um incidente;

17. Implemente uma política de prevenção a perda de dados (DLP);

18. Terceirize a detecção de violação usando um corretor de segurança de acesso à nuvem (CASB) para analisar as actividades de saída;

19. Estabeleça um baseline de configurações e conduza regularmente uma auditoria de configuração para verificar se está havendo um afastamento do baseline;

20. Implementar a tecnologia de descobrimento e classificação de dados. Identificar todos os dados críticos para o negócio e sensíveis que tens; saber quais usuários, contratantes e parceiros tem acesso a eles; monitorar suas actividades a procura de sinais de tendências de actividade suspeita, como um número grande de falhas de tentativa de acesso. Estar ciente das actividades do usuário ao redor dos dados sensíveis e críticos para o negócio te ajuda a identificar operações maliciosas antes delas causarem dano real.

As formas de mitigação das principais ameaças de segurança na computação das nuvens, são técnicas aplicáveis para minimizar ou impedir qualquer ataque que posso surgir durante a gestão ou distribuição dos serviços em online. Das 20 formas de mitigação acima exposto, a aplicação varia em função o tipo de ataque que se deseja impedir. Razão pela qual, as organizações devem estudar profundamente os possíveis ataques que possam surgir e vulnerabilidades que os sistemas podem apresentar. É de lembrar que, a segurança de informações deve sempre estar em primeiro lugar, em qualquer actividade de Tecnologia de Informação e Comunicação (TIC) ou Tecnologia de Informação (TI).

CONSIDERAÇÕES FINAIS

Segundo a nossa pesquisa, concluímos que existem sete (7) pilares de segurança de informação, nomeadamente: Confidencialidade, Integridade, Disponibilidade, Autenticidade, Irretratabilidade, Conformidade e Segurança Física;

A segurança de informação é o ponto de partida para qualquer serviço ou negócio digital. E a computação em nuvem, não foge a regra, pela sua complexidade, carece de

estudos mais profundos de segurança, no sentido de garantir maior segurança aos próprios provedores de serviços e aos clientes;

As ameaças na computação das nuvens são os principais inimigos do gerenciamento e venda de serviços pela internet. Todavia, devem se ter em conta as tecnologias mais avançadas para que ajudem na mitigação o mais rápido possível, pelos profissionais de Tecnologia de Informação (TI), para evitar danos incalculáveis aos serviços de nuvem.

Os provedor de serviços em nuvem oferecem hardware e software de segurança em nuvem de última geração, para salvaguardar os dados e serviços dos clientes da melhor forma possível;

Os riscos de ataques cibernéticos na computação das nuvens, podem ser reduzidos através de tecnologias avançadas, gerenciamento a altura, treinamento contínuo de funcionários e clientes, principalmente sobre a técnica de phishing.

REFERÊNCIAS BIBLIOGRÁFICAS

Aiqon. (2020). S**egurança no Cloud: Como Mitigar os Principais Problemas**. Obtido de https://aiqon.com.br/blog/as-6-principais-ameacas-na-computacao-na-nuvem-e-como-mitiga-las/

Barbieri, C. (2019). **Governança de Dados: Práticas, conceitos e novos caminhos**. São Paulo.

Gatinfosec. (s.d.). **Pilares da Segurança da Informação**. Obtido de https://www.gatinfosec.com/blog/5-pilares-da-seguranca-da-informacao/

Kaspersky. (2023). **Segurança na Nuvem**. Obtido de https://www.kaspersky.com.br/resource-center/definitions/what-is-cloud-security

Kinsta. (16 de 11 de 2022). **Como funciona a cloud security?** Obtido de https://kinsta.com/pt/blog/cloud-security/

Microsoft. (2023). **Segurança na Nuvem**. Obtido de https://www.microsoft.com/pt-br/security/business/security-101/what-is-cloud-security

Netsupport. (2022). **Pilares da Segurança de Informação**. Obtido de https://netsupport.com.br/pilares-seguranca-da-informacao#:~:text=Tradicionalmente%2C%20a%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o,ou%20n%C3%A3o%20rep%C3%BAdio)%20e%20conformidade.

Paula, A. D. (14 de Fevereiro de 2022). **Conceitos de Ameaças e Riscos em Segurança de Informação**. Obtido de https//pt.linkedin.com/pulse/entendendo-na-prática-os-conceitos-de-ameaça-e-risco-albert

Silva, G. F., & Schimiguel, J. (03 de 2017). **Segurança em Ambiente de TI**. Obtido de https://www.eumed.net/cursecon/ecolat/br/17/jundiai.html

TOTVS, E. (11 de Fevereiro de 2022). **Computação em Nuvem: Aplicações, Tipos e Vantagens.** Obtido de HTTPS://WWW.TOTVS.COM/BLOG/NEGOCIOS/COMPUTACAO-EM-NUVEM/

Anildo Joaquim da Silva - Docente no Instituto Superior Politécnico Internacional de Angola, ISIA, na Faculdade de Engenharia, Benfica-Luanda. Mestrando em Engenharia Informática, na Especialidade de Gestão de Redes de Computadores e Sistemas de Comunicação, na Faculdade de Engenharia e Novas Tecnologias, Universidade Gregório Semedo, Talatona, Luanda – Angola.

ORGANIZAÇÃO:
Manuel Francisco Neto
Vilma Maria da Silva

AUTORES(AS):

Andréa Godoy Miyashiro
Anildo Joaquim Da Silva
Célia Maria Batista
Diego Daniel Duarte dos Santos
Herbert Madeira Mendes
Joseneide dos Santos Gomes
Luís Filipe Narciso
Miriam Ferreira
Nayane Brito Veras Godinho Hermisdorf
Priscila Paula da Costa da Silva
Rafael Fernando da Silva Santos Fitipaldi
Viviane de Cássia Araujo

ISSN 2675-2573 41

https://doi.org/10.52078/issn2673-2573.rpe.41

Produzida com utilização de softwares livres

FREE SOFTWARE FOUNDATION

debian LibreOffice

Platform & workflow by OJS / PKP

www.primeiraevolucao.com.br

ABEC BRASIL Associação Brasileira de Editores Científicos · doi · Crossref · OJS Open Journal Systems · CiteFactor Academic Scientific Journals · Google Acadêmico