Revista Multidisciplinar do Nordeste Mineiro, v.06,2024
ISSN 2178-6925

VAZAMENTO DE DADOS NO AMBIENTE HOSPITALAR: AVALIAÇÃO DOSRISCOS, IMPACTOS E MEDIDAS DE MITIGAÇÃO.

TITLE: DATA LEAKAGE IN THE HOSPITAL ENVIRONMENT: ASSESSMENT OFRISKS, IMPACTS AND MITIGATION MEASURES.

Jaqueline de Jesus Santos
Graduada em Direito, Faculdade de Ensino Superior de Linhares, Brasil
Email:jaquelinesantosdejesus99@gmail.com

Matheus Lopes da Silva
Mestre, Faculdade de Ensino Superior de Linhares, Brasil
E-mail:matheus.silva@csc.ufsc.edu.br

Resumo

O vazamento de dados no ambiente hospitalar é uma preocupação crescente devido ao uso crescente de tecnologias digitais para armazenar e compartilhar informações de pacientes. Este artigo analisa os riscos associados ao espalhamento de informações em hospitais, seus impactosna segurança dos pacientes e nas operações hospitalares, e discute medidas de mitigação para prevenir tais incidentes. Utilizando uma abordagem de revisão sistemática da literatura, examinamosestudos recentes sobre divulgações de bases em hospitais e destacamos as lacunas existentes na pesquisa. Além disso, propomos diretrizes para fortalecer a segurança da informação em ambientes hospitalares e reduzir a probabilidade de exposições de elementos.
Palavras-chave: Vazamento de dados, segurança da informação, hospital, privacidade do paciente, mitigação de riscos.

Abstract

Data leakage in the hospital environment is a growing concern due to the increasing use of digital technologies to store and share patient information. This article analyzes the risks associated with the spread of information in hospitals, its impacts on patient safety and hospital operations, and discusses mitigation measures to prevent such incidents. Using a systematic literature review approach, we examine recent studies on hospital base disclosures and highlight existing gaps in the research. Additionally, we propose guidelines to strengthen information security in hospital environments and reduce the likelihood of element exposures.

Keywords: Data leak, information security, hospital, patient privacy, risk mitigation.

1. Introdução

No entanto, juntamente com os avanços tecnológicos, surgem desafios substanciais relacionados com a segurança da informação e a proteção da privacidade dos pacientes. O vazamento de dados emerge como uma ameaça crítica, colocando em risco a segurança dos pacientes e comprometendo a confidencialidade de suas informações médicas. Esses espalhamentos podem ocorrer devido a vulnerabilidades nos sistemas de informação hospitalar, ataques cibernéticos, acesso não autorizado de funcionários ou erro humano. As consequências de tais divulgações podem ser devastadoras, incluindo danos à proteção da instituição de saúde, perda de confiança do paciente, exposição a fraudes médicas e proteção de regulamentos de privacidade de bases.

A LGPD (Brasil, 2018) estabelece princípios e normas que devem ser seguidos por empresas e profissionais que coletam e processam dados pessoais, incluindo os profissionais de saúde que lidam com prontuários médicos. Outro aspecto relevante da lei é a adoção de medidas de segurança adequadas para proteger as informações pessoais. Os estabelecimentos de saúde devem garantir que o acesso aos prontuários médicos seja restrito apenas aos profissionais autorizados, utilizando sistemas seguros para o armazenamento e a transmissão de informações sensíveis. Esse arcabouço legal representa um amparo no que se refere ao uso inadequado de dados e ao vazamento de informações pessoais sensíveis, sobretudo na área da saúde, onde as consequências do acesso não autorizado podem ser devastadoras.

A análise cuidadosa da novel legislação de proteção de dados e a sua aplicação aos casos como o de Klara Castanho são fundamentais para garantir a proteção dos direitos dos pacientes e a integridade dos profissionais envolvidos no tratamento de dados pessoais sensíveis na área da saúde. Portanto, este estudo busca analisar as responsabilidades legais e éticas dos profissionais de saúde no contexto da proteção de dados, com o objetivo de contribuir para uma prática mais segura e consciente no contexto da LGPD (Brasil, 2018)

As divulgações de dados é uma problemática que preocupa a diversos setores do mercado que passaram pelo processo de automatização e de adoção de tecnologias para o armazenamento de dados, pois coloca em risco a segurança dos pacientes, expondo a confidencialidade das informações médicas destes. Estas divulgações podem ocorrer por uma série de razões, incluindo erros humanos, violações de segurança cibernética e uso incorreto de informações por parte de funcionários e de prestadores de serviços.

Além disso, o principal objetivo desse trabalho é apresentar dados e desafio do cenário atual: analisar o tratamento conferido pela LGPD à proteção de dados relativos à saúde Avaliação dos Riscos, Impactos e Medidas de Mitigação, objetivando também investigar quais são as causas de publicação de elementos de ambiente hospitalar; Investiga as vulnerabilidades nos sistemas de informação e o que leva criminosos a se apossar dos dados vazados; Considerar as consequências que os difusão de bases podem causar tanto para o paciente quanto para o hospital lesado; e debater medidas cabíveis para evitar tais acontecimentos.

2. Aplicação da Lei Geral De Proteção De Dados Pessoais (LGPD), Lei N°13.709/18.

Assim como garantir na Lei Geral de Proteção de Dados no Art.1° da Lei n° 13.709, de 14 de agosto de 2018 (LGPD) representa um marco importante na legislação brasileira no que diz respeito à proteção de dados pessoais, e suas implicações no ambiente hospitalar são significativas. Essa lei, que entrou em vigor em setembro de 2020, tem como objetivo principal garantir a privacidade e a segurança das informações pessoais, inclusive aquelas relacionadas à saúde, e tem um impacto profundo nas práticas de tratamento de noções em hospitais e clínicas de saúde. (Brasil, 2018)

De acordo com Garde (2019):

> No Brasil, depois de dois anos de tramitação no Senado, o governo brasileiro viu-se obrigado a acelerar a regulamentação desta lei e se adequar aos moldes europeus. Pela urgência e pressão internacional, a LGPD se apresenta como uma versão compacta e simplificada da GDPR, mas com os mesmos pilares que garantem a privacidade dos usuários digitais.

Um dos principais pilares da LGPD é o consentimento informado, que estabelece que o tratamento de dados pessoais só pode ocorrer com a permissão explícita do titular dos dados. Isso significa que os pacientes devem ser informados de maneira clara e transparente sobre como seus elementos serão coletados e utilizados, além de terem o direito de aceitar ou recusar o tratamento. No contexto hospitalar, isso se traduz em obter o consentimento para procedimentos médicos, o compartilhamento de informações entre profissionais de saúde e até mesmo o armazenamento de registros médicos.

Além da autorização, a LGPD exige a necessidade de garantir a segurança dos dados. Os hospitais devem adotar medidas de segurança técnicas e organizacionais para proteger as informações médicas dos pacientes contra exposição, acessos não autorizados e incidentes de segurança. Isso inclui a implementação de criptografia, controles de acesso e políticas de segurança sólidas.

A lei também confere aos pacientes uma série de direitos, Art. 2° da Lei n° 13.709, de 14 de agosto de 2018, como o acesso aos seus próprios conceitos, o direito de corrigir informações incorretas e o direito de solicitar a exclusão de dados, quando aplicável. Isso coloca um poder maior nas mãos dos pacientes, permitindo que controlem suas informações médicas. (Brasil, 2018)

Em caso de violação da LGPD, hospitais e profissionais de saúde podem enfrentar responsabilidade legal e multas substanciais. Portanto, é fundamental que as instituições de saúde estejam em conformidade com a lei e tenham políticas de proteção de noções rigorosas.

De acordo com o Art. 4° da Lei n° 13.709, de 14 de agosto de 2018, também

estabelece regras para a transferência de conhecimentos pessoais para países estrangeiros, garantindo que os mesmos padrões de proteção sejam aplicados quando os fatos saírem do Brasil. isso é relevante para hospitais que colaboram com instituições internacionais ou enviam informações médicas para fora do país. (Brasil, 2018)

3. Riscos e Causas de Vazamento de Dados em Ambientes Hospitalares:

Os sistemas de informação hospitalar frequentemente lidam com uma vasta quantidade de referências que envolvem os pacientes, incluindo informações médicas, pessoais e financeiras. A falta de controle adequado de acesso pode resultar em vulnerabilidades, permitindo que indivíduos não autorizados obtenham acesso indevido a esses aspectos.

A transmissão e armazenamento de dados sem criptografia adequada podem expor as informações a riscos de interceptação por terceiros mal-intencionados. Sem criptografia, os materiais podem ser facilmente acessados e comprometidos durante a transmissão pela rede ou armazenamento em dispositivos.

A não aplicação de *patches*[1] de segurança e atualizações de software pode deixar os sistemas vulneráveis a ataques de hackers que exploram vulnerabilidades conhecidas. Os sistemas desatualizados podem ser alvos simples para invasões e comprometimento de dados.

A crescente adoção de dispositivos médicos conectados à Internet das Coisas (IoT) introduz novos pontos de vulnerabilidade em sistemas de informação hospitalar. Falhas de segurança nestes dispositivos podem permitir que hackers comprometam os sistemas e acessem aspectos sensíveis dos pacientes.

[1] O termo patch, em inglês significa “remendo”, “esparadrapo”, ou seja, um elemento utilizado para remendar ou consertar algo. Trazendo isso para o mundo da tecnologia, pode-se dizer que são programas que visam fazer correções de erros e bugs em softwares. Ferrão explica que, mesmo após diversos testes, problemas com falhas e vulnerabilidades são muito comuns após o lançamento de um software.

3.1 Análise das Possíveis Causas de Vazamento de Dados:

Vulnerabilidades em sistemas de informação hospitalar, como falta de criptografia, controle de acesso inadequado e falhas de atualização de segurança, podem ser exploradas por hackers para obter acesso não autorizado a conceitos.

Podem surgir por falta ou falhas nos controles de segurança, ou por erros ou ações intencionais das pessoas envolvidas no processo em questão. Essas fraquezas de segurança podem ocorrer durante a concepção, implementação, configuração ou operação de um ativo, controle ou processo. Elas podem ser geradas nas empresas através de falhas humanas, materiais ou tecnológicas, de forma acidental ou intencional.

Ao se identificar uma vulnerabilidade de segurança é necessária uma análise da mesma buscando a identificação da causa raiz dessa fraqueza, em muitos casos, uma única causa raiz gera mais de uma vulnerabilidade de segurança.

Hackers podem realizar uma variedade de ataques cibernéticos, como phishing, ransomware e ataques de negação de serviço, para comprometer os sistemas de informação hospitalar e obter acesso não autorizado aos dados dos pacientes.

Na distinção feita por Newton De Lucca (2001), da qual é trazido à colação o trecho em que, com muita propriedade, distingue hackers:

> Os hackers são especialistas em informática, capazes de invadir computadores alheios, mas também, de impedir invasões dos outros. Não existe, necessariamente, uma conotação pejorativa para os hackers que podem prestar serviço de extrema valia.

A falta de treinamento e conscientização dos funcionários sobre práticas adequadas de segurança da informação pode aumentar o risco de vazamento de matérias devido a comportamentos negligentes ou inadvertidos.

O crescente número de delitos cibernéticos é alarmante e de acordo com Patrícia Peck Pinheiro, uma pesquisa de estatística feita pela Polícia Federal dos Estados Unidos (FBI), concluiu que os crimes cibernéticos chegaram a US$3,5 bilhões de prejuízos em 2019 (Pinheiro, 2021).

No Brasil, temos mais 152 milhões de usuários de internet, isso corresponde a 81% da população, e com este vasto campo de acesso por usuários conectados isto proporciona facilidades aos criminosos para agirem diuturnamente, desenvolvendo programas de sites falsos, links de sorteios, mensagens com vírus, estelionato virtual, *fake News* e outras formas de ataques (Silva, 2022).

Essas são algumas das principais vulnerabilidades nos sistemas de informação hospitalar e possíveis causas de espalhamento de dados que precisam ser abordadas para fortalecer a segurança da informação e proteger a confidencialidade dos dados dos pacientes.

4. Impactos do Vazamento de Dados no Ambiente Hospitalar:

As divulgações de dados abalam a confiança dos pacientes nos hospitais e instituições de saúde. Quando os pacientes percebem que suas informações médicas foram comprometidas. Notícias sobre difusão de dados são frequentemente divulgadas pela mídia e compartilhadas nas redes sociais, o que pode resultar em uma ampla cobertura negativa e impactar a percepção pública sobre a qualidade e confiabilidade dos serviços prestados pelo hospital.

É discutida a importância da proteção de dados sensíveis no setor de saúde e a falta de conformidade das empresas e hospitais com os requisitos da lei geral de proteção de dados (LGPD) no Brasil os conceitos de saúde são considerados sensíveis devido à natureza extremamente particular das informações, por que com os aspectos sensíveis são capazes de consequências discriminatória sobre o

“dono” dos dados.

De acordo com o Art. 5° da Lei n° 13.709, de 14 de agosto de 2018, são casos destes dados aqueles relacionados ao estado de saúde do paciente, como ele ter - ou ter tido - alguma doença, ser pessoa com deficiência ou algum tipo de transtorno alimentar. Informações relacionadas à orientação sexual e identidade de gênero dos pacientes também devem ser preservadas, assim como dados sobre ISTs (Infecções Sexualmente Transmissíveis). (Brasil, 2018)

Todos esses fatos, caso indevidamente compartilhados, podem ser mobilizados por empresas para fins econômicos. É o caso, tipo de operadoras de planos de saúde que se recusam a oferecer serviços para pessoas que já tenham feito algum tipo de cirurgia. A LGPD estabelece a necessidade de tratamento cuidadoso, gestão e transmissão desses conceitos, porém, segundo pesquisa de setembro de 2019, realizada pela Serasa Experian, apenas 8,7% das empresas do setor de saúde estão em conformidade com a lei. (Pinheiro, 2019).

São enfatizados que os elementos contidos em exames, diagnósticos e procedimentos são confidenciais e ultra privativos, não devendo ser repassados nem mesmo para parentes do paciente, e muito menos para terceiros, assim como aconteceu no caso da atriz Klara Castanho, a publicação de suas informações causou danos pessoais, psicoemocionais e midiáticos. Como figura pública, ela foi vítima de violação de seu direito ao anonimato e sofreu exposição negativa de um trauma pessoal. O hospital é responsabilizado civilmente pelas disseminações, afetando tanto a esfera extrapatrimonial quanto a patrimonial da atriz. (Moutinho, 2023).

A LGPD é destacada como uma lei efetiva, e os locais que não se adequarem às diretrizes estão sujeitos a sanções judiciais severas. É enfatizada a necessidade de um projeto bem elaborado para o tratamento e manuseio dos dados, a fim de garantir conformidade com a lei.

A pandemia fruto do coronavírus coloca a área da saúde ainda mais em evidência. Segundo Garcia (2022) um cenário de 663 milhões casos confirmados e cerca de 15 milhões mortes espalhadas pelo mundo, o setor hospitalar precisa estar cada vez mais atento ao tratamento de seus pacientes, mas não apenas no plano dos cuidados médicos, como também no plano da proteção de bases pessoais.

Na área da saúde há tempos se beneficiou dos avanços propiciados pela era digital, tornando prática comum a disponibilização, entre hospitais, de prontuários e diagnósticos de pacientes em plataformas virtuais, como forma de facilitar e tornar mais organizada e eficiente a relação estabelecida entre médico, paciente e hospitais.

A proteção de informações pessoais na área da saúde é essencial para preservar a privacidade dos pacientes e garantir a integridade das informações médicas. O Brasil possui regulamentações específicas, como a Lei n° 13.787/2018 e a LGPD, que estabelecem diretrizes claras para a gestão segura de informações médicas em formato eletrônico. Profissionais de saúde e instituições têm a responsabilidade de cumprir essas regulamentações e garantir a confidencialidade e segurança dos fatos dos pacientes. (Brasil, 2018).

4.1 Avaliação dos Custos Financeiros e Legais:

Os hospitais enfrentam custos significativos para remediar os efeitos de uma divulgação de dados, incluindo investigações forenses para determinar a extensão do incidente, notificação aos pacientes afetados, implementação de medidas corretivas de segurança e contratação de serviços de proteção contra roubo de identidade.

Incidentes de exposições de bases podem levar à perda de pacientes e receita, à medida que os pacientes optam por buscar cuidados médicos em outras instituições percebidas como mais seguras e confiáveis.

Os hospitais enfrentam ações legais por parte dos pacientes afetados e reguladores governamentais devido à privacidade e segurança de conceitos. Isso pode resultar em custos substanciais relacionados a processos judiciais, indenizações e multas por não conformidade com regularidade de proteção de fatos.

No entanto, esses avanços também trazem consigo desafios significativos, visto que o setor se tornou alvo frequentemente de ataques cibernéticos. De acordo com a pesquisa “Cost of Data Breach”, promovida pela IBM traz importantes informações acerca dos impactos econômicos das publicações de conhecimentos pelas empresas. Segundo o levantamento realizado,no Brasil, nos primeiros 6 meses de 2019, ocupa a 4ª posição no ranking de regiões com maior volume de informações vazadas. O custo médio suportado pelas empresas em cada evento de vazamento de informações no Brasil é de 1,35 milhões de dólares, algo em torno de 5,4 milhões de reais. (Tavernard, 2019).

5. Medidas de Mitigação e Prevenção:

Revisão das melhores práticas de segurança da informação para hospitais, incluindo criptografia de elementos, e de conscientização sobre segurança para funcionários.

Recomendações para políticas de governança de elementos e conformidade com regulamentos de privacidade, como a LGPD no Brasil. A LGPD visa proteger direitos fundamentais de privacidade e liberdade dos indivíduos, estabelecendo regras claras sobre como as organizações devem coletar, armazenar, processar e compartilhar bases pessoais.

Portanto, a governança de referências é essencial para que as empresas cumpram os princípios exigidos pela LGPD no Brasil e a Autoridade Nacional de Proteção de Dados (ANPD), como a transparência, finalidade, adequação, necessidade, livre acesso, qualidade, segurança, prevenção de fatos e responsabilização.

Os hospitais devem garantir a conformidade com os regulamentos de privacidade de aspectos relevantes, como a Lei Geral de Proteção de Dados Pessoais (LGPD). o tratamento dos aspectos pessoais pode ser realizado por dois agentes de tratamento, o Controlador e o Operador. Além deles, há a figura do Encarregado, que atua como canal de comunicação entre o Controlador, o

Operador, os titulares dos conceitos e a Autoridade Nacional de Proteção de Dados (ANPD). Isso inclui a nomeação de um oficial de proteção de conhecimento, avaliações regulares de risco à privacidade e a implementação de medidas técnicas e organizacionais para proteger os conhecimentos dos pacientes.

Além de políticas e procedimentos, é fundamental proteger a infraestrutura de TI e os dispositivos médicos contra ameaças cibernéticas. Isso inclui a seleção de hardware, software e serviços adequados para suportar as operações da empresa.

Ao adotar e implementar essas melhores práticas de segurança da informação e conformidade regulatória, os hospitais podem reduzir significativamente o risco de espalhamento de dados e proteger eficazmente a confidencialidade e integridade das informações médicas dos pacientes.

6. Considerações finais:

Identificamos que os principais pontos de vulnerabilidade em sistemas de informação hospitalar incluem acesso não autorizado, falta de criptografia de referência, falhas de segurança, deficiências de autenticação e dispositivos médicos conectados. A partir da realização deste trabalho, foi possível identificar que os pontos principais de vulnerabilidade presentes em sistemas de informações hospitalares abrangem a falta de (ou ineficaz) criptografia de matérias, acesso não autorizado, e a ausência ou deficiência de autenticação de dispositivos médicos conectados.

A exposição de informações pode ocorrer por meio de falhas na segurança, acesso não autorizado de funcionários e erros humanos, o que facilita a exposição da máquina e, consequentemente, a possibilidade de ataques cibernéticos. Também, não se pode deixar de citar nessa revisão os efeitos negativos causados pela divulgação de matérias pessoais do paciente, o que pode ser desastroso tanto para este quanto para a instituição detentora dos mesmos, devido aos pesados custos financeiros (por meio da aplicação de multas) associados a tais incidentes.

Ressalta-se a necessidade de melhorias nas práticas de segurança de informação, tais como criptografia de fatos e treinamento da conscientização sobre a segurança para funcionários a fim de reverter o risco de vazamento de conhecimento. Recomenda-se também a aplicação de políticas governamentais de bases abrangentes, tal como a conformidade com leis de privacidade, tais como a LGPD, a fim de garantir a proteção de noções desses pacientes.

Em suma, o propósito dessa revisão é de abordar o tema de maneira proativa: a regulação de proteção de referências no Brasil abre um caminho claro para que as organizações atuem com maior segurança jurídica, reduzindo os riscos de suas atividades e criando oportunidades de ganho de reputação no mercado. Hospitais que adotem medidas de segurança técnica e organizacionais adequadas para a proteção de conhecimento de saúde de seus pacientes, e que cumpram com as normas brasileiras no geral, passarão maior credibilidade e segurança aos seus pacientes.

Nesse sentido, o propósito deste artigo é transmitir, em linhas gerais, quais são os pontos de atenção que os profissionais na área da saúde devem ter em

mente durante o tratamento de bases coletas, para evitar justamente que ocorra as difusões de conhecimento importantes que constam em prontuários médicos.

Referências

BRASIL. Lei nº 10.406, de 14 de maio de 2018. Institui o Código Civil. **Diário Oficial da União**: seção 1, Brasília, DF, 18 maio de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm . Acesso em: 28 maio 2024.

DE NEWTON, Lucca. Títulos e contratos eletrônicos: o advento da informática e seu impacto no mundo jurídico (2001): Direito e internet : aspectos jurídicos relevantes. Bauru -São Paulo: Edipro, 2021.

GARCIA, Mariana. Com cerca de 15 milhões, o mundo teve 3 vezes mais mortesna pandemia do que apontam os dados oficiais até 2021, diz OMS. Coronavírus, [*s.l.*], p 1, 5 maio de 2022. Disponível em: https://g1.globo.com/saude/coronavirus/noticia/2022/05/05/covid-19-oms- mortes.ghtml. Acesso em: 2 maio 2024.

MARTINS, Antônio Eduardo Senna. O Direito à Privacidade na Era Digital: Desafios e Implicações Jurídicas. Direito à Privacidade na Era Digital, [*s. l.*], 9 meses, 2023. Disponível em: https://www.jusbrasil.com.br/artigos/o-direito-a-privacidade-na-era- digital-desafios-e-implicacoes-juridicas/1971830331 . Acesso em: 24 maio 2024.

MOUTINHO, Maria Carla. Migalhas de Responsabilidade civil. Caiu na rede é dano:o caso Klara Castanho e a violação da privacidade, [*s. l.*], 18 maio 2023. Disponívelem: https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/386724/caiu-na-rede-e-dano-o-caso-klara-castanho-e-a-violacao-da- privacidade . Acesso em: 23 maio 2024.

OLIVEIRA, Elenilcio Dauto de; ALEXANDRE, Weliton do Nascimento. DIREITO DIGITAL NO COMBATE A CRIMES CIBERNÉTICOS. **DIREITO DIGITAL NO COMBATE A CRIMES CIBERNÉTICOS**, [*s. l.*], ano 2023, p. 1-35, 20 nov. 2023.
DOI 10.32749/núcleoconhecimento.com.br/lei/combate-a-crimes-cibernéticos. Disponível em: https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes- ciberneticos . Acesso em: 23 maio 2024.

PINHEIRO, Patrícia Peck. Direito digital. 6.ed, São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. Direito digital. 7.ed, São Paulo: Saraiva, 2021.

PINHEIRO, Patrícia Peck. LGPD e saúde: os fins justificam os meios?. NOTÍCIASE ARTIGOS, [*S. l.*], p. 1, 23 set. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados- sensiveis-saude . Acesso em: 19 abr. 2024.
SILVA, Gilsimar. Crimes digitais: evolução dos crimes e a aplicação do direito. Repositório

Universitário da Ânima (RUNA), [*S. l.*], p. 1, 17 jun. 2022. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/22552 . Acesso em: 19 abr. 2024.

TAVERNARD (Brasil-BH-Minas Gerais). Setor da saúde é o que mais sofre impactos financeiros com vazamento de dados: Pesquisas revelam números, informações e impactos econômicos do vazamento de dados em diferentes setores no primeiro semestre de 2019. Tavernard, Belo Horizonte-MG I Brasil, p. 1, 22 ago. 2019. Disponível em: https://tavernard.adv.br/nosso-escritorio/ . Acesso em: 18 abr.2024.