

Uma análise da adoção de assinaturas digitais de uma instituição pública de ensino superior no período da pandemia do covid-19 utilizando técnicas de open source intelligence

An analysis of the adoption of digital signatures by a public institution of higher education during the covid-19 pandemic using open source intelligence techniques

Matheus Vinícius Ferreira Pinheiro¹

Reudismam Rolim de Sousa²

RESUMO

A pandemia do COVID-19 afetou a forma como a sociedade teve que lidar com a tecnologia. Neste trabalho, objetiva-se realizar uma análise da adoção de assinaturas digitais em uma instituição pública de ensino superior no período da pandemia do COVID-19, utilizando técnicas de Inteligência de Fontes Abertas, obtenção de dados e informações disponíveis dentro de um domínio público. Foi desenvolvido uma metodologia e sistemas de coleta e verificação de assinaturas digitais em documentos públicos na instituição alvo. Como resultado encontrado, foi constatado que há indícios de mudança cultural na forma como a instituição valida documentos digitais.

Palavras-chave: OSINT. Assinaturas digitais. Documentos

ABSTRACT

The COVID-19 pandemic has affected the way society has had to deal with technology. In this work, the objective is to carry out an analysis of the adoption of digital signatures in a public institution of higher education in the period of the COVID-19 pandemic using techniques of Intelligence of Open Sources, obtaining data and information available within a public domain. A methodology and systems for collecting and verifying digital signatures on public documents at the target institution were developed. As a result, it was found that there are signs of cultural change in the way the institution validates digital documents.

Key words: OSINT. Digital signatures. Documents

Disponibilidade: <https://conjecturas.org/index.php/edicoes/article/view/2047>

1 Matheus Vinícius Ferreira Pinheiro – Graduando em Tecnologia da Informação pela Universidade Federal Rural do Semi-Árido.

2 Reudismam Rolim de Sousa - Doutor pela Universidade Federal de Campina Grande.

1. INTRODUÇÃO

Com o início da pandemia, causada pelo novo coronavírus, decretada pela Organização Mundial da Saúde (OMS), em 11 de março de 2020, também se inaugurou um novo ciclo na história da humanidade. Para que a maioria das organizações pudesse continuar desenvolvendo suas atividades habituais, tornou-se necessária a readequação destas ao novo modelo de interação social, em que era obrigatório, via de regra, o distanciamento social entre as pessoas. Dessa forma, a comodidade proporcionada pela internet (e seus mais variados desdobramentos tecnológicos), que já estava disponível, em grande escala, passou por uma espécie de revisitação, possibilitando, que as atividades pudessem ser realizadas de forma virtual.

Em meio a essa crise sanitária, e como forma de viabilizar o trabalho, várias instituições públicas de ensino superior optaram por realizar atividades administrativas e de ensino, pesquisa e extensão de maneira remota. Uma dessas instituições foi a Universidade Federal Rural do Semi-Árido (UFERSA). Além disso, considerando a necessidade de modernização da gestão de fluxos dos documentos da UFERSA para substituir o papel pelo meio digital, ainda durante o contexto pandêmico, o Conselho de Administração (CONSAD) da UFERSA emitiu a Resolução Nº 003/2020, na qual adota e reconhece as assinaturas digitais como ferramenta para substituir as assinaturas de punho, em documentos emitidos pela instituição.

A redação do Art. 3º da referida regulamentação assim dispõe: "Adotar e reconhecer assinaturas: digitais, eletrônicas, e cadastradas, conforme caracterizadas no capítulo I deste dispositivo, como plenas substitutas a assinaturas de punho a documentos impressos." Vale salientar, por oportuno, que as assinaturas manuscritas eram a principal forma de validação dos documentos oficiais da entidade; porém, diante do cenário pandêmico e com a necessidade da digitalização de processos e documentos, surge a necessidade de aprimorar a segurança dos arquivos que seriam legitimamente assinados e validados. O mecanismo de assinaturas digitais provê uma forma de trazer garantias de integridade, confidencialidade e validade jurídica aos documentos digitais, os quais são assinados de forma totalmente eletrônica.

Então, esse trabalho surge da ideia de se verificar em que medida se deu a adesão/incidência de utilização das assinaturas digitais no âmbito da aludida instituição de ensino superior, durante a pandemia da COVID 19, com vistas a se verificar os (possíveis) efeitos práticos causados pela aderência da entidade pública a esse tipo de identificação pessoal. A extração dos dados para a realização da pesquisa ocorreu por meio das técnicas de OSINT (Inteligência de Fontes Abertas), em que se extraem informações de domínio público para geração de inteligência. Os objetos de estudo deste trabalho são os documentos a serem examinados de propriedade pública - disponíveis no domínio documentos.ufersa.edu.br, de modo que não haverá acesso a qualquer documento de caráter sigiloso.

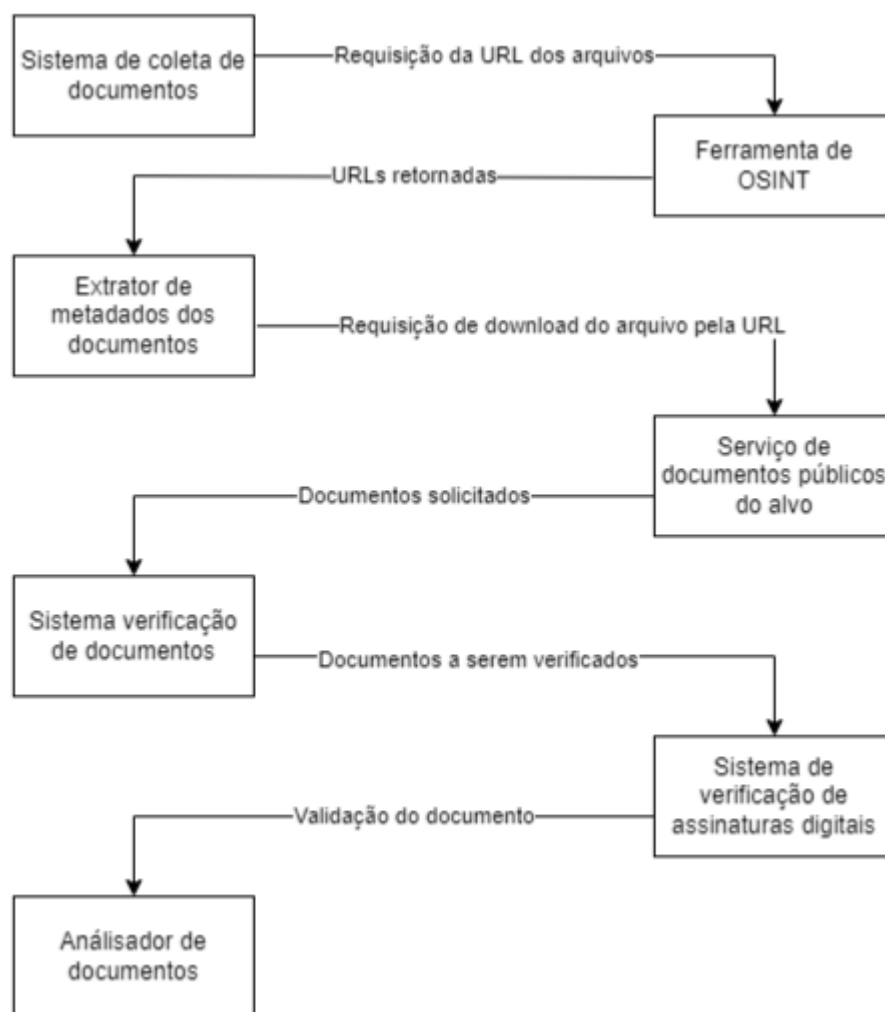
Um sistema de coleta de documentos analisa documentos desse domínio com o auxílio da ferramenta de OSINT, chamada Google Hacking, um mecanismo de busca avançada que utiliza os motores de rastreamento do próprio Google. Após a coleta desses documentos, a validação das assinaturas digitais é realizada, o que possibilitará inferir sobre como a pandemia impactou a adoção desse tipo de tecnologia na instituição alvo.

O restante deste trabalho está organizado da forma seguinte: na Seção 2 é abordada a metodologia da pesquisa, descrevendo a sequência de atividades de coleta, extração e verificação de documentos digitais, emitidos do domínio da instituição alvo; na Seção 3 é detalhado o desenvolvimento da pesquisa, em que se detalha a arquitetura do sistema desenvolvido de coleta e validação de assinaturas digitais nos documentos analisados; na Seção 4 são abordados os resultados e realizada a discussão desses resultados, apresentando a análise dos documentos coletados na pesquisa; por fim, na Seção 5 são apresentadas as considerações finais, em que se descreve as limitações e conclusões do trabalho.

1. METODOLOGIA

O objetivo deste trabalho é realizar uma análise da adoção de assinaturas digitais em uma instituição pública de ensino superior no período da pandemia do COVID-19, utilizando técnicas de Inteligência de Fontes Abertas. Neste trabalho, a UFERSA foi a instituição alvo. Ademais, visando alcançar esse objetivo, foi necessário desenvolver uma metodologia que acomode as etapas de documentos digitais que tem, ou não, assinaturas digitais válidas. As etapas desse processo podem ser vistas na Figura 1.

Figure 1: Metodologia para coleta e validação dos documentos



Fonte: Autoria própria

A primeira etapa da metodologia é a aplicação de uma ferramenta de coleta de documentos digitais, que busca endereços Uniform Resource Locator (URL), através da ferramenta de OSINT, Google Hacking. O período temporal é informado como parâmetro da ferramenta nessa consulta e o domínio dos documentos da instituição alvo. O retorno dessa consulta são as URL dos documentos a serem analisados.

Em seguida, é realizada a etapa de extração de metadados, informações que descrevem o arquivo, dos documentos digitais. Os arquivos precisam ser expedidos pela instituição alvo, que no caso da UFERSA, o formato do arquivo deve ser Portable Document

Format (PDF). Os arquivos devem estar em ambiente de consulta pública, gerenciado pela instituição (no caso, o endereço do portal de documentos da UFERSA - <https://documentos.ufersa.edu.br/>). No final desse procedimento, os arquivos são baixados para uma máquina e separados para a verificação de assinaturas digitais.

A última etapa é descobrir se os documentos contém assinaturas digitais. Para isso, eles são enviados a um sistema de verificação de assinaturas digitais, em que é possível saber se há ou não assinaturas válidas nesses documentos. Portanto, a hipótese que testa o objetivo desse trabalho é se há aumento no número de documentos com assinaturas digitais válidas ao longo do período da pandemia, em detrimento de documentos que não são assinados digitalmente.

1.1 DESENVOLVIMENTO

Para a aplicação da metodologia descrita anteriormente, foi necessário a construção de software que auxilie na coleta, análise de metadados, download de arquivos e verificação de assinaturas digitais, nesses documentos da instituição alvo. Assim, em termos de software, foram desenvolvidos dois componentes: um sistema de coleta de documentos e um sistema de verificação de documentos.

1.2 SISTEMA DE COLETA DE DOCUMENTOS

Neste trabalho foi utilizada a técnica de Google Hacking, que faz a indexação das pesquisas e realiza as buscas de forma assertiva. Trata-se de um conceito de busca avançada que utiliza agrupamentos de alguns operadores específicos, os quais, combinados, são capazes de gerar os Dorks (item no Google Hacking Database - GHBD). A presente investigação está restrita a documentos que contenham assinaturas digitais, em formato PDF, inseridos no domínio documentos.ufersa.edu.br, mediante a utilização do seguinte Dorks de busca: `inurl:documentos.ufersa.edu.br filetype:pdf`. Para fins de verificação do período pandêmico, foram utilizadas marcações temporais nessas buscas, com o intuito de restringir os achados neste intervalo de tempo. Uma vez de posse dos arquivos no referido formato, é averiguado a existência de assinaturas digitais válidas, buscando validar ou refutar a hipótese do trabalho.

A coleta de documentos foi realizada através de uma ferramenta automatizada, construída com a linguagem Python3. Primeiramente, este software realiza requisições aos servidores do Google, com os parâmetros a serem analisados. Em seguida, é coletado todas as URLs dos documentos desejados (filtragem da busca utilizando técnicas do Google Hacking). Após receber o retorno dessas requisições, as URLs obtidas são adicionadas a um arquivo organizado como Comma-Separated Values (CSV). Em seguida, esse software realiza o download dos arquivos indicados pelas URLs, através da leitura do arquivo CSV. O retorno de cada download, gera a escrita de um arquivo local na máquina em formato PDF. Para facilitar a análise de cada arquivo no formato PDF, os arquivos são renomeados com a data de publicação. Essa informação da data foi extraída dos metadados dos documentos, realizados na primeira etapa de busca de URLs.

1.3 VERIFICAÇÃO DAS ASSINATURAS DIGITAIS

A verificação das assinaturas de forma automatizada, foi realizada a fim de se potencializar a autenticidade das identificações pessoais nos documentos digitais. Para isso, foi construída uma ferramenta, também, na linguagem Python3. Nela, a verificação das assinaturas é realizada através do envio de cada arquivo PDF para uma plataforma de verificação de assinaturas. O sistema de verificação de documentos utiliza os sistemas Web da UFSC e o IPCEdu de endereços <https://assina.ufsc.br/verificador/> e <https://pessoal.icpedu.rnp.br/public/verificar-assinatura>, respectivamente. O resultado dessa consulta é utilizado para gerar um novo arquivo do tipo CSV, que serve como base de dados para a construção de um gráfico de análise dos resultados, que mostra a utilização das assinaturas digitais em virtude do tempo, tendo como lapso temporal o período pandêmico.

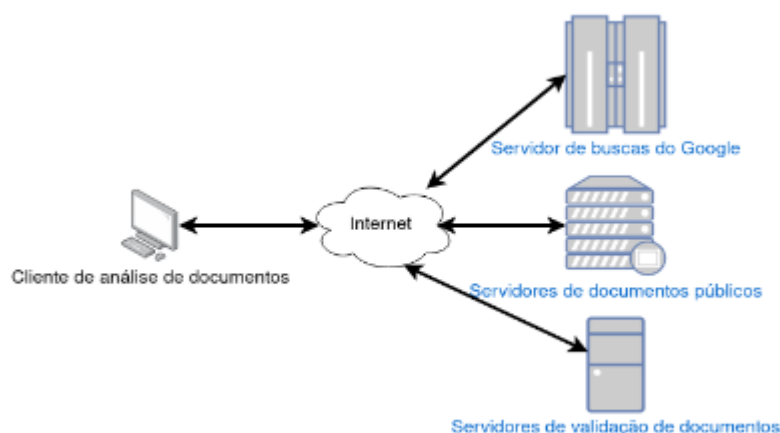
1.4 ARQUITETURA DO SISTEMA

A arquitetura de sistema descreve a organização física dos componentes. Como descrito nas duas subseções anteriores, há dois componentes desenvolvidos neste trabalho:

1. Sistema de coleta de documentos (SCD): objetivo de coletar os documentos digitais a serem analisados;
2. Sistema de verificação de assinaturas (SVA): automatizar o processo de verificação das assinaturas digitais nos documentos coletados;

Ambos os sistemas SCD e SVA foram executados em uma arquitetura cliente-servidor como pode ser visto na Figura 2.

Figure 2: Arquitetura do sistema de análise de documentos digitais



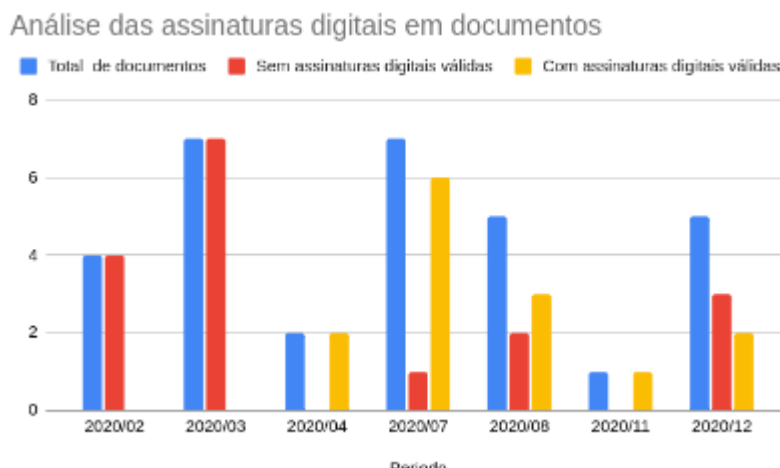
Fonte: Autoria própria

Primeiro, o SCD envia solicitações aos servidores de busca do Google e em seguida faz consultas aos servidores de documentos públicos da instituição alvo. Por fim, o sistema SVA realiza a verificação de assinaturas digitais nos documentos digitais coletados em serviços de sistemas Web.

1.5 RESULTADOS E DISCUSSÃO

Por uma questão de limitação de tempo para análise, o período considerado nesta pesquisa ficou limitado aos meses de janeiro a dezembro do ano de 2020. Sendo assim, o sistema de coleta de dados utilizou o Google Hacking, ferramenta de OSINT, com a informação desse período. E, no total, foram analisados 31 arquivos dentro do período de 2020. Na Figura 3 pode ser visto esse período e os resultados obtidos.

Figura 3 - Análise das assinaturas digitais nos documentos



Fonte: Autoria própria

É possível perceber que os primeiros documentos com assinatura digital apenas aparecem a partir do mês de abril de 2020. E posterior a essa data, é possível notar um aumento de documentos com assinatura digital. Somente no mês de dezembro, o número de documentos sem assinatura digital foi maior.

Como saldo do ano de 2020, tem-se 31 documentos, sendo que 14 contém a presença de assinatura digital, o que nos traz uma porcentagem de aproximadamente 45%. Já os documentos não assinados digitalmente foram 17, trazendo uma porcentagem de aproximadamente 55% deste universo analisado.

Este resultado indica que a adoção de assinaturas digitais na instituição pública de ensino superior, UFERSA, no período da pandemia do COVID-19 reflete uma mudança de comportamento cultural. A publicação da Resolução CONSAD Nº 003/2020 estimulou que atos administrativos, na UFERSA, publicados através de documentos digitais, fossem possíveis de serem verificados com relação à integridade da origem, com o uso de assinatura digitais, resultando na confiabilidade necessária para a validação da informação.

2 CONSIDERAÇÕES FINAIS

No processo de automatização da coleta de dados com o *Google Hacking*, verificou-se a presença do *recaptcha* em algumas consultas. O *recaptcha* é um mecanismo de segurança, que foi desenvolvido com o intuito de proteger sites contra acesso indevido por parte de robôs, softwares que automatizam a interação Web com os servidores na Internet. Essa foi uma dificuldade presente na elaboração do software de coleta de dados fornecidos pela busca indexada com o *Google Hacking*. Como eram feitas muitas requisições, partindo do mesmo ponto de origem (máquina cliente), isto provocava o aparecimento do *recaptcha* nessas consultas. Como consequência, o sistema SCD falha.

Burlar o mecanismos de *recaptcha* é algo que está fora do escopo desta pesquisa. Como estratégia de mitigar essa dificuldade, a alteração do IP de origem das requisições e menor número de testes acabou sendo as alternativas para se construir o sistema de SCD, pois o *recaptcha* só vai aparecer quando são feitas muitas solicitações de forma consecutiva ao servidor de dados.

Outra limitação do desenvolvimento do software do SVA está no fato dos sistemas Web de verificação de assinaturas digitais não possuírem uma *Application Programming Interface* (API), que permitisse a automatização dessa verificação. Há uma perspectiva da Rede Brasileira

de Educação e Pesquisa (RNP) de prover uma API neste sentido, mas essa não está disponível ao público.

Este trabalho propôs uma análise da adoção de assinaturas digitais em um instituição pública de ensino superior no período da pandemia do COVID-19, utilizando técnicas de Inteligência de Fontes Abertas. Para isso, foi desenvolvido sistemas de software que coletaram documentos emitidos pela instituição pública analisada e foi constatado que há indícios de mudança cultural na forma como a instituição valida documentos digitais.

REFERÊNCIAS

ANTONIO, Joas. Fundamentos de Osint. Disponível em:
<https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU>.
Acesso em 10 Ago. 2022

GANDINI, João Agnaldo Donizeti; SALOMÃO, Diana Paola da Silva; JACOB, Cristiane. A Validade jurídica dos documentos digitais. 2016.

PEREIRA, Samaris Ramiro. Certificação Digital através de algoritmo RSA. FATEC, São Caetano do Sul, v. 1, n. 1, p. 74 a 86. Disponível em:
<https://www.fatecsaocaetano.edu.br/fascitech/index.php/fascitech/article/view/9>. Acesso em: 05 Ago. 2022

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

RESENDE, Dilma. Certificação Digital. Revista Jurídica UNIGRAN. Dourados, MS | v. 11 | n. 22 | Jul./Dez.2009. Disponível em:
https://www.unigran.br/dourados/revista_juridica/ed_anteriores/22/artigos/artigo09.pdf.
Acesso em: 13 Ago. 2022

RIBEIRO, Oseias Gomes. et al. A CERTIFICAÇÃO DIGITAL NA ICP-BRASIL. Tékhne e Lógos, Botucatu, SP, v.2, n.2, fev. 2011.