Vulnerabilidade da Chave de Acesso à Nota Fiscal Eletrônica: Riscos à Segurança de Empresas e Consumidores

Elmano Ramalho Cavalcanti[1], **Isabella Tito de Oliveira Silva**[1], **Jonathan Saturnino Souto**[1], **Estevão Lima Junior**[1], **Danyllo Wagner Albuquerque**[1]

[1] Instituto Federal da Paraíba (IFPB)

{elmano.cavalcanti, isabella.tito, jonathan.saturnino, estevao.holanda, danyllo.albuquerque}@ifpb.edu.br

Abstract. *The Electronic Invoice (NF-e) is a pillar of the Brazilian digital government, making taxation more transparent and efficient. This study analyzes a critical security vulnerability that enables unauthorized access to electronic invoices. We assessed the compliance of issuing systems with technical security standards by analyzing 200 companies from different sectors, six open-source projects on GitHub, and developing a tool to detect the level of vulnerability. The results indicate that 52% of companies use insecure methods, with 75% of those exhibiting high vulnerability. We conclude that there is a structural risk compromising the confidentiality of fiscal data, requiring immediate action from companies and tax authorities.*

Resumo. *A Nota Fiscal Eletrônica (NF-e) é um pilar do governo digital brasileiro, tornando a tributação mais transparente e eficiente. Este estudo analisa uma vulnerabilidade de segurança crítica que possibilita acesso não autorizado às notas fiscais. Avaliamos a conformidade de sistemas emissores com os padrões técnicos de segurança, analisando 200 empresas de diferentes setores, seis projetos de código aberto no GitHub e desenvolvendo uma ferramenta para detecção do nível de vulnerabilidade. Os resultados apontam que 52% das empresas utilizam métodos inseguros, sendo 75% delas com alta fragilidade. Conclui-se que há um risco estrutural que compromete a confidencialidade de dados fiscais, exigindo ações imediatas de empresas e autoridades tributárias.*

1. Introdução

Mais de 130 bilhões de Notas Fiscais de Consumidor Eletrônicas (NFC-e) já foram emitidas no Brasil desde 2014, alcançando uma média diária de 60 milhões atualmente[1]. Esses documentos contêm informações sobre a empresa emissora, os produtos comercializados, a forma de pagamento e, em alguns casos, dados sensíveis do cliente como nome, CPF, endereço e número de telefone.

Idealmente, o acesso a esses dados deveria ser restrito à empresa emissora, ao destinatário e, eventualmente, ao contador da empresa, sempre mediante o uso de um certificado digital. No entanto, para facilitar a consulta por parte dos cidadãos, o acesso completo aos dados da NFC-e é disponibilizado por meio do portal web da Secretaria da Fazenda (SEFAZ) estadual para qualquer pessoa que possua a chave de acesso da nota fiscal. Dessa forma, utilizando um dispositivo móvel, o consumidor pode simplesmente escanear o código QR impresso no Documento Auxiliar da Nota Fiscal Eletrônica - DANFE

[1] https://nfce.encat.org/estatisticas/

(Figura 1) e ser redirecionado ao portal da SEFAZ da respectiva unidade federativa, onde poderá visualizar os dados do documento fiscal.

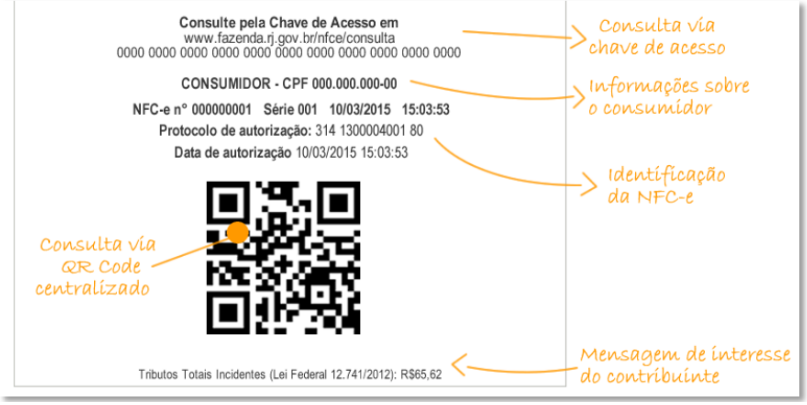

Figura 1. Trecho do leiaute do DANFE da NFC-e.
Fonte: [ENCAT 2024]

A chave de acesso, composta por 44 dígitos, inclui um campo de oito dígitos denominado código da nota fiscal (`cNF`), que deveria ser idealmente gerado aleatoriamente. No entanto, não há qualquer mecanismo que impeça a adoção de práticas inadequadas pelos sistemas utilizados pelas empresas emissoras, uma vez que os sistemas das SEFAZs apenas rejeitam algumas sequências triviais, como 12345678 ou 11111111, sem verificar se o `cNF` foi efetivamente gerado de forma aleatória. Consequentemente, a partir de uma ou poucas chaves de acesso não seguras de uma empresa, torna-se possível deduzir as demais chaves de acessos, acessando dados de empresas e seus clientes de modo indevido.

A falha de segurança que resulta em acesso não autorizado a notas fiscais pode ter consequências drásticas, tanto no campo empresarial, criminal, como jurídico. No primeiro, possibilita ações de espionagem industrial [Hou and Wang 2020], permitindo, por exemplo, que uma empresa concorrente saiba quem são os clientes, os produtos mais vendidos e a política de preços e descontos da empresa alvo. Quanto ao segundo, há relatos recentes de tentativas de golpes que se utilizam dessa falha de segurança [Martins 2024]. Quanto à esfera jurídica, as empresas são obrigadas legalmente a adotar medidas técnicas para proteger dados sensíveis de seus clientes contra acessos não autorizados (Art. 6º, inciso VII, da Lei Geral de Proteção de Dados Pessoais - LGPD). O descumprimento dessa lei pode resultar em penalidades e sanções para a empresa.

O principal objetivo deste artigo é investigar até que ponto os sistemas utilizados por empresas emissoras de NF-e/NFC-e estão gerando a chave de acesso em conformidade com o padrão técnico nacional estabelecido pelos órgãos tributários. O referencial teórico que fundamenta esta pesquisa é apresentado na Seção 2, seguido de alguns trabalhos relacionados (Seção 3). Os materiais e métodos utilizados estão detalhados na Seção 4. As principais contribuições deste estudo incluem[2]:

1. Um levantamento e análise da segurança do acesso à NFC-e em 200 empresas do setor varejista, abrangendo diferentes portes e segmentos econômicos (Seção 5);

[2]Os artefatos produzidos durante o projeto, como planilhas e código da aplicação, encontram-se no repositório `https://github.com/elmanorc/nfe-vulnerability-detector`.

2. Uma análise técnica de quatro bibliotecas e dois sistemas de emissão de NF-e/NFC-e disponíveis na plataforma GitHub (Seção 6);
3. O desenvolvimento de uma ferramenta pública e gratuita capaz de detectar vulnerabilidades nas notas fiscais de uma empresa a partir de uma amostra de chaves de acesso (Seção 7);
4. Uma validação externa dos achados e evidências de generalização do problema em nível nacional, baseada na análise de dados públicos (Seção 8).

Por fim, as conclusões, limitações e possíveis desdobramentos desta pesquisa são discutidos na Seção 9.

2. Fundamentação Teórica

Em 2004, no intuito de modernizar e informatizar o processo de emissão de notas fiscais, seguindo as tendências mundiais de governo digital [Manoharan et al. 2021], o projeto Nota Fiscal eletrônica (NF-e) foi concebido. Esse projeto integrava o Sistema Público de Escrituração Digital (SPED), idealizado para melhorar a relação entre o fisco e o contribuinte e visando a modernização e simplificação das obrigações fiscais no Brasil [Bonfim et al. 2012].

A NF-e é um arquivo digital no formato XML que substituiu as antigas notas fiscais em papel. Ela é gerada e transmitida eletronicamente, via serviços web, pelas empresas para a SEFAZ, permitindo o registro e a fiscalização das operações de forma mais eficiente e segura [ENCAT 2024]. Por motivos semelhantes, outros documentos fiscais eletrônicos foram desenvolvidos pelo poder público, a exemplo da nota fiscal de serviços eletrônica (NFS-e) e da nota fiscal de consumidor eletrônica (NFC-e) [Cunha 2022].

A NFC-e foi idealizada para substituir os documentos fiscais em papel utilizados no varejo (i.e., o cupom fiscal e a nota fiscal modelo 2) [Gonzaga 2017]. Em termos geográficos, a abrangência da NF-e é nacional, enquanto que a da NFC-e é estadual, devendo ser consultada exclusivamente no portal da SEFAZ da respectiva unidade federativa. Por conseguinte, diferentemente da NF-e, a adoção da NFC-e ocorreu de forma independente entre os estados, cada um estabelecendo seu próprio cronograma de obrigatoriedade. Atualmente, a NFC-e está presente em todas as unidades da federação.

Por ser voltada à pessoa física, a NFC-e tem algumas particularidades. No ato da compra, o consumidor recebe o DANFE, o qual contém, além dos dados dos produtos adquiridos, outras informações como a data e horário da compra, a numeração da nota fiscal (nNF) e a chave de acesso (rever Figura 1). Com esta última informação em mãos, qualquer pessoa pode acessar os dados do documento fiscal no site da respectiva SEFAZ estadual.

A chave de acesso é composta por 44 dígitos que referenciam metadados do documento fiscal, de acordo com a sequência a seguir [ENCAT 2024]:

- cUF: indica o código da UF do emitente (e.g., RS é 43);
- AAMM: ano e mês de emissão;
- CNPJ do emitente: 14 dígitos;
- mod: modelo do documento (55 para NF-e e 65 para NFC-e);
- ser: série da nota fiscal, contendo três dígitos;
- **nNF**: número da nota fiscal, contendo nove dígitos (geralmente sequencial);
- tpEmis: forma de emissão, contendo um dígito;

- **cNF**: código numérico, contendo oito dígitos;
- cDV: dígito verificador (módulo 11), contendo um dígito.

Conforme alerta o Manual de Orientação ao Contribuinte da Receita [ENCAT 2024], é necessário que o código numérico, `cNF`, da chave de acesso, seja uma sequência aleatória, evitando que alguém consiga deduzir a numeração de outras chaves de acesso. Para isso, o programador deve utilizar apropriadamente um bom e seguro gerador de números pseudo-aleatórios, a fim de não enfraquecer a aleatoriedade do código gerado [Bhattacharjee and Das 2022].

Um gerador de números pseudo-aleatórios (do inglês, PRNG, *Pseudo-random Number Generator*) é um algoritmo que produz uma sequência de números que se aproxima de uma sequência de números aleatórios verdadeiros [Cormen et al. 2022]. Esses números são gerados a partir de uma semente (ou estado inicial) e podem ser reproduzidos se a mesma semente for utilizada novamente. Os PRNGs são amplamente utilizados em diversas áreas, incluindo simulações computacionais, criptografia, jogos de lazer, jogos de azar e reconhecimento de padrões [Johnston 2018].

Uma característica importante é que qualquer PRNG gera sempre a mesma sequência quando recebe a mesma semente. Isso é vital, por exemplo, em simulações computacionais, dada a necessidade de ser possível repetir e verificar um experimento [Johnston 2018]. Entretanto, essa previsibilidade pode fragilizar sistemas que o utilizam para fins de segurança, como é o caso dos sistemas de emissão de notas fiscais eletrônicas.

3. Trabalhos Relacionados

Um artigo publicado na época do lançamento do Projeto NF-e [Santos 2006] por um especialista da área jurídica em proteção de dados, discutiu algumas preocupações concernentes aos crimes cibernéticos, sugerindo a necessidade de parcerias entre administrações fiscais e órgãos de criminalística para aprimorar a segurança do sistema.

Uma avaliação de segurança em sistemas públicos disponíveis ao público é apresentada em [Botacin and Grégio 2021]. Os autores utilizaram a metodologia OWASP Top-10 para identificar vulnerabilidades em alguns serviços governamentais. Os autores destacam que os serviços não protegidos apresentam níveis inadequados de segurança, enfatizando a necessidade de medidas corretivas urgentes. Entretanto, o artigo não menciona os serviços de consulta à NFC-e oferecidos pelas SEFAZs.

Na medida do nosso conhecimento, a dimensão da problemática abordada neste artigo ainda não foi investigada na literatura. Este estudo representa uma contribuição inédita ao identificar, analisar e quantificar vulnerabilidades em sistemas de emissão de NF-e/NFC-e no Brasil, evidenciando riscos de acessos não-autorizados ao conteúdo das notas fiscais.

4. Materiais e Métodos

Inicialmente, realizou-se um levantamento de campo no município de Campina Grande - PB, com o objetivo de coletar DANFEs de uma amostra representativa de empresas locais. Para tal, visitaram-se 200 estabelecimentos comerciais de diversos setores, empregando um dos seguintes métodos de coleta: (1) aquisição de produtos ou serviços como cliente; (2) busca em áreas de descarte de papel; (3) solicitação direta aos gerentes ou funcionários, mediante a apresentação dos objetivos do projeto acadêmico. A coleta de dados foi realizada ao longo de um período de aproximadamente dois meses.

O universo da pesquisa compreende todas as empresas emissoras de NF-e ou NFC-e credenciadas junto à SEFAZ-PB com endereço no município de Campina Grande, excluindo-se os Microempreendedores Individuais (MEIs), que não são obrigados a emitir documentos fiscais para pessoas físicas, exceto sob solicitação. De acordo com dados do sistema DataSebrae[3], cuja fonte é a Receita Federal, o município em questão possui 6200 empresas no comércio. A amostra selecionada confere um grau de confiança de 95%, com margem de erro de 6,75% [Anderson et al. 2021].

Durante a coleta de dados, registraram-se informações relevantes, tais como: CNPJ, razão social, nome fantasia, porte e Classificação Nacional de Atividades Econômicas (CNAE) das empresas, além dos metadados contidos na chave de acesso e a versão do software de emissão. Posteriormente, cada chave de acesso foi analisada com o intuito de inferir o método de geração do `cNF`. Em diversas ocasiões, a análise requereu a comparação de duas ou mais chaves de acesso sequenciais, o que prolongou o processo.

Após a análise estatística dos dados coletados (Seção 5), procedeu-se à análise técnica de seis projetos de código aberto relacionados à NFC-e, disponíveis na plataforma GitHub (Seção 6). Os critérios de seleção priorizaram projetos com maior número de estrelas e *forks*, indicativos de engajamento ativo da comunidade, e linguagens de programação amplamente utilizadas em soluções de automação comercial no varejo, como Java, C/C++, C#, Delphi e PHP.

Por fim (Seção 7), desenvolvemos uma ferramenta para detecção de vulnerabilidades em chaves de acesso. A ferramenta foi implementada utilizando a linguagem Python e o *framework* Flask. A interface de programação de aplicações (API) foi projetada para receber uma lista de chaves de acesso como entrada e fornecer informações sobre o método de geração do código numérico da nota fiscal e o nível de vulnerabilidade de acesso não autorizado às NF-e/NFC-e da empresa.

5. Estudo de Campo

Para esta pesquisa, foram analisados os DANFEs emitidos entre 01/08/2024 e 30/09/2024 de 200 empresas, distribuídas em 23 setores. A amostra incluiu 97 microempresas, 46 empresas de pequeno porte, 11 empresas de médio porte e 46 grandes empresas. Os dados de porte e da Classificação Nacional de Atividades Econômicas (CNAE) das empresas foram consultados no portal da Receita Federal[4].

Considerando a CNAE principal de cada empresa, a amostra abrangeu 7 Seções, 16 Divisões, 29 Grupos e 47 Classes, o que demonstra uma ampla diversidade de atividades econômicas. Para assegurar uma amostra representativa do universo, buscou-se, na medida do possível, manter a proporção de empresas de acordo com a CNAE.

Após uma análise minuciosa das chaves de acesso, constatou-se a presença de algoritmos determinísticos inseguros na geração do `cNF`. As seguintes vulnerabilidades foram identificadas:

- **Código Fixo (F):** Emprego de um valor constante no `cNF`, caracterizando uma falha de segurança crítica. Este método, surpreendentemente, foi observado em uma das maiores redes atacadistas do Brasil.

[3] `https://datasebrae.com.br/`

[4] `https://solucoes.receita.fazenda.gov.br/Servicos/cnpjreva/cnpjreva_Solicitacao.asp`

- **Espelhamento com Deslocamento (E):** Utilização da relação $cNF = nNF + K$, onde nNF é o número da nota fiscal e K é uma constante (tipicamente 1, 2 ou 3). Esta técnica, implementada como uma solução alternativa à restrição de igualdade direta ($cNF = nNF$) imposta pelas SEFAZs ([ENCAT 2023]) para a NF-e, configura uma vulnerabilidade de alta severidade.
- **Incremento Sequencial (I):** Geração do `cNF` através de incrementos sequenciais, similares ao `nNF`, ou pela fórmula $I + K$, onde K pode ser uma constante ou um valor extraído da chave de acesso (e.g., a série). Esta abordagem também expõe o sistema a alto risco.
- **Incremento Temporal ($I + X$):** Variação do método incremental, onde o `cNF` é ajustado com base no horário de emissão da nota fiscal. Este método aumenta a suscetibilidade a ataques de força bruta, sendo classificado como de vulnerabilidade média.
- **Aleatoriedade Parcial:** Geração de `cNF` com apenas alguns dígitos aleatórios. A presença de padrões previsíveis eleva o risco de descobertas por força bruta, resultando em uma classificação de vulnerabilidade média.

A análise da frequência de utilização dos métodos de geração de `cNF` revelou a seguinte distribuição (Figura 2): o método Incremental predominou com 41 ocorrências (39%), seguido pelo método Parcialmente Aleatório, presente em 24% dos casos. Os métodos Espelho e Fixo apresentaram frequência equivalente, ambos com 17%. Em contrapartida, o método Baseado no Horário foi identificado em apenas três empresas.

Figura 2. Distribuição dos métodos não seguros de geração do `cNF`.

A análise do nível de vulnerabilidade revelou que 52,5% dos estabelecimentos comerciais estão suscetíveis a acessos não autorizados aos dados de suas notas fiscais (Figura 3). Destes, 75% apresentaram alta vulnerabilidade, enquanto os 25% restantes demonstraram vulnerabilidade média.

Empresas de grande porte exibiram uma segurança ligeiramente superior às demais, com 56% classificadas como de baixa vulnerabilidade (Figura 4). Contudo, a disparidade observada entre os diferentes portes empresariais foi mínima, salientando a prevalência de chaves de acesso inseguras em todos os segmentos.

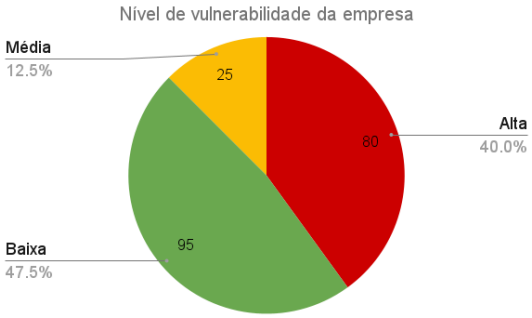

Figura 3. Nível de vulnerabilidade das empresas analisadas.

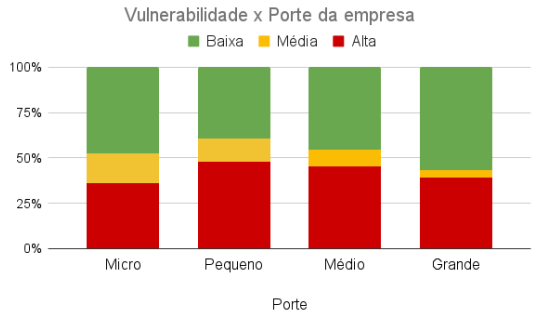

Figura 4. Vulnerabilidade por porte das empresas.

Quanto ao nível de vulnerabilidade por setor de atividade econômica, o comércio de móveis destacou-se como o mais vulnerável, com apenas um estabelecimento considerado seguro em um total de oito (Figura 5). É relevante ressaltar que transações neste setor frequentemente envolvem dados pessoais dos consumidores, devido ao valor elevado dos produtos e à necessidade de garantia.

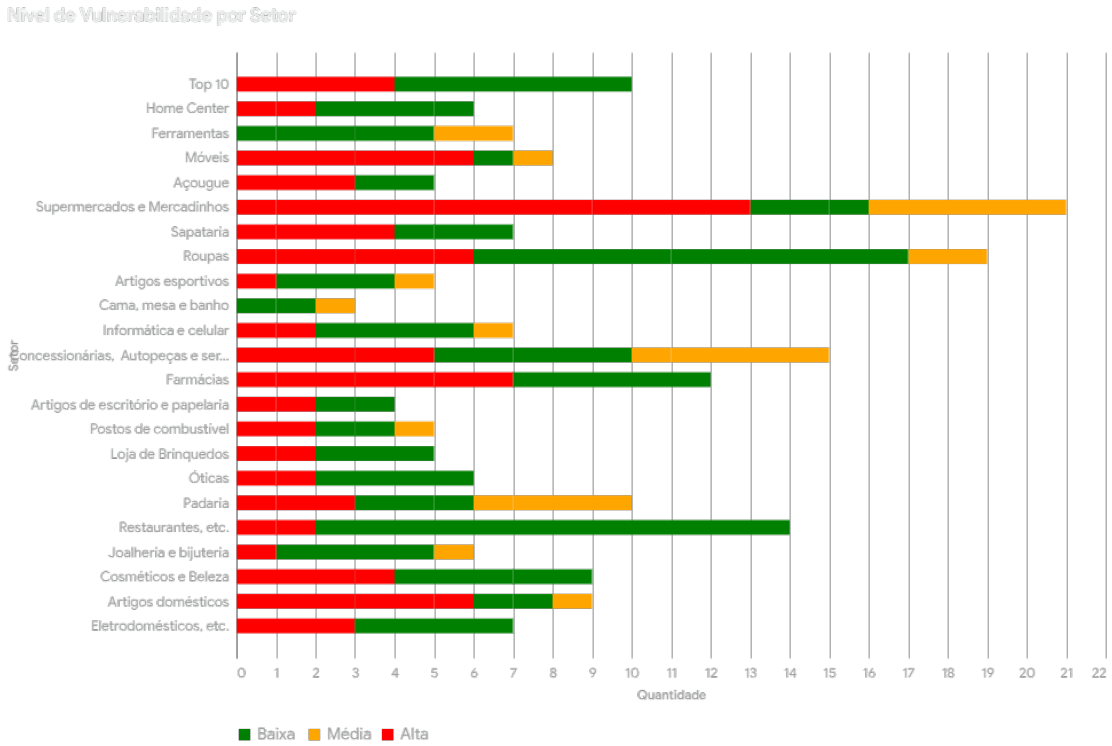

Figura 5. Nível de vulnerabilidade por setor.

O setor de supermercados e mercadinhos também apresentou alta fragilidade, com apenas 3 das 21 empresas analisadas gerando chaves de acesso seguras. A coleta do CPF do consumidor é comum neste setor, devido às regulamentações das SEFAZs estaduais que exigem a identificação em compras acima de um determinado valor. Em contrapartida, os setores de lojas de equipamentos e ferramentas, joalherias, comércio de cama, mesa e banho e lojas de artigos esportivos demonstraram maior segurança.

A categoria `Top 10`, composta pelas dez maiores empresas emissoras de NF-e do estado da Paraíba, inclui empresas de grande porte atuantes nos setores industrial e comercial. Verificou-se que quatro dessas empresas utilizam sistemas de emissão de NF-e vulneráveis, evidenciando a gravidade do problema.

Finalizando a discussão desta seção, ressaltamos que, embora este estudo tenha se concentrado em empresas de uma localidade específica, a prevalência de vulnerabilidades nas chaves de acesso de NF-e e, particularmente, de NFC-e, provavelmente se estende a todo o território nacional. Essa inferência é corroborada pela constatação de que muitos dos provedores de sistemas de gestão financeira utilizados pelas empresas analisadas atendem clientes em diversas cidades e estados do país. As seções subsequentes apresentarão evidências adicionais que reforçam esta hipótese.

6. Análise de Sistemas de Código Aberto

Realizou-se uma busca por bibliotecas, APIs e sistemas de emissão de NF-e/NFC-e de código aberto na plataforma GitHub. Foram selecionados seis projetos, compostos por quatro bibliotecas e dois sistemas completos. A Tabela 1 apresenta informações detalhadas sobre cada projeto, incluindo indicadores de popularidade e uso, a linguagem de programação empregada e o número de colaboradores do repositório.

A análise revelou que a maioria das bibliotecas se concentra na implementação da lógica de geração e comunicação das notas fiscais com as SEFAZs autorizadoras, delegando a geração da chave de acesso ao sistema que as utiliza. A geração e leitura das notas fiscais são realizadas por meio de serialização e desserialização de objetos em formato XML. A transmissão e recepção de dados são efetuadas por meio de serviços web.

Tabela 1. Projetos relacionados à NFC-e selecionados no GitHub.

Projeto	Tipo	Forks	Stars	C	Ling.	URL (github.com/)
Nfe[1]	B	384	668	82	Java	/wmixvideo
Java_NFe [2]	B	237	604	16	Java	/Samuel-Oliveira
ERP-Desktop-Java [3]	S	26	42	1	Java	/MarcosGabrielL
DFe.NET [4]	B	485	757	96	C#	/ZeusAutomacao
sped-NFe [5]	B	543	1200	104	PHP	/nfephp-org
Emissor Nota Fiscal [6]	S	21	64	1	PHP	/LukasMeine

(Nota) “B”: bibliotecas; “S”: sistemas; “C”: total de contribuidores.

Constatou-se que as bibliotecas `DFe.NET` e `JavaNFe` não implementam a geração do `cNF` da chave de acesso. A biblioteca `Nfe`, desenvolvida em Java, contém a classe `NFGeraChave` responsável pela geração da chave de acesso. O método `geraCodigoRandomico` (Código 1) utiliza o construtor `java.util.Random()` com o dia e horário de emissão da nota fiscal como argumento. Duas observações são cruciais aqui. Primeiramente, a prática recomendada para aplicações de segurança exige o uso da classe `java.security.SecureRandom()` em detrimento da utilizada. Em segundo lugar, e de maior gravidade, a semente para o gerador é definida como o valor em milissegundos do *timestamp* da data de emissão da nota fiscal. Consequentemente, para uma mesma data e horário, os números gerados serão idênticos.

Essa abordagem no código introduz uma vulnerabilidade de previsibilidade explorável. A utilização do *timestamp* do momento de emissão como semente do gera-

dor, juntamente com a previsibilidade dos horários de emissão, possibilita a recriação da mesma semente e consequente geração do mesmo código numérico, revelando o valor da chave de acesso. Essa fragilidade é particularmente notável em estabelecimentos como restaurantes, supermercados e grandes lojas de departamento, onde o volume de emissão de notas fiscais é alto em curtos intervalos de tempo.

```
1 public String geraCodigoRandomico() {
2     final Random random = new Random(this.nota.getInfo().
          getIdentificacao().getDataHoraEmissao().toInstant().
          toEpochMilli());
3     return StringUtils.leftPad(String.valueOf(random.nextInt
          (100000000)), 8, "0");}
```

Código 1. Geração do cNF na biblioteca JavaNFe.

No sistema `ERP-Desktop-Java` (Código 2), a geração do `cNF` é realizada de forma aleatória utilizando a classe `java.util.Random()`. No entanto, devido a questões de previsibilidade e fragilidade de segurança [Ferguson et al. 2011], essa classe não é adequada para a geração de um código que garante o acesso aos dados da nota fiscal. A classe `java.security.SecureRandom()` deveria ter sido utilizada.

```
1 import java.util.Random;
2 Random r = new Random();
3 String cNF = String.valueOf(r.nextInt(100000000));
```

Código 2. Geração do cNF no sistema ERP-Desktop-Java.

A geração do `cNF` no sistema `Emissor Nota Fiscal`, desenvolvido em PHP, é implementada na classe `app/controllers/EmiteController.php`. O método utilizado (Código 3) emprega um valor fixo. O desenvolvedor, inclusive, inseriu o seguinte comentário: "deveria ser aleatório, mas não tem problema ser fixo". Essa afirmação, feita por um programador com experiência internacional, evidencia o risco de desconhecimento da documentação técnica e dos impactos decorrentes do não cumprimento das recomendações das notas técnicas da Receita Federal.

```
1 $std = new stdObject();
2 $std->cUF = substr($_POST['ibge_cidade'],0,2);
3 $std->cNF = '80070008';
```

Código 3. Geração do cNF no sistema 'Emissor Nota Fiscal'.

No projeto `sped-nfe`, identificou-se o uso da função `mt\_rand` no método de geração do `cNF` (Código 4). A função `mt\_rand()` gera um número aleatório de 8 dígitos para o código numérico, produzindo um valor entre 0 e 99.999.999. Caso o número gerado possua menos de 8 dígitos, zeros à esquerda são adicionados. Em seguida, é realizada uma validação que verifica se o valor consta na lista de valores inválidos especificados na norma técnica da NF-e (e.g., 11111111, 12345678, etc.) e se é diferente do `nNF`. Se o número gerado for inválido, o processo é repetido até que um valor válido seja obtido.

A utilização da função `mt\_rand()` não é recomendada devido à sua fragilidade criptográfica. Alternativas mais seguras incluem o uso de funções como `random\_int()`. Apesar disso, o projeto `sped-nfe` foi o que demonstrou maior aderência às recomendações da norma NT2019.001 [ENCAT 2023].

```php
public static function random($nnf = null) {
    do {
        $cnf = str_pad(mt_rand(0, 99999999), 8, '0', STR_PAD_LEFT);
    } while (!self::cNFIsValid($cnf) || (!empty($nnf) && intval($cnf)
        === intval($nnf)));
    return $cnf;}
```

Código 4. Geração do cNF no sistema sped-nfe.

7. Ferramenta para Detecção de Vulnerabilidade

A ferramenta web para análise de chaves de NFC-e foi implementada utilizando uma arquitetura cliente-servidor, seguindo o padrão REST (*Representational State Transfer*). A aplicação foi desenvolvida em Python (versão 3.11) com uso do framework Flask (versão 3.1) no backend, e HTML, Bootstrap 5 e JavaScript no frontend. A comunicação cliente-servidor é realizada através de requisições AJAX utilizando a API Fetch.

O sistema implementa validações de formato usando expressões regulares e tratamento de erros para garantir a integridade dos dados, validação de caracteres numéricos e a verificação de CNPJ consistente entre chaves.

Ao acessar a aplicação web (Figura 6), o usuário pode fornecer até cinco chaves de acesso que são enviadas para análise no servidor. Durante este processo, o serviço decompõe as chaves, verificando o formato e determinando o padrão de geração do cNF usando a classe NFCeAnalyzer. Após a análise, o servidor retorna ao cliente um objeto JSON que contém os resultados, incluindo o padrão identificado e o nível de vulnerabilidade associado a esse padrão.

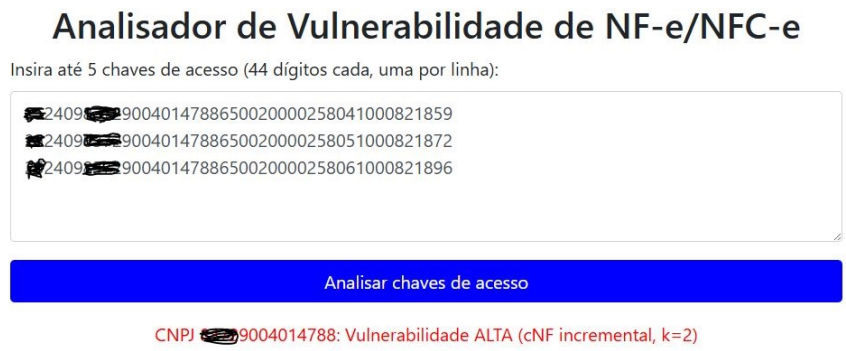

Figura 6. Ferramenta para detecção de vulnerabilidade nas chaves de acesso.

No exemplo apresentado na Figura 6 o resultado da análise indica que o cNF segue um padrão de alta vulnerabilidade do tipo incremental, com $k = 2$, ou seja, que a numeração do código cresce de dois em dois (00082185, 00082187, 00082189). Caso apenas uma chave de acesso seja informada, o sistema tentará inferir o valor da próxima chave de acesso considerando os métodos Fixo, Espelho e Incremental. Dessa forma, o usuário poderá verificar se a chave calculada é válida ao consultá-la no site da SEFAZ.

8. Validação Externa e Generalização dos Achados

Para avaliar a aplicabilidade da ferramenta (Seção 7) e, principalmente, validar externamente os achados do estudo de campo (Seção 5), investigando a generalidade do problema

para além do município de Campina Grande - PB, realizou-se uma análise complementar. Foram utilizadas 30 NFC-e coletadas aleatoriamente de repositórios públicos federais que agregam documentos fiscais de diversas origens geográficas, referentes às comprovações para prestação de contas da Cota para Exercício de Atividade Parlamentar (CEAP) de deputados federais e senadores [5].

O uso da ferramenta de análise nesse conjunto de dados revelou uma distribuição de vulnerabilidades (46,7% alta, 13,3% média, 40% baixa) notavelmente similar à observada no estudo de campo (Fig. 3). O método de geração de `cNF` mais frequente também coincidiu, sendo o Incremental (56%), seguido pelo Parcialmente Aleatório (22%), razoavelmente próximos aos valores encontrados no estudo de campo (Fig. 2).

A consistência entre os resultados obtidos em Campina Grande e nesta amostra de dados de diversas localidades fornece forte indício de que a vulnerabilidade na geração da chave de acesso da NFC-e não é um fenômeno local, mas sim um problema estrutural e de ampla abrangência no Brasil, corroborando os riscos apontados.

9. Conclusão

Até onde sabemos, este é o primeiro estudo a realizar uma análise e dimensionamento de uma vulnerabilidade crítica na geração da chave de acesso da Nota Fiscal Eletrônica, a qual expõe dados sensíveis de empresas e consumidores a acessos não autorizados. A análise de 200 empresas mostrou que 52% utilizam métodos inseguros na geração do código numérico da chave de acesso, sendo que 75% dessas empresas apresentam vulnerabilidades de alta severidade. Esses achados evidenciam um risco estrutural que compromete a confidencialidade das notas fiscais e pode ter impactos significativos em segurança empresarial, privacidade dos consumidores e conformidade legal.

Além do levantamento empírico, a investigação de seis projetos de código aberto no GitHub demonstrou que falhas na geração do `cNF` são comuns, às vezes decorrentes do uso inadequado de geradores de números pseudoaleatórios. Como resposta a essa lacuna, desenvolvemos uma ferramenta capaz de identificar o nível de vulnerabilidade a partir de uma ou mais chaves de acesso, contribuindo para a detecção e mitigação do problema.

Uma limitação do estudo de campo apresentado na Seção 5 foi ter sido realizado em uma única localidade, o que torna possível os resultados não refletirem com precisão o cenário nacional. No entanto, evidências sugerem que os índices de vulnerabilidade não possuem restrições geográficas ou econômicas, visto que muitas empresas utilizam sistemas desenvolvidos por fornecedores de software que atendem clientes em nível nacional. As análises apresentadas nas Seções 6 e 8 reforçam essa hipótese de que a insegurança na geração da chave de acesso da NFC-e é um problema estrutural.

Como continuidade do trabalho, propomos expandir o estudo para incluir mais empresas de diferentes localidades e setores, além de tornar a detecção de vulnerabilidade mais eficiente mediante integração aos serviços web das SEFAZs estaduais.

Por fim, diante da dimensão do problema descrito neste artigo, esperamos que empresas, desenvolvedores e autoridades fiscais adotem medidas imediatas para reforçar a segurança na geração da chave de acesso, garantindo a proteção dos dados de empresas e consumidores.

[5] www.camara.leg.br/cota-parlamentar/, www6g.senado.leg.br/transparencia/

Agradecimentos

Somos gratos pelo apoio financeiro no formato de bolsa estudantil e ajuda de custo concedidos pelo Instituto Federal da Paraíba (IFPB) mediante seleção nas Chamadas Interconecta de 2024 e 2025, Editais Nº 03/2024 e 01/2025, respectivamente.

Referências

Anderson, D., Sweeney, D., Williams, T., Camm, J., and Cochran, J. (2021). *Estatística Aplicada a Administração e Economia*. Cengage, São Paulo, 5 edition.

Bhattacharjee, K. and Das, S. (2022). A search for good pseudo-random number generators: Survey and empirical studies. *Computer Science Review*, 45:100471.

Bonfim, D. P., Moraes, D., Machado, H., Amorim, M. O., and Raimundini, S. L. (2012). Nota fiscal eletrônica: uma mudança de paradigma sob a perspectiva do fisco estadual. *ConTexto-Contabilidade em Texto*, 12(21):17–28.

Botacin, M. and Grégio, A. (2021). A [in]segurança dos sistemas governamentais brasileiros: Um estudo de caso em sistemas web e redes abertas. *arXiv preprint arXiv:2109.06068*.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., and Stein, C. (2022). *Introduction to algorithms*. MIT press.

Cunha, J. P. P. d. (2022). Nota fiscal eletrônica: arquitetura tecnológica e contábil. Monografia (Graduação). Universidade Federal de Uberlândia.

ENCAT (2023). Nota técnica 2019.001: Regras de validação. Disponível em `www.nfe.fazenda.gov.br/`. Acesso em: 12 nov. 2024.

ENCAT (2024). Manual de orientação do contribuinte. Disponível em `www.nfe.fazenda.gov.br/`. Acesso em: 10 fev. 2025.

Ferguson, N., Schneier, B., and Kohno, T. (2011). *Cryptography engineering: design principles and practical applications*. John Wiley & Sons.

Gonzaga, L. M. (2017). Percepções dos consumidores finais sobre dados informacionais com base na nfc-e (nota fiscal de consumidor eletrônica). Monografia (Graduação). Universidade do Extremo Sul Catarinense.

Hou, T. and Wang, V. (2020). Industrial espionage–a systematic literature review (slr). *computers & security*, 98:102019.

Johnston, D. (2018). *Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers*. Walter de Gruyter GmbH & Co KG.

Manoharan, A. P., Ingrams, A., Kang, D., and Zhao, H. (2021). Globalization and worldwide best practices in e-government. *International Journal of Public Administration*, 44(6):465–476.

Martins, R. (2024). Você conhece o novo golpe do boleto falso? Disponível em: `http://bit.ly/3Zekmdb`.

Santos, C. A. d. A. C. (2006). A nota fiscal eletrônica e o atual cenário do cibercrime. Disponível em: `www.migalhas.com.br/depeso/33537/a-nota-fiscal-eletronica-e-o-atual-cenario-do-cibercrime`.