



Plataforma para novos processos de migração e medição no varejo de energia com enfoque em cibersegurança

Tema: Sistemas de Controle, Automação e Proteção

Autores: Carlos José Alves Santos

Co-Autores: Alexandre Braga; Guilherme Maia Martins

Empresa: Way2 Technology; Centro de Pesquisa e Desenvolvimento em Telecomunicações; Auren

Resumo

Este artigo explora o desenvolvimento de uma plataforma para distribuidoras e comercializadoras de energia no Brasil, com foco em cibersegurança. A plataforma aborda novos processos simplificados no ambiente varejista do mercado de energia, estabelecidos pela Agência Nacional de Energia Elétrica (ANEEL) a partir da Consulta Pública 028/2023. A plataforma foi desenvolvida no contexto de um projeto P&D ANEEL e engloba os novos processos de mercado, tendo sido submetida a testes de segurança e registro de software.

A abertura do mercado de energia para todos os consumidores do grupo A trouxe desafios para os processos existentes de migração, cadastro e gerenciamento de unidades consumidoras. Os processos manuais, a ausência de uma estrutura robusta de APIs (interfaces de programação) e o alto volume de migrações geraram complexidade e sobrecarga. A CCEE (Câmara de Comercialização de Energia Elétrica) introduziu APIs para digitalizar os processos simplificados do varejo, o que representa um avanço significativo na digitalização do mercado.

A plataforma descrita neste artigo oferece funcionalidades para gerenciar processos de migração, medição e portabilidade de unidades consumidoras no novo modelo simplificado. Ela se integra às APIs da CCEE e a outros sistemas, permitindo uma gestão eficiente dos dados de medição. A segurança cibernética é crucial nessas aplicações, e parte importante do estudo e implementação foi a submissão a testes de segurança rigorosos, incluindo testes de intrusão.

O artigo conclui que a plataforma oferece uma solução eficaz para os desafios do varejo de energia no Brasil, enfatizando a importância da segurança cibernética. A atenção contínua à segurança é essencial para garantir a integridade das soluções implementadas para os agentes do setor elétrico.

1. Introdução

A utilização de plataformas para realizar atividades cotidianas para os agentes do setor elétrico é uma realidade há pelo menos duas décadas. Isso se aplica tanto a processos tradicionais e bem estabelecidos, como o gerenciamento e a coleta de dados de medição e a administração dos dados cadastrais dos clientes, quanto a novos processos que surgem com a modernização do setor elétrico, como a adoção de novas APIs obrigatórias impostas por agentes reguladores. Porém, todo o movimento de digitalização de

processos e utilização de ferramentas de alguma maneira conectadas à internet aumenta preocupações referentes a exposição de dados e ataques cibernéticos.

O presente artigo explora o desenvolvimento de uma plataforma para distribuidoras e comercializadoras. Esta plataforma é voltada para lidar com os novos processos simplificados da comercialização no varejo que estão sendo estabelecidos pela ANEEL a partir das saídas da Consulta Pública 028/2023 (ANEEL, 2025). O projeto foi desenvolvido no contexto do P&D Plataforma Tecnológica para Digitalização da Portabilidade e Agregação da Medição no Ambiente Varejista de Energia (PD-00061-0064). A solução englobou os novos processos do mercado e passou por diversos testes de segurança de mercado, além de ter sido objeto de registro de software.

Contexto do mercado

Com a abertura do mercado para todas as unidades consumidoras do grupo A, ficou claro que alguns dos atuais processos que eram utilizados para se realizar a migração, cadastro e gerenciamento de unidades consumidoras para o Ambiente de Contratação Livre (ACL) poderiam não ser ideais para lidar com o novo volume de unidades consumidoras que agora poderiam efetuar a contratação de energia bilateralmente (RUDDY, 2024). A partir do retorno de alguns agentes do setor, como distribuidoras e varejistas, ficou evidenciado que o modelo de migração, principalmente, estaria gerando uma sobrecarga de gerenciamento e análises. O fluxo de migração para distribuidora (Figura 1) e o fluxo de migração para comercializadora (Figura 2) são descritos abaixo.

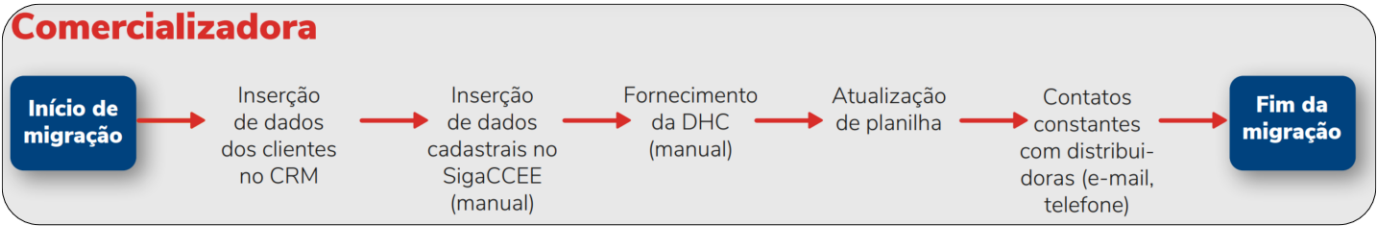


Figura 1 - Processos de migração seguidos pela comercializadora

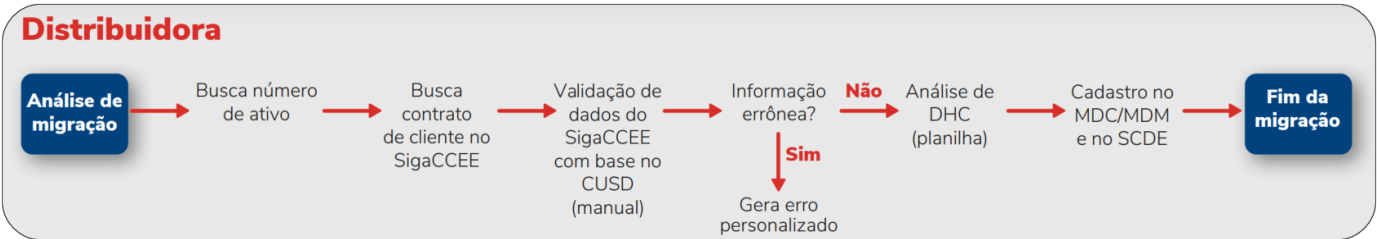


Figura 2 - Processos de migração seguidos pela distribuidora

Três eram os elementos principais que geravam complexidade na gestão destes fluxos. Primeiramente, os processos manuais, onde as migrações eram realizadas exclusivamente a partir de plataformas pré-existentes, com exceção dos passos diretos entre cliente e comercializadora ou entre comercializadora e distribuidora. Essas plataformas não permitiam personalização para os agentes do setor, e, embora fosse possível implementar automação por meio de *crawlers* ou outras tecnologias para requisição e preenchimento automático das informações, essa abordagem trazia riscos de retrabalho e custos e tempo dedicados à manutenção. Em segundo lugar, a inexistência de APIs para solicitar ou inserir informações dos clientes era uma preocupação constante entre os agentes. É comprovado (KHANYI et al., 2024) que a utilização de APIs facilita

processos manuais, porém, como é necessário que estas sejam disponibilizadas pelo agente que gerencia o fluxo principal, não havia possibilidade de se explorar este caminho inicialmente.

Por fim, o alto volume de migrações representava o fator mais evidente de sobrecarga. Embora, atualmente, a abertura esteja limitada ao grupo A, há uma preocupação sobre como a falta de digitalização poderia impactar o sistema em um cenário de abertura para as unidades consumidoras do grupo B, aumentando ainda mais a complexidade do processo.

Mudança de contexto e APIs da CCEE

Ciente das problemáticas decorrentes da abertura do mercado, foi instaurada a consulta pública 028/2023, que até o momento em que este artigo foi escrito passou por duas fases e recebeu contribuições de diversas empresas. Dentre essas, a CCEE apresentou uma proposta que representa um marco na digitalização dos processos simplificados do varejo. Além de sua participação na consulta pública, a CCEE promoveu um hackathon, durante o qual foi oficialmente lançada a primeira versão das APIs, conforme demonstrado na Figura 3.

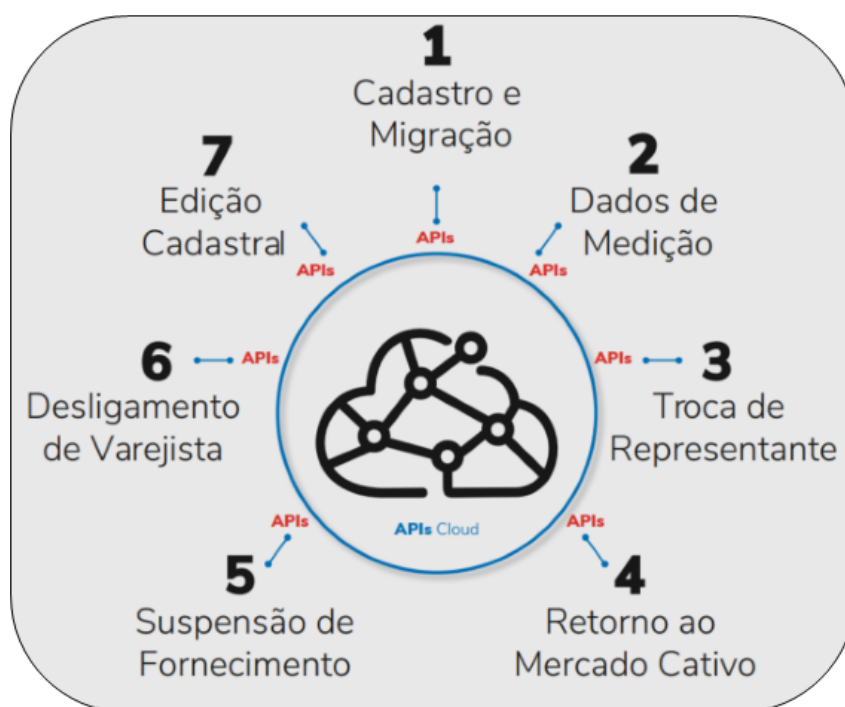


Figura 3 - Casos de uso e aplicações nas APIs da CCEE (Adaptado de CCEE, 2024)

De acordo com a CCEE, as APIs foram organizadas conforme a ordem de necessidade do mercado, com prioridade para os processos de cadastro e migração, seguidos pela edição cadastral. Essa nova ferramenta introduz uma dinâmica inovadora no mercado, permitindo uma abordagem mais eficiente para resolver os pontos de insatisfação dos clientes. Com isso, as plataformas anteriormente utilizadas pela CCEE, como SigaCCEE, SCDE e CliqCCEE, deixarão de ser empregadas para as etapas de migração, registro de pontos de medição e gerenciamento de clientes após a migração do modelo simplificado, respectivamente.

A dinâmica agora estabelece que distribuidoras e comercializadoras devem utilizar as APIs para realizar todos os registros associados a esses processos junto à CCEE. Não haverá mais interfaces ou plataformas específicas para esses procedimentos. A responsabilidade recai sobre os agentes, que podem empregar suas próprias equipes de TI para realizar a integração ou utilizar soluções oferecidas por outros agentes, como é o exemplo da solução apresentada neste artigo.

O novo modelo está previsto para entrar em operação no segundo semestre de 2025 e é importante destacar que, até o momento, apenas unidades que são exclusivamente consumidoras de energia podem

migrar pelo modelo simplificado. Unidades com autoprodução ou participantes de programas de resposta à demanda, por exemplo, devem seguir o modelo de migração tradicional. Unidades consumidoras que já migraram e são elegíveis para o modelo simplificado poderão eventualmente realizar a migração através desse modelo, embora ainda não tenha sido estabelecido um método para tal.

O planejamento para a liberação das APIs no mercado incluiu um período de teste sombra, iniciado em setembro de 2024 e estendendo-se até o final do ano, com a liberação parcial dos blocos. A partir de janeiro/25, as APIs foram oficialmente disponibilizadas, permitindo que as empresas do setor realizassem suas integrações, com a expectativa de que, até julho de 2025, todos os sistemas necessários estivessem integrados e plenamente operacionais.

De maneira resumida, as APIs supriram uma necessidade latente dos agentes que, de modo geral, demonstraram satisfação com sua implementação. No entanto, alguns pontos de retorno já podem ser observados: as migrações em 2024 ocorreram em ritmo acelerado, com mais de 20 mil ocorrências. Agora, os agentes começam a focar em clientes que anteriormente não eram prioritários, como aqueles com mini ou microgeração. O sistema, que atualmente não se aplica a esses cenários, poderia ser de grande valor para atender a essa nova demanda de UCs que passam a ser alvo das comercializadoras. Outro aspecto a ser considerado é que alguns processos ainda não estão disponíveis por meio das APIs, como, por exemplo, a situação em que um cliente, anteriormente alocado no varejo, deseja migrar para o modelo de atacado. O ponto central é que as APIs solucionaram uma necessidade significativa do mercado, embora possam sofrer algumas modificações com base no feedback recebido pela CCEE após o término do período de testes e nas definições futuras da ANEEL. Pode-se afirmar que as APIs da CCEE representam um grande avanço na digitalização do mercado e devem continuar gerando valor agregado para os agentes, uma vez que entre os serviços disponibilizados estão funcionalidades como o envio e acesso a medições, portabilidade de UCs entre varejistas e retorno ao mercado cativo. Os dois últimos, em particular, embora não sejam eventos recorrentes no mercado, tornam-se mais prováveis no novo cenário do ACL.

Importância da segurança cibernética nestas aplicações

Historicamente, as preocupações com segurança na geração e distribuição de energia estavam associadas à disponibilidade (por exemplo, detecção, prevenção de eventos de interrupção). À medida que o setor de energia evolui e incorpora Tecnologias de Informação e Comunicação (TICs) a sua operação, ameaças cibernéticas e contra a privacidade tornam-se mais sérias.

As questões de segurança cibernética em sistemas sofisticados de monitoramento de consumo de energia são comumente alcançadas por meio da implementação de controles (salvaguardas e medidas preventivas) técnicos e gerenciais, bem como pela sensibilização das pessoas para a aderência a práticas seguras, ajuste de comportamentos e observância a regulamentos e padrões. No contexto da segurança digital, uma grande parcela do trabalho de defesa reside na identificação precoce de fragilidades que possam ser exploradas de forma mal-intencionada em ataques concretos. Idealmente, a presença de fragilidades deve ser prevenida desde o princípio da criação dos sistemas computacionais. Por essa razão, existe também um esforço coordenado para obter garantias de segurança incorporadas desde o início do projeto.

Por outro lado, as violações de privacidade não podem ser atribuídas apenas aos ataques cibernéticos e explorações de vulnerabilidades. Pelo contrário, a divulgação de informações pessoais pode ocorrer durante o uso normal de sistemas, APIs e aplicativos, quando tecnologias de preservação de privacidade não são usadas no design do sistema. Por exemplo, as infraestruturas avançadas de medição das redes inteligentes (*Smart Grids*) precisam coletar dados detalhados de consumo de energia para tarefas comerciais comuns, como por exemplo a precificação dinâmica e as previsões de demanda. Essas tarefas podem representar riscos significativos aos dados dos consumidores e comprometer sua privacidade. Além disso, em caso de vazamento de dados de medição, seria possível deduzir os hábitos dos consumidores. Um exemplo simples é identificar quando os consumidores estão em casa (alto consumo) ou fora de casa (baixo consumo).

As questões de privacidade podem ser tratadas com a privacidade diferencial (DWORK, 2006), uma tecnologia de preservação da privacidade que pode proteger os direitos de privacidade dos consumidores, permitindo ao mesmo tempo o acesso a análises úteis. Nessa abordagem, o ruído estatístico é adicionado aos resultados das consultas em um conjunto de dados, a fim de dificultar a identificação de informações pessoais. Esse ruído geralmente é gerado a partir de distribuições estatísticas como Laplaciana ou Gaussiana e é modulado conforme o equilíbrio entre privacidade e utilidade dos dados. Para o setor elétrico, essa técnica é importante porque permite análise de séries temporais de consumo, distribuição e negociações em aplicações como previsão de demanda e até mesmo precificação, garantindo que os padrões individuais de consumo permaneçam protegidos contra a proteção da privacidade individual dos consumidores (PAIXÃO et al., 2025).

2. Desenvolvimento

Funcionalidades da plataforma

A plataforma é uma ferramenta voltada para o gerenciamento de processos de Migração, Medição e Portabilidade de Unidades Consumidores que se enquadrem no novo modelo simplificado que está sendo estabelecido pelos órgãos reguladores. Com a utilização da solução, é possível monitorar e responder solicitações de migração de unidades consumidoras para o mercado livre, bem como acompanhar e responder solicitações de portabilidade de unidades consumidoras entre comercializadoras varejistas. Além disso, é possível utilizar a plataforma para efetuar o envio e o ajuste de dados de medição destas unidades consumidoras.

Os módulos de migração e medição podem ser utilizados por distribuidoras e comercializadoras. O módulo de Portabilidade é de uso exclusivo da comercializadora, uma vez que este é o único agente envolvido neste processo.

A Figura 4 demonstra a arquitetura da plataforma, e deixa evidente a natureza modular da solução. Compreendendo que os agentes do setor elétrico já fazem uso de outras soluções tecnológicas, a plataforma oferece a capacidade de se integrar a essas ferramentas, assegurando a digitalização completa dos processos. Os dados de medição podem ser solicitados diretamente aos coletores de dados das distribuidoras, enquanto as informações relacionadas aos clientes são requisitadas das plataformas de gerenciamento de clientes, como por exemplo Salesforce, SAP, entre outros CRMs e ERPs.

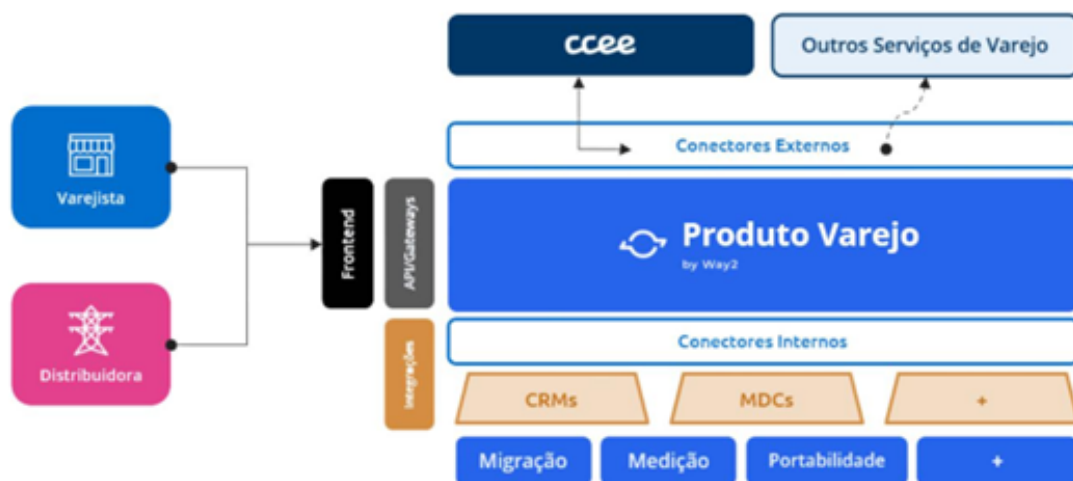


Figura 4 - Arquitetura da plataforma

A plataforma também funciona de maneira isolada, disponibilizando todas as funcionalidades necessárias para que as empresas realizem os seus processos relacionados à migração, portabilidade e medição do varejo simplificado.

A integração eficiente com as APIs da CCEE tem se mostrado um ponto crucial para a otimização dos processos no setor elétrico. Soluções tecnológicas que permitem essa integração sem a necessidade de desenvolvimento adicional por parte das empresas oferecem uma gestão mais ágil e precisa dos dados de medição. Tais sistemas possibilitam ajustes automáticos e manuais nas informações, assegurando a precisão e a consistência necessárias para a gestão eficiente desses dados.

Sobre os módulos da plataforma

A plataforma foi projetada para permitir a criação de novas solicitações de migração para comercializadoras, além de possibilitar o recebimento dessas solicitações pelas distribuidoras. Com a implementação de filtros, é possível priorizar os pedidos com base no prazo remanescente para a conclusão da migração. Considerando que o prazo de resposta das distribuidoras foi consideravelmente reduzido, todos os processos implementados visam garantir maior agilidade e praticidade no atendimento às solicitações.

De maneira geral, todo o fluxo da Figura 5 está sendo gerenciado pela plataforma.

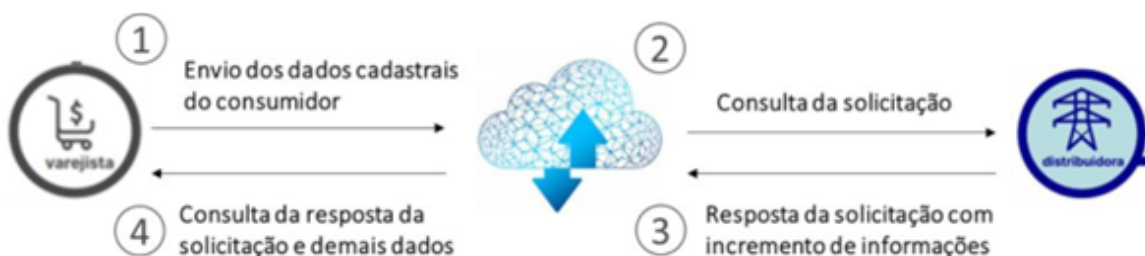


Figura 5 - Novo fluxo de migração estabelecido pela CCEE (CCEE, 2024)

A responsabilidade pelo envio dos dados de medição permanece com a distribuidora, que transmite apenas os dados de energia ativa em intervalos de 5 minutos. A plataforma assegura a compatibilidade com o novo

modelo proposto pela CCEE, além de permitir ajustes nos dados, tanto para atender às regras regulatórias quanto para corrigir os principais erros que podem ser detectados nos medidores.

O fluxo é representado na Figura 6.

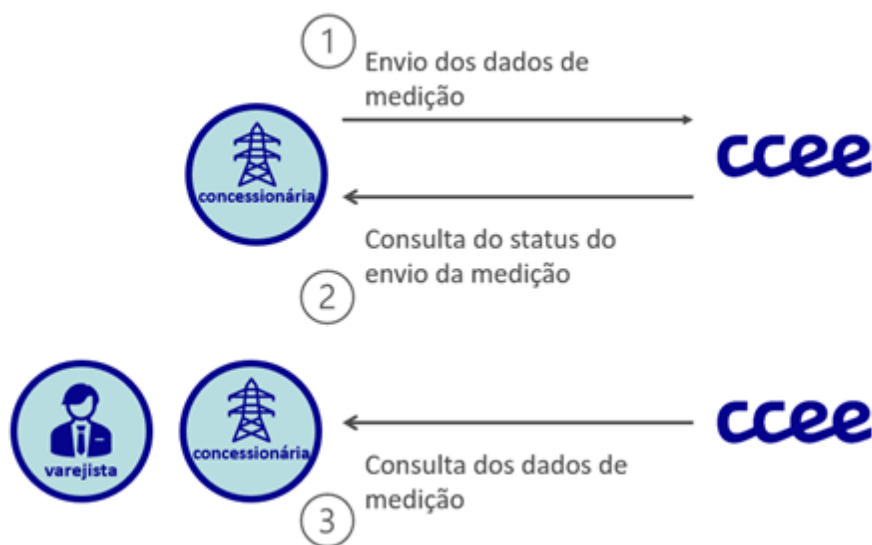


Figura 6 - Fluxo de envio e consulta dos dados de medição (CCEE, 2024)

Sobre possibilidade de disponibilização para clientes e correlação com segurança

A solução é oferecida aos clientes de duas maneiras. A primeira é através do modelo Software as a Service (SaaS), que, embora seja mais suscetível a vulnerabilidades devido à sua hospedagem em recursos acessíveis externamente, é uma opção preferida pelas comercializadoras, que frequentemente optam por soluções SaaS. Nesse contexto, é fundamental não apenas proteger contra acessos e ataques externos, mas também assegurar a segurança interna dos dados das comercializadoras. Isso envolve garantir que cada agente tenha acesso exclusivo aos seus próprios dados, prevenindo qualquer tipo de exposição indesejada.

Em contrapartida, há também a possibilidade de instalação da solução diretamente na infraestrutura do cliente, no modelo *on-premises*. Esse caso de uso é mais comum entre distribuidoras, que geralmente preferem internalizar as soluções em suas próprias instalações. Nesse cenário, os ataques externos se tornam uma preocupação maior para a distribuidora, embora a plataforma ainda precise se comunicar com as APIs da CCEE e outras APIs de terceiros, essenciais para o envio e requisição de dados críticos. Portanto, os testes de segurança realizados na plataforma abrangem todos esses casos de uso.

Testes de segurança na plataforma

Segurança não é uma característica que pode ser simplesmente adicionada ao software. Em vez disso, ela se comporta como uma propriedade emergente obtida a partir de como o software é construído e usado. Assim, o software seguro é aquele que contempla com um grau alto de confiança justificada, mas não com certeza, um conjunto substancial de propriedades explícitas de segurança e de serviços de segurança. Por isso, o software seguro resulta de um ciclo de desenvolvimento com segurança e de uma arquitetura de segurança, cujas propriedades emergentes se expressam durante o seu funcionamento.

Durante o projeto foram adotadas boas práticas de desenvolvimento ágil de software seguro que se torna viável com grande uso de automação e o apoio dos desenvolvedores. Isto não significa que, por exemplo, foram evitados os testes de intrusão manuais, detalhados e demorados, realizados por hackers éticos. Eles aconteceram, porém, fora do ciclo curto de desenvolvimento. Já as verificações e testes de segurança

automatizados complementam os testes manuais e foram usados para ganhar escala na testagem com detecção rápida dos problemas simples.

Neste projeto, adotou-se os princípios DevSecOps de integração contínua de processos e tecnologias de segurança às práticas da cultura DevOps (BRAGA, 2023). A adoção plena da cultura DevSecOps é uma jornada em que a automação das atividades de segurança avança em estágios. No início do desenvolvimento, o time de desenvolvimento adotou um repositório de software e boas práticas de programação, compilação e empacotamento. Com isso, a equipe de segurança foi capaz de incentivar a adoção de práticas de programação segura com o auxílio de ferramentas SAST (*Static Application Security Testing*) e SCA (*Software Composition Analysis*), sobre o repositório de código fonte e geração do software executável.

No segundo estágio, o time de software adotou as práticas fundamentais de construção ou geração, integração e teste contínuos. A existência de um ambiente de teste tornou possível a realização de varreduras de vulnerabilidades automáticas com o auxílio de ferramentas DAST (*Dynamic Application Security Testing*). No terceiro estágio, a automação das tarefas corriqueiras tornou possível a realização de testes com frequência alta e escala. Além disso, a construção e instalação automatizadas e as varreduras de vulnerabilidades e testes com ferramentas DAST são complementados, no ambiente de implantação (e produção) por testes de intrusão (manuais) para avaliação de segurança na lógica de negócios, como por exemplo, testes de segurança em APIs (OWASP, 2023).

Finalmente, no último estágio, para as ações de monitoramento contínuo e proteção em tempo de execução da aplicação no ambiente de produção, usam-se as ferramentas de proteção automática da aplicação, como por exemplo, um WAF (*Web Application Firewall*), uma ferramenta de segurança bastante comum oferecidas por provedores de nuvem.

Verificações de segurança e testes de intrusão

O processo de teste de intrusão (*Penetration Test*, ou simplesmente Pentest) envolve várias etapas. O objetivo do processo é ter uma interação do ciclo em cada momento ou módulo desenvolvido do sistema alvo a fim de eliminar possíveis explorações através de ameaças presentes e brechas de segurança. Os testes de intrusão dos protótipos seguiram as etapas:

- Reconhecimento - Verificação e análise da infraestrutura do alvo.
- Coleta de informações - Como tecnologias usadas e informações públicas disponíveis.
- Análise da superfície de ataque - Análise de possíveis pontos de entrada e ataque.
- Planejamento do ataque - Planejamento do ataque com exploits e rotinas de ataque.
- Exploração de vulnerabilidades - Execução de exploits, scripts e exploração de vulnerabilidades em brechas conhecidas ou não ao sistema alvo.
- Pós exploração - Verificação e obtenção de informações sensíveis ao sistema, como senhas de bancos de dados e outras informações pertinentes.
- Relatório - Escrita do relatório de pentest.
- Publicação de resultados - Comunicação às partes interessadas do teste realizado.

Ao longo do desenvolvimento do projeto, foram realizados testes de intrusão sobre cada protótipo disponibilizado pela equipe de desenvolvimento. Em particular, a estratégia de teste foi efetivada em três aspectos:

usuário - sistema; sistema - sistema (comunicação interface e API); sistema - banco de dados. Cada aspecto da estratégia foi abordado em três elementos táticos listados a seguir:

- **INTERFACE** - Representação visual do sistema com comunicação direta com o usuário. Ataques focados na interface, tais como Ataques do tipo XSS (*Cross Site Scripting*), manipulação de usuários e permissões do sistema.
- **API** - Interface de comunicação entre a interface, sistema e banco de dados. Ataques de elevação de privilégios, verificação de permissionamento e definições de papéis baseados na regra de negócio do sistema.
- **COMUNICAÇÃO** - Verificação do canal de comunicação entre interface, sistema e banco de dados. Ataques de interceptação de informações, com possível quebra de integridade e autenticidade dos dados trafegados.

Cada componente tático foi operacionalizado em tarefas específicas, conforme a necessidade:

- **Verificação de API** - Verificação das chamadas da API e permissionamento dos papéis.
- **Verificação de Imagem Docker** - Busca automática de vulnerabilidades conhecidas.
- **Validação de ambiente** - Criação local e validação de ambiente da imagem Docker.
- **Execução do pentest** - Sobre a vulnerabilidade da aplicação construída a partir da imagem Docker.

3. Conclusão

A abertura do mercado livre de energia no Brasil apresentou desafios consideráveis para os agentes do setor, especialmente na gestão de processos de migração, portabilidade e medição de unidades consumidoras. A implementação de APIs pela CCEE significou um avanço crucial na digitalização do mercado, simplificando e otimizando esses processos. A plataforma desenvolvida e apresentada no artigo oferece uma solução completa para gerenciar os novos processos do mercado varejista, integrando as APIs da CCEE e outras soluções tecnológicas já em uso pelas empresas. Ela se destaca pela capacidade de monitorar e responder a solicitações de migração e portabilidade, além de enviar e ajustar dados de medição. O sistema se adapta à necessidade de cada empresa, podendo ser integrado a outras plataformas ou funcionar de forma independente, incluindo funcionalidades para os processos de migração, portabilidade e medição do varejo simplificado.

A segurança foi um aspecto central no desenvolvimento da plataforma. Testes rigorosos de intrusão foram realizados para assegurar a proteção dos dados dos clientes, abrangendo diferentes cenários, como o acesso via SaaS, mais comum entre comercializadoras, e a instalação local (*on-premises*), preferida por distribuidoras. A metodologia empregada nos testes de segurança envolveu a análise de vulnerabilidades em diversos níveis, incluindo interface, API e comunicação entre os sistemas. As boas práticas de desenvolvimento de software seguro, com a integração dos princípios DevSecOps, foram incorporadas ao projeto desde o início, garantindo a verificação contínua de segurança em todas as etapas.

Por fim, a plataforma, com sua estrutura modular e capacidade de integração, demonstra ser uma ferramenta valiosa para os agentes do setor, permitindo que se adaptem às mudanças regulatórias e às demandas do mercado de forma eficiente e segura.

4. Referências bibliográficas

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA. **Consulta Pública nº 028/2023**. Disponível em: <https://antigo.aneel.gov.br/web/guest/consultas-publicas>

RUDDY, Gabriela. **Na abertura do mercado livre de energia, comércio e serviços saem na frente**. InfoMoney, 29 ago. 2024. Disponível em: <https://www.infomoney.com.br/business/na-abertura-do-mercado-livre-de-energia-comercio-e-servicos-saem-na-frente/>. Acesso em: 19 de janeiro de 2025.

KHANYI, Mduduzi B.; XABA, Sfundo N.; MLOTSHWA, Nokunqoba A.; THANGO, Bonginkosi; MATSHAKA, Lerato. **A Roadmap to Systematic Review: Evaluating the Role of Data Networks and Application Programming Interfaces in Enhancing Operational Efficiency in Small and Medium Enterprises**.

Sustainability, v. 16, n. 23, p. 10192, 2024. Disponível em: <https://doi.org/10.3390/su162310192>.

CÂMARA DE COMERCIALIZAÇÃO DE ENERGIA ELÉTRICA. **Editais Hackathon CCEE**. 2024.

BRAGA, A. **Desenvolvimento ágil de software seguro e cultura DevSecOps**. In: **XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2023)**, Anais [...].

DWORK, C. **Privacidade diferencial**. Em: **Colóquio Internacional sobre Autômatos, Linguagens e Programação (ICALP)**, 2006, pp. 1–12.

OWASP. **Top 10 de segurança da API OWASP - 2023**. Disponível em: <https://owasp.org/www-project-api-security>.

PAIXÃO, ACP; CAMARGO, GFL; BRAGA, AM (*Submetido*) **Testando bibliotecas de código aberto para contagens privadas e médias em séries temporais de medição de energia**. In: **20th European Dependable Computing Conference (EDCC 2025)**, 2025.