JANELA DE TRANSPARÊNCIA DE AUDITORIA

1. OBJETIVO

1.1. A janela de transparência de auditoria visa apresentar à contratante os laudos técnicos comprobatórios e detalhados de que o sistema eleitoral sofreu exaustiva carga de testes e análises de auditoria, comprovando e gerando transparência aos procedimentos adotados para sua execução e formulação. Visa maximizar a segurança do processo eleitoral, garantido que o Sistema Eleitoral se submeteu ao processo de auditoria por empresa especializada.

2. ROTEIRO

2.1. Apresentação na sede do Cofen, pela empresa que auditará o processo, de laudos detalhados dos testes efetuados no Sistema Eleitoral com os requisitos de segurança exigidos nesse termo de referência, após contratação do Sistema Eleitoral.

2.1.1 A empresa fornecedora do Sistema Eleitoral disponibilizará os acessos e recursos necessários para o fiel cumprimento do requisitado nessas especificações.

2.2. O laudo técnico deverá conter, minimante, evidências de que foi averiguado o conteúdo da prova de conceito abaixo, e serão aplicados aos ambientes de homologação e produção que hospedam o Sistema Eleitoral:

2.2.1. Busca de falhas em aplicação e que poderiam ser exploradas por atacantes danificando ou modificando o sistema e o resultado final das eleições. Por ser um processo eleitoral que utilizará a rede de computadores como base de seu desenvolvimento e uma página *Web* como camada de apresentação, trabalhará fundamentalmente sob a camada 7 do modelo OSI, devendo ser realizado o processo de auditoria de segurança de aplicação por meio de testes específicos para aplicações *Web*, incluindo os testes do OWASP TOP10, requisitos do PCI-DSS, ISO-27001, dentre outros.

2.2.2. Os serviços de Auditoria Informática devem contemplar:

a) Análise Funcional: realização de estudo geral da aplicação, adquirindo uma visão global das funcionalidades;

b) Análise Técnica: realização de estudo dos módulos que compõem a aplicação, determinando como eles se interagem (Ex. objetos distribuídos entre diferentes servidores, etc.) e destacando as entradas e saídas do sistema que podem ser visíveis desde a Internet. Garantir que cada módulo faz única e exclusivamente o que foi especificado de modo a não haverem códigos divergentes ou maliciosos que coloquem em risco a integridade, confidencialidade e autenticidade dos dados e/ou do sistema de eleição como um todo ou em partes, bem como quaisquer ouros critérios estabelecidos no presente Termo de Referência;

c) Desenvolvimento de testes: preparação do cronograma de testes de aplicação e os tipos de testes que serão executados;

d) Aplicação de testes: realização de todo tipo de testes de sistemas, tomando nota do seu resultado e, em caso de se obter novas possíveis falhas, retorna-se para a fase de desenvolvimento de testes para tentar explorá-las, conforme previsto no termo de referência do sistema automatizado para o processo eleitoral e seus anexos;

e) Ambiente de teste: a Contratada deverá realizar uma exaustiva revisão nas aplicações auditadas abrangendo os seguintes aspectos da segurança da informação:

1 - Validação de entradas: Injeção (*Injection*) de código malicioso; criação e alteração de comandos SQL; execução de comandos do sistema operacional; execução de comandos e observação de dados em diretórios não permitidos; utilização de byte null com a finalidade de alterar os parâmetros de uma *Universal Resource Locator - URL*, etc;
2 - Canonização de *URL*: Ataques que exploram a capacidade de armazenar caracteres com múltiplos bytes de codificação *Unicode* ou outras que permitem ocultar ações e ataques que utilizam diferentes possibilidades de codificação de *URL* que aceitam os servidores *web*;
3 - Manipulação de parâmetros: Ataques de modificação de dados enviados entre o cliente e a aplicação *web* no cabeçalho *HTTP* ou *HTTPS*, requisições de *URL*, campos de formulários e informações armazenadas pelo servidor *web* no navegador (*cookies*);
4 - Autenticação e Gestão de Sessões: Busca exaustiva de senhas. Ataques baseados na falsificação de credenciais reais ou evitando a sua necessidade mediante a exploração de dependências existentes no aplicativo ou por meio de ataques diretos ao aplicativo. Furto de dados, Interceptação de tráfego e Ataque de personificação;
5 - *Overflows* (transbordamentos/sobrecargas): Ataques que permitem a execução de código malicioso no *Heap* (memória estática), na pilha do processo, etc;
6 - Fugas de Informação: Análise do código fonte para localizar comentários que possam ajudar os programadores a incrementar o processo de documentação; revisão para descobrir estruturas ou informação de depuração não eliminada; descoberta de mensagens e códigos de erro para obter informação de aplicações *web*, sistemas operacionais, bases de dados, etc;
7 - Criptografia: Ataques que exploram o uso de algoritmos criptográficos fracos e outros baseados na captura de dados cifrados e seu uso para ter acesso a senha cifrada ou ao texto plano;
8 - Assinatura Digital ICP-Brasil: Verificação de assinaturas digitais conforme as normas vigentes da ICP-Brasil;
9 - Configurações: Ataques que empregam contas de usuário ou do sistema criadas por padrão nas implementações, explorando vulnerabilidades de configurações deficientes ou a falta de atualização da aplicação *web*;
10 – ***Exploits*:** Planejar e executar testes utilizando *Exploits* que explorem, unicamente ou conjuntamente, vulnerabilidades nos seguintes quesitos: Sistema Operacional; Banco de Dados; Servidor Web; Protocolos da rede/internet; Linguagem de Programação; Tecnologia de Criptografia; *Firewall*; IDS; IPS;
11 – Identificação e análise conclusiva dos itens de log: logs de sistema operacional, logs da aplicação, logs do firewall, logs do IDS/IPS, senhas, credenciais, trilha de auditoria e *rollback*.

f) Validação e Teste do algoritmo criptográfico e função de *hash* (sequência única de identificação de informação) utilizada na alteração da senha pelos usuários finais: Visando garantir o sigilo da senha do usuário, ou seja, constatar que nenhum agente envolvido com o processo de análise, desenvolvimento e interlocução do processo eletrônico, tais como programadores, analistas, técnicos, representantes do Contratante,

poderão conhecer qualquer que seja a senha de votação utilizada por qualquer eleitor do sistema automatizado do processo eleitoral, deverão ser efetuadas verificação de padrões de programação segura, análises de componentes de transmissão e análises de guarda das informações.

2.2.3. Garantias de premissas do processo eleitoral

2.2.3.1. Garantias ao eleitor de que o voto é secreto: O voto é secreto e o sistema tem a obrigatoriedade de assegurar o sigilo e inviolabilidade do voto do eleitor. Na versão assinada digitalmente não pode existir a possibilidade de rastrear o voto dos eleitores, ou seja, não há como associar um voto a um eleitor, os trabalhos de auditoria garantem ao eleitor essa premissa.

2.2.3.2. Garantias ao eleitor de que seu voto realmente foi computado para o candidato escolhido: Serviços de análises com exaustão nos códigos fontes da aplicação assinada digitalmente à procura de falhas ou códigos maliciosos que pudessem modificar o resultado das eleições. Garantias de que não há nada nocivo que pudesse manipular o resultado das eleições, tanto nos códigos fontes auditados quanto no código binário assinado digitalmente.

Certificação de recursos implementados pelo sistema que permita ao eleitor confirmar o registro de seu voto e de que seu voto integra o total de votos computados.

2.2.4. Testes de performance e *stress* de sistema

2.2.4.1. Utilizando ferramentas profissionais o sistema deverá ser estressado a 125% de sua capacidade nominal de eleitores realizando duas simulações do processo eleitoral. Uma simulação da aplicação será em bancada de testes e outra simulação da aplicação em ambiente de produção utilizando a internet.

2.2.4.2. Requisitos para execução dos testes:

1 - A empresa que desenvolver a aplicação Web Eleitoral fornecerá os dados necessários para os testes de *stress* do sistema;

2 - A aplicação a ser utilizada para execução dos testes será de propriedade e responsabilidade da empresa contratada;

3 - Os testes deverão ser efetuados tanto no ambiente de homologação quanto no ambiente de produção, cujos horários para execução serão acordados entre as empresas de desenvolvimento e de auditoria.

2.2.5. Validação e testes do ambiente de produção do ponto de vista da segurança e confiabilidade

2.2.5.1. A Contratada deverá verificar:

1 - Validação de arquitetura de redes;

2 - Verificação de *hardenização* (aplicação de procedimentos de segurança) de servidores de aplicação;

3 - Verificação de *hardenização* de servidores de banco de dados;

4 - Verificação de sistemas de balanceamento de carga (*Load balance*);

5 - Verificação de Firewall de Alta disponibilidade (*High Avaliability* – HA);

6 - Teste de intrusão e verificação de resposta a incidentes;

7 - Teste de energia elétrica (*Nobreak* e geradores de energia);

8 - Testes de outros itens que de alguma forma provoquem impacto no ambiente em produção.

2.2.5.1.1. A auditoria poderá, mantidas suas competências e responsabilidades contratuais, homologar validações relacionadas à infraestrutura do *datacenter* por meio de certificações obtidas de institutos que regulam serviços de missão crítica, tais como:

- Certificados em vigor, baseados na norma ANSI/TIA 942 ou equivalente que se aplica a infraestrutura de um *datacenter*, que comprovem que a infraestrutura do local de hospedagem da solução automatizada para o processo eleitoral possua: capacidade de execução, sem interromper a operação dos serviços contratados, de manutenções preventivas e corretivas de forma programada, de conserto, de troca, de remoção ou de inclusão de elementos em ambiente de produção, de teste dos componentes físicos e lógicos do sistema; mais de uma via de distribuição de energia; HVAC, quadros de distribuição, gerador e UPS redundantes; alimentação dual para todos os equipamentos de TI; cabeamento estruturado que seja dedicado para os serviços contratados; disponibilidade mínima de 99,9% para o dia da eleição.

2.2.5.1.2. Certificado(s) em vigor, baseados nas normas ISO 9001 e 27002, ou normas equivalentes, que comprove(m) a gestão da segurança da informação e da qualidade dos processos relacionados à hospedagem e continuidade dos serviços mantidos pelo data center.