SERVIÇO PÚBLICO FEDERAL

CONSELHO FEDERAL DE ENGENHARIA E AGRONOMIA - CONFEA

DESPACHO CEF

Processo: 00.004888/2023-54
Tipo de Processo: Eleições: Procedimentos Gerais
Assunto: Requer esclarecimentos sobre as Eleições Gerais do Sistema Confea/Crea e Mútua
Interessado: José Manoel Ferreira Gonçalves

Ao Senhor José Manoel Ferreira Gonçalves

Em resposta ao requerimento administrativo apresentado por Vossa Senhoria, no qual requer informações e esclarecimentos sobre as Eleições do Sistema Confea/Crea e Mútua, temos a informar o seguinte:

1) Quem vai estar apto a votar?

De acordo com a Resolução nº 1.114, de 2019 - Regulamento Eleitoral, todo profissional registrado e em dia com as obrigações perante o Sistema Confea/Crea até 30 (trinta) dias antes da data da eleição é considerado eleitor, independente da modalidade profissional, sendo o voto facultativo. O Calendário Eleitoral aprovado pela Decisão Plenária nº PL-0983/2023, previu o dia 18 de outubro como sendo a data-limite para quitação de eventuais débitos pelos profissionais para fins de ser considerado eleitor. O profissional inadimplente após essa data não pôde ser incluído na relação de profissionais aptos a votar na circunscrição do Crea, ainda que comprovasse ter quitado seus débitos posteriormente.

Os Creas observaram essa data para fins de fechamento de listagens de eleitores, não sendo permitida a inclusão de eleitores após essa data (artigos 53 e 62, da Resolução nº 1.114, de 2019 - Regulamento Eleitoral).

2) Será necessário um novo cadastro?

A Comissão Eleitoral Federal, através da Gerência de Comunicação do Confea promoveu ao longo do ano, diversas campanhas sobre a conscientização da necessidade de atualização cadastral por parte dos profissionais do Sistema Confea/Crea e Mútua com a finalidade de recebimento da senha através do e-mail e do celular cadastrados no banco de dados do Regional. Não houve a necessidade de qualquer cadastro prévio para acesso ao ambiente de votação. Mas tão somente e observância aos requisitos informados no item anterior.

3) Como será gerada a senha que habilita o eleitor a votar?

Conforme manifestação da empresa Webvoto (Sei nº 0814322), as senhas foram geradas em uma biblioteca geradora de números aleatórios criptográficos (CSPRNG, do inglês "Cryptographically

Secure Pseudo-Random Number Generator"). Este gerador de números pseudoaleatórios (PRNG) atende a seguintes propriedades para uso em criptografia:

• Próximo-bit Imprevisibilidade: Dado os primeiros k bits de uma saída aleatória, o k+1 bit é imprevisível e independente dos primeiros k bits.

• Backtracking resistance: Mesmo que partes da saída do gerador sejam conhecidas, devem ser computacionalmente inviáveis reconstruir sequências anteriores que tenham sido produzidas.

4) Essa senha é única dentre todos os eleitores?

A Webvoto informa que seguindo boas práticas de segurança não armazena as senhas dos eleitores, sendo assim é impossível saber se o CSPRNG criou duas senhas iguais.

5) Existe alguma validação dessa senha que impossibilite de ser reutilizada?

As senhas são utilizadas para o eleitor votar, como ele só pode votar uma única vez, pode-se dizer que a senha só pode ser utilizada uma vez.

6) Essa senha é gerada a partir de algum dado do eleitor? Quais?

As senhas são geradas conforme descrito no item 3, de modo que não é utilizado qualquer dado do eleitor.

7) Qual o provedor que irá hospedar o site (front) para o sistema de votação?

Os requisitos estabelecidos no processo licitatório exigem altos níveis de segurança, confiabilidade e disponibilidade do serviço, o que leva a uma necessidade de disponibilização, por parte da contratada, de uma estrutura robusta para suportar o sistema dentro destes requisitos.

A contratada disponibilizou os serviços dentro da plataforma Microsoft Azure, que é uma plataforma de computação em nuvem abrangente e altamente escalável oferecida pela Microsoft. Ela oferece várias vantagens em termos de aplicação, bem como requisitos rigorosos de segurança e disponibilidade.

Em um foco mais detalhado dos itens elencados, podemos apresentar alguns deles como os que seguem:

1. Como vantagens temos:

a) Escalabilidade e Flexibilidade: permite dimensionar seus recursos de computação, armazenamento e rede de acordo com as demandas do seu aplicativo, possibilitando aumentar ou diminuir recursos conforme necessário, evitando custos excessivos e garantindo que sua aplicação seja capaz de lidar com picos de tráfego.

b) Variedade de Serviços: oferece uma ampla gama de serviços, desde máquinas virtuais e bancos de dados até inteligência artificial e Internet das Coisas (IoT), permitindo criação e disponibilização de aplicativos altamente especializados usando os serviços adequados para suas necessidades.

c) Rede Global de Data Centers: possui data centers distribuídos em várias regiões do mundo, permitindo que você hospede seus aplicativos próximos aos seus usuários finais, melhorando o desempenho e a latência.

d) Segurança Avançada: oferece ferramentas avançadas de proteção de dados, detecção de ameaças e conformidade regulatória, permitindo controlar o acesso aos seus recursos e proteger seus dados de forma robusta.

e) Disponibilidade Elevada: oferece acordos de nível de serviço (SLAs) que garantem alta disponibilidade para seus serviços, permitindo que seus aplicativos possam ser executados de forma confiável e com pouca interrupção.

f) Ferramentas de Gerenciamento e Monitoramento: fornece uma série de ferramentas para monitorar e gerenciar seus aplicativos, como o Azure Monitor e o Azure Security Center, possibilitando identificar e resolver problemas rapidamente.

2. Como Requisitos de Segurança e Disponibilidade na Microsoft Azure:

a) Criptografia de Dados: Todos os dados em trânsito e em repouso na Azure são criptografados para proteger contra acesso não autorizado.

b) Firewalls e Controle de Acesso: oferece firewalls e sistemas de controle de acesso para proteger seus recursos contra ameaças externas, possibilitando configurar regras de firewall e políticas de acesso com base nas necessidades do seu aplicativo.

c) Recuperação de Desastres: oferece serviços de recuperação de desastres, como a replicação de máquinas virtuais e backups automatizados, para garantir a continuidade dos negócios em caso de falhas.

d) Monitoramento e Detecção de Ameaças: oferece ferramentas de detecção de ameaças para identificar e responder a atividades suspeitas em seus recursos.

e) Conformidade Regulatória: atende a várias regulamentações globais e padrões de segurança, tornando-a adequada para setores altamente regulamentados, como saúde e finanças.

f) SLAs de Alta Disponibilidade: oferece acordos de nível de serviço (SLAs) que garantem alta disponibilidade para serviços essenciais. Isso inclui a garantia de tempo de atividade para serviços críticos.

g) Autenticação Multifatorial (MFA): Reforce a segurança dos seus recursos com autenticação multifatorial, que requer múltiplos métodos de autenticação para acessar suas contas e recursos.

Noutro giro, entendendo que os pormenores devam ser respondidos pela empresa contratada, damos como esclarecido o ponto questionado na visão técnica do Confea na sua posição de contratante.

8) Qual o ambiente do servidor que irá armazenar e processar os votos?

O voto é encriptado no navegador do eleitor, portanto já está protegido durante o tráfego na rede e ao chegar aos servidores da aplicação. O voto é então armazenado, de forma a manter sua anonimidade, no banco de dados da aplicação. Ao final da eleição, todos os votos estão embaralhados no banco e ocorre a decriptação dos votos para contagem e apuração do resultado final mediante fornecimento da chave privada, que fica detida pela Comissão Eleitoral.

9) Qual a segurança aplicada no ambiente de infraestrutura?

Todos os servidores estiveram protegidos por Firewalls de Aplicação (WAFs). Os WAFs são uma categoria de dispositivos de segurança de rede ou serviços de segurança em nuvem projetados para proteger aplicativos web contra ameaças e ataques cibernéticos direcionados a vulnerabilidades específicas de aplicativos. Eles funcionam como uma camada de segurança entre um aplicativo web e o tráfego da Internet, filtrando, monitorando e bloqueando atividades maliciosas ou suspeitas. Aqui estão algumas características e funcionalidades comuns de firewalls de aplicação:

• Filtragem de Tráfego HTTP/HTTPS: Os WAFs inspecionam o tráfego HTTP e HTTPS, analisando cada solicitação e resposta para identificar atividades maliciosas.

• Proteção contra Injeção de SQL: Eles podem detectar e bloquear tentativas de injeção de SQL, um tipo comum de ataque usado para explorar vulnerabilidades em aplicativos web.

• Prevenção de Cross-Site Scripting (XSS): Os WAFs ajudam a prevenir ataques XSS, que envolvem a inserção de scripts maliciosos nas páginas da web para roubar informações ou redirecionar os usuários para sites maliciosos.

• Deteção de Ataques de Força Bruta: WAFs monitoram tentativas de login de força bruta e podem bloquear endereços IP suspeitos ou implementar medidas de autenticação adicional.

• Proteção contra Botnets e Scrapers: Eles podem identificar e bloquear bots maliciosos, como botnets usados para ataques de negação de serviço (DDoS), e web scrapers que coletam dados do site de forma não autorizada.

• Logging e Alertas: Geralmente fornecem logs detalhados de atividades e alertas em tempo real para que os administradores de segurança possam monitorar e responder a incidentes. • Customização de Regras: WAFs permitem que os administradores personalizem regras de segurança para atender às necessidades específicas do aplicativo.

10) Existe um ambiente de contingência em tempo real?

Todos os recursos utilizados possuem redundância tripla. A redundância tripla é uma estratégia de redundância aplicada a infraestruturas de hospedagem de sites para garantir alta disponibilidade e resiliência. Essa abordagem envolve a criação de três instâncias independentes do ambiente de hospedagem, cada uma capaz de manter o site em funcionamento, mesmo em caso de falha em uma das instâncias.

11) Em caso de algum desastre (ataques, falhas no sistema, sobrecarga, etc.) no ambiente, quais serão as medidas adotadas?

O sistema do votação utilizado nas Eleições Gerais do Sistema Confea/Crea e Mútua possui diversas camadas de segurança, em observância aos critérios estabelecidos no Processo licitatório realizado pelo Confea. Além disso, o sistema passou por testes frequentes de carga e funcionalidade, além de processos de revisão de código e infraestrutura.

12) Requer-se sejam apresentados os contratos referentes às empresas de desenvolvimento, teste e auditoria do sistema de votação pela internet que será utilizado nas eleições de 2023, nos termos do artigo 93 e parágrafo único, da Resolução CONFEA nº 1.114/2019, bem como, os respectivos editais de licitação referentes a tais contratações.

Os materiais solicitados estão disponíveis em processos públicos, e portanto, acessíveis a qualquer tempo pelos interessados.

Informamos que a Assessoria da CEF disponibilizou a aba "Contratações para viabilização das Eleições" na área da Comissão Eleitoral Federal, no site do Confea, acessível pelo seguinte link: https://www.confea.org.br/funcionamento/eleicoes/2023, e que os documentos solicitados seguirão anexados a este despacho.

13)Considerando os ataques cibernéticos ao CREA/SP, ocorridos em dezembro de 2022, em que é sabido que houve o vazamento de dados de inscritos (v.g. CPF, RG, órgão expedidor do RG, data de emissão, Título de Eleitor, filiação, endereços físicos, números de telefones e e-mails), sobretudo diante do fato de o CREA/SP não ter agido em conformidade com a Lei Geral de Proteção de

Dados Pessoais (Lei nº 13.709/2018) e não estar agindo em conformidade com a Lei de Acesso à Informação e Transparência (Lei nº 12.527/2011), questiona-se:

13.1 O CONFEA e esta i. Comissão Eleitoral Federal e as empresas de desenvolvimento, teste e auditoria referidas no item 12, estão cientes em sua inteireza dos ataques cibernéticos e do vazamento de dados do sistema CREA/SP? Estão acompanhando o deslinde do caso? Estão considerando os dados vazados no desenvolvimento do sistema de segurança e monitoramento de possíveis invasões e tentativas de corrompimento?

Após a situação relatada, o Confea instaurou através da Portaria 539/2022 o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais - CGSI no Sistema Confea/Crea, tendo como finalidade o que segue:

> Art. 1º Instituir o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais - CGSI no âmbito do Sistema Confea/Crea.
>
> Parágrafo único. O CGSI tem como finalidade:
>
> I - promover a cultura da segurança da informação e proteção de dados pessoais;
>
> II - discutir diretrizes gerais e específicas quanto à segurança e inviolabilidade do banco de dados do Sistema Confea/Crea;
>
> III - propor novas tecnologias, medidas e ações com vistas à segurança digital;
>
> IV - promover, coordenar e acompanhar as ações relacionadas à segurança da informação e proteção de dados pessoais;
>
> V - propor diretrizes, normas gerais e procedimentos para a efetiva implementação da segurança da informação e proteção de dados pessoais;
>
> VI - instituir grupos de trabalho específicos para tratar de temas e propor soluções específicas sobre segurança da informação e proteção de dados pessoais;
>
> VII - propor diretrizes e normas gerais para a continuidade dos serviços essenciais de TIC;
>
> VIII - criar e manter o Sistema de Gestão da Segurança da Informação;
>
> IX - garantir conformidade entre os sistemas e procedimentos adotados no Sistema Confea/Crea e a legislação que rege os temas segurança da informação, transparência, acesso à informação e proteção de dados pessoais.
>
> X - propor da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação, em conformidade com a legislação existente sobre o tema, bem como de suas alterações; e
>
> XI - propor sobre as normas internas relativas à segurança da informação;
>
> XII - manifestar-se sobre ações em segurança da informação e proteção de dados pessoais;

Desta forma, todos os assuntos relacionados à ocorrência supracitada bem como demais assuntos correlatos tem sido tema de várias reuniões e ajustes contratuais e procedimentais visando sanar todas os incidentes e problemas relacionados à segurança da informação, sejam eles de caráter técnico (infraestrutura, sistemas, etc.), de proteção de dados ou de permissionamento, pelo referido Comitê.

Como pontos principais de efetividade do Comitê após sua instauração, podemos elencar a realização de análises junto às empresas contratadas de vários entes do Sistema Confea/Crea e Mútua, como por exemplo a prestadora de serviços tipo NOC/SOC (Network/Security Operation Center), contratada pelo Confea, que trata de, entre outros, acompanhamento, controle e registro de monitoramento dos logs dos firewalls e eventos de segurança, respostas aos incidentes, análise de vulnerabilidades com ferramentas utilizadas (Tenable, Picus, Backbox) e monitoramento de comportamentos suspeitos, bem como a empresa contratada pelo Crea-SP com mesma atuação nos serviços de tecnologia da informação, além de outras soluções contratadas para a gestão e controle destas áreas de TI.

Também foram realizados testes de penetração (Pentest) em estruturas de TI de Regionais e empresas contratadas, visando buscar a existência de vulnerabilidades em suas infraestruturas, sendo

os resultados trabalhados para a obtenção de melhorias contínuas nas infraestruturas avaliadas.

Por fim, e diante do relatado, informamos que tanto o Confea quanto os Regionais estão trabalhando para a evolução da segurança de tecnologia da informação adotando as melhores práticas de gerenciamento e controle dos seus ativos e soluções, bem como considerando todos os possíveis impactos relacionados à segurança tanto no dia a dia da rotina dos órgãos quanto, e de forma especial, nos processos específicos como o processo eleitoral.

É necessário reiterar que o vazamento de dados ocorrido no Crea-SP em nada afetou a realização das Eleições Gerais do Sistema Confea/Crea e Mútua 2023, uma vez que o sistema de votação eletrônico estava parametrizado de forma robusta para prevenir eventuais ataques, e sobretudo pelo fato de que o mero conhecimento de dados pessoais não seria suficiente para alguém mal intencionado acessar o ambiente de votação, e proferir votos por outra pessoa, em razão do procedimento adotado para autenticação na ferramenta de votação.

13.2 O CONFEA e essa i. Comissão Eleitoral Federal, têm informações claras e detalhadas sobre a segurança cibernética e física promovida pelo CREA/SP e por terceiros aos quais os dados são compartilhados pela Autarquia, que demonstram a integridade dos dados pessoais, apontam quais medidas técnicas e administrativas eram adotadas à época dos ataques cibernéticos ao sistema CREA/SP, no ano de 2022, e quais são adotadas atualmente, demonstrando quais melhorias de cibersegurança foram implantadas no sistema e se tais medidas podem ser reputadas aptas à proteção eficaz dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração comunicação ou difusão, com a devida justificação técnica embasa nas matrizes de segurança de informação?

Da mesma forma que a resposta anterior, o Comitê vem adotando as práticas de avaliação, controle e evolução da infraestrutura de TI, buscando uma evolução das soluções utilizadas por todos os Regionais e Confea, bem como buscando uma possível unificação dos serviços de segurança a nível nacional.

Desta forma, como já relatado, tanto o Confea quanto os Regionais estão trabalhando para a evolução da segurança de tecnologia da informação adotando as melhores práticas de gerenciamento e controle dos seus ativos e soluções.

13.3 Quais meios e métodos de segurança física e digital estão sendo adotados para garantir a fidedignidade do processo eleitoral, considerando, especialmente, o vazamento de dados do CREA/SP; e

O datacenter onde está hospedado sistema, na Microsoft Azure, possui as certificações:

• SOC 1 - se refere a um relatório de auditoria emitido pela Microsoft Azure que avalia o controle interno sobre a segurança e a integridade dos serviços e sistemas relacionados à infraestrutura em nuvem do Azure. SOC 1 (Service Organization Control 1) é uma norma de auditoria reconhecida internacionalmente que se concentra em controles financeiros e de relatórios

• SOC 2 - se concentra nos controles de segurança, disponibilidade, processamento de dados e privacidade em uma organização de serviços, especificamente relacionada aos serviços em nuvem oferecidos pelo Microsoft Azure. SOC 2 (Service Organization Control 2) é uma norma de auditoria que avalia a segurança e a integridade dos controles de uma organização de serviços em relação à proteção de dados e à conformidade com padrões específicos.

• SOC 3 - fornece uma visão resumida e simplificada dos controles de segurança e conformidade da plataforma Microsoft Azure em relação aos princípios do SOC 2. SOC 3 (Service Organization Control 3) é uma norma de auditoria semelhante ao SOC 2, mas o relatório SOC 3 é projetado para ser mais acessível ao público em geral. CIS benchmark -

são conjuntos de melhores práticas e diretrizes de configuração de segurança para vários produtos e plataformas de tecnologia.

• CSA STAR - A CSA STAR, ou Certificação de Segurança, Confiança e Risco (Security, Trust, and Assurance Registry) da Cloud Security Alliance (CSA), é um programa de certificação que ajuda as organizações a avaliar a segurança de provedores de serviços em nuvem, como a Microsoft Azure. O CSA STAR fornece um registro de provedores de serviços em nuvem que atendem a padrões de segurança e privacidade reconhecidos.

• ISO 20000-1 - Essa norma tem como objetivo ajudar as organizações a estabelecer e manter um sistema eficaz de gerenciamento de serviços de TI, garantindo a entrega de serviços de alta qualidade aos clientes. A Microsoft Azure, como um provedor de serviços em nuvem, está em conformidade com várias normas e padrões de segurança e gerenciamento de serviços de TI, incluindo a ISO 20000-1.

• ISO 22301 - Essa norma visa ajudar as organizações a desenvolver e implementar um sistema eficaz de gerenciamento de continuidade de negócios, garantindo que estejam preparadas para enfrentar e se recuperar de incidentes e interrupções que possam afetar suas operações. A Microsoft Azure, como um provedor de serviços em nuvem, está em conformidade com várias normas e padrões de segurança e gerenciamento de continuidade de negócios, incluindo a ISO 22301.

• ISO 27001 - A ISO 27001 abrange diversas áreas, incluindo políticas de segurança da informação, gestão de riscos, controles de segurança e conformidade, e tem o objetivo de garantir a proteção das informações sensíveis de uma organização. A Microsoft Azure, como um dos principais provedores de serviços em nuvem, busca conformidade com a ISO 27001 para demonstrar seu compromisso com a segurança da informação e a proteção dos dados.

• ISO 27017 - A ISO/IEC 27017 é uma norma internacional que fornece diretrizes específicas para o uso seguro de serviços de computação em nuvem, abordando preocupações de segurança da informação relacionadas à computação em nuvem. Essa norma complementa a ISO/IEC 27001, que é um padrão mais amplo para sistemas de gestão de segurança da informação, fornecendo orientações específicas para provedores de serviços em nuvem e clientes que utilizam serviços em nuvem.

• ISO 27018 - A ISO/IEC 27018 é uma norma internacional que estabelece diretrizes específicas para a proteção da privacidade de dados pessoais em ambientes de computação em nuvem. Essa norma complementa a ISO/IEC 27001, que é um padrão mais amplo para sistemas de gestão de segurança da informação, fornecendo orientações detalhadas sobre como os provedores de serviços em nuvem devem proteger informações pessoais de seus clientes.

• ISO 27701 - A ISO/IEC 27701 é uma norma internacional que estabelece diretrizes para a proteção da privacidade de informações pessoais por meio do gerenciamento de informações pessoais (PIMS) em ambientes de tecnologia da informação. Essa norma é uma extensão da ISO/IEC 27001 (Sistema de Gerenciamento de Segurança da Informação) e da ISO/IEC 27002 (Código de Prática para Controles de Segurança da Informação), e é voltada especificamente para a privacidade de dados pessoais. A Microsoft Azure, como um importante provedor de serviços em nuvem que processa e armazena uma grande quantidade de dados, incluindo informações pessoais, busca conformidade com a ISO/IEC 27701.

• ISO 9001 - A ISO 9001 é uma norma internacional que estabelece os requisitos para um Sistema de Gestão da Qualidade (SGQ) em uma organização. Ela é focada na melhoria contínua da qualidade dos produtos e serviços fornecidos pela organização e abrange diversos aspectos relacionados à gestão da qualidade, processos, documentação, monitoramento e medição, entre outros. A Microsoft Azure, como uma divisão da Microsoft que oferece serviços em nuvem, busca conformidade com a ISO

9001 para garantir que seus processos e práticas de gestão da qualidade estejam em conformidade com os requisitos estabelecidos por essa norma. A conformidade com a ISO 9001 implica que a Microsoft Azure segue padrões e práticas reconhecidos internacionalmente para garantir a qualidade de seus produtos e serviços.

• WCAG - A Microsoft Azure, como parte da Microsoft, está comprometida com a acessibilidade e a conformidade com as diretrizes de acessibilidade da Web (Web Content Accessibility Guidelines - WCAG) para seus produtos e serviços. As WCAG são diretrizes internacionais estabelecidas pelo World Wide Web Consortium (W3C) para garantir que os conteúdos da web sejam acessíveis a pessoas com deficiência. A conformidade com as WCAG é essencial para garantir que os serviços em nuvem, como os oferecidos pela Microsoft Azure, sejam acessíveis a todos os usuários, independentemente de suas habilidades ou necessidades específicas.

13.4 Tais métodos e meios estão de acordo com os protocolos, padrões, diretrizes e práticas internacionais recomendadas no gerenciamento de riscos de segurança cibernética? Descreva-os pormenorizadamente.

Da mesma forma que os itens anteriores, fica claro na leitura dos processos que trataram sobre as contratações realizadas , que os protocolos e práticas adotados estiveram de acordo com as práticas mais atuais e recomendadas, visando garantir todo o controle e gerenciamento dos riscos envolvidos no pleito eleitoral.

Atenciosamente,

Daltro de Deus Pereira

Coordenador da Comissão Eleitoral Federal 2023

Documento assinado eletronicamente por **Daltro de Deus Pereira**, **Conselheiro(a) Federal**, em 20/12/2023, às 18:35, conforme horário oficial de Brasília, com fundamento no art. 4º, § 3º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.confea.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0883202** e o código CRC **2D244F9B**.

Referência: Processo nº 00.004888/2023-54 SEI nº 0883202