Justiça Eleitoral

GT-SI - GRUPO DE TRABALHO DE SEGURANÇA DA INFORMAÇÃO

Arquitetura de Cibersegurança

Versão 1.0 - setembro de 2021

Brasília, 2021

Sumário

Introdução 05

Metodologia 05

Ferramentas 06

Linha do Tempo da Arquitetura 07

Eixos de atuação 08

Sugestão para Contratação de Ferramentas 12

Priorização das Contratações - 2021 12

Marcos a serem acompanhados por cada Tribunal 13

Considerações Finais 14

Anexo I - Ferramentas 16

Anexo II - Matriz 5W2H 17

Anexo III - Considerações dos servidores do TSE e TREs 18

EQUIPE DE ELABORAÇÃO DO DOCUMENTO

Membros do GT-SI dedicados exclusivamente ao trabalho:

- Luiz Gustavo Marques Florindo - TRE/MG
- Juarez de Oliveira - TRE/PR
- Marcelo Silva de Novaes - TRE/MS

Membros do GT-SI que apoiaram na elaboração:

- Dra. Simone Trento - Juíza Auxiliar da Presidência TSE – Coordenadora
- Carlos Eduardo Miranda Zottmann - TSE
- Kemeo Ramalho de Melo - TSE
- Hanniery Freire - TRE/PB
- Ricardo Macedo Baudel - TRE/PE
- Marcelo Carneiro Rodrigues - TSE (*)
- Sidney Santos Doria - TRE/BA (*)
- Jean Carlos Alves dos Anjos - TRE/RO (*)
- Luís César Darienzo Alves - TRE/MT (*)
- Rommel Baia Silva - TRE/ES (*)

(*) Autorizados pelos Tribunais. Aguardando formalização de Portaria TSE.

Consultores Técnicos

- Edcley da Silva Firmino - TRE/AC
- Emanoel Flexa - TRE/AP
- Jonas de Araújo Luz Junior - TRE/CE
- Ricardo Negrão de Oliveira - TRE/DF
- André Alves Alencar - TRE/MG
- Euder Monteiro - TRE/MG
- Luciano Chapuis de Oliveira - TRE/MG
- Valéria Aparecida Antunes Freitas - TRE/MG
- Marcos de Almeida Alves - TRE/MG
- Mozart Fernandes Moreira Lima - TRE/MG
- Divaldo Lima Chaves - TRE/MG
- Ulysses Almeida - TRE/MS
- Daniel Nelo Soares - TRE/PA
- Felipe Cavalcanti Alves - TRE/PB
- Pedro de Figueirêdo Lima Neto - TRE/PB
- Romero de Azevedo Góes - TRE/PE
- Carlos Alberto Ribeiro do Nascimento Júnior - TRE/PI
- Carlos Eduardo Gomes Pinheiro - TRE/RJ
- Denilson Bastos da Silva - TRE/RN
- Francisco de Assis Paiva Leal - TRE/RN
- Helder Jean Brito da Silva - TRE/RN
- Alexandre Márcio Cavalcanti Machado - TRE/RN
- Andson de Lima Gomes - TRE/RR
- Márcio Barbosa de Carvalho - TRE/RS
- Ivo Antonio Guimarães Neto - TRE/RS
- André Amâncio de Jesus - TRE/SE
- Cosme Rodrigues de Souza - TRE/SE
- Selmo Pereira de Almeida - TRE/SE
- Paulo Sérgio Furtado Abreu - TRE/SP
- Renata Vidon de Carvalho - TRE/SP
- Fábio Prado - TRE/SP
- Cleórbete Santos - TRE/TO
- Ivanildo Ferreira Gomes - TSE
- Cristiano Moreira Andrade - TSE
- Célio Castro Wermelinger - TSE

Diagramação/Arte:

André Chiochetta Licks - TRE/MS

Introdução

Este documento integra a Estratégia Nacional de Cibersegurança e foi organizado pelo Grupo de Trabalho de Segurança da Informação da Justiça Eleitoral GT-SI, com o apoio de diversos servidores do TSE e dos Tribunais Regionais Eleitorais, cujas contribuições estão listadas no anexo III.

Dentre as considerações dos Regionais, destaca-se um ponto comum: todos reconhecem a necessidade de se investir em ações de cibersegurança, mas ponderam não haver quantidade ou qualidade necessários de pessoal de TI para as ações proporcionais às ameaças postas.

Para o desenvolvimento desse documento, optou-se por uma abordagem de alto nível, visual e objetiva, considerada mais adequada para o momento.

Importante frisar que uma arquitetura de cibersegurança é um cenário vivo e dinâmico, que prevê vários pontos de checagem de modo a surtir o efeito desejado.

Neste documento não foi abordada de forma intensiva a alocação dos recursos humanos necessários para os projetos, tendo em vista que o tema foi tratado diretamente no documento **"Proposta de Estrutura Organizacional para Segurança da Informação e Cibersegurança no Âmbito da Justiça Eleitoral"**, também criado pelo GT-SI. É importante ponderar que a estrutura adequada de pessoal é fator crítico de sucesso para implantação da estratégia.

Metodologia

Foram utilizados como fonte de referência para elaborar a arquitetura de cibersegurança os frameworks NIST v.1.1, ISO 27002:2013, ISO 27005:2019, ISO 22301:2013 e CIS Controls v.7.1. Após o levantamento das ferramentas de segurança que podem atender à arquitetura, foram realizadas consultas a diversos servidores dos tribunais eleitorais, visando entender melhor os contextos regionais.

Optou-se por uma descrição mais sucinta e objetiva, com foco na priorização de contratações e implementação de processos que surtam o maior efeito possível na cibersegurança das eleições de 2022, mas mantendo a perspectiva de projetos de longo prazo.

Ferramentas

Foi elaborado um rol de soluções tecnológicas para atender à Estratégia de Cibersegurança da JE, com priorização em três níveis de criticidade. O primeiro nível convém que esteja operacional até março de 2022, com alguns projetos sendo realizados ainda em 2021. O segundo nível convém que esteja operacional até agosto de 2022 e o terceiro nível que seja contratado até o final de 2023. A priorização levou em conta os riscos e impactos derivados de ataques cibernéticos diretos à Justiça Eleitoral e quais soluções podem atuar mais rapidamente para mitigar estes ataques. O escopo do trabalho, inicialmente, não aborda um protocolo de tratamento para casos de desinformação.

A lista detalhada de ferramentas está no anexo I.

Foi elaborada uma planilha de controle, no modelo 5W2H, anexo II, para apoiar o acompanhamento dos projetos derivados. Convém que o acompanhamento seja feito pelo TSE e por cada um dos Tribunais Regionais, envolvendo todas as áreas que forem necessárias, não apenas as áreas de tecnologia da informação.

Aos Tribunais que já possuem as soluções propostas no nível 1 ou 2, convém que avancem para os próximos níveis de priorização, de acordo com suas capacidades operacionais.

Cada ferramenta listada possui requisitos funcionais fundamentais e indicações de marcas e fabricantes em caráter exemplificativo, sendo necessário que os grupos responsáveis pelas contratações, façam análise pormenorizada, preferencialmente de forma colaborativa. Convém que esta análise se estenda à capacidade de operação das soluções.

Conforme as soluções forem sendo implantadas, é imprescindível que os processos de trabalho sejam documentados, bem como padrões e boas práticas de operação, suporte e manutenção sejam criados. Estes documentos devem ficar disponíveis com acesso restrito às equipes técnicas e de gestão afetas.

Elencou-se uma lista de soluções tecnológicas extensa, no entanto, pode não ser aplicável em 100% dos cenários, cabendo a cada regional efetuar sua própria análise antes de qualquer contratação. Muitas soluções de cibersegurança de mercado podem não ter sido incluídas, seja pela oportunidade ou pelo custo e complexidade de implantação. A inclusão ou exclusão de soluções e processos pode ocorrer nas etapas do ciclo PDCA propostas, devendo ser adequadamente fundamentadas e documentadas.

Linha do Tempo da Arquitetura

Convém que a arquitetura seja avaliada periodicamente. Sendo assim, sugere-se um ciclo PDCA, com ao menos duas revisões anuais:

Eixos de atuação

Foram elencados 8 eixos de atuação para agrupar as iniciativas:

1 - Governança e Conformidade

Este tópico aborda uma gestão mais adequada de GRC (governança, risco e conformidade), ponto primordial na implementação de qualquer controle ou ferramenta. Além dos riscos de segurança da informação, convém que seja feito um mapeamento dos dados pessoais e dos riscos relativos à sua proteção. A forma mais eficiente é com a contratação de uma solução de GRC que atenda aos dois temas.

2 - Conscientização e Capacitação

Este tópico aborda a implementação de um programa de conscientização (awareness) em segurança da informação adequado ao porte da Justiça Eleitoral e à quantidade de pessoas que utilizam, suportam e mantêm as soluções tecnológicas. Propõem-se a aquisição de soluções de software ou serviços específicos, com vistas a testar rotineiramente o modo como os colaboradores reagem em casos de golpes de engenharia social, como phishing,

smishing e outros. Eles devem conhecer o básico sobre os conceitos de cibersegurança. Os programas de conscientização e capacitação inicialmente podem ocorrer por meio de ferramentas digitais, através de técnicas de gamificação, por exemplo.

3 - Sistema Eletrônico de Votação

A Segurança do Sistema Eletrônico de Votação, bem como a sua confiabilidade, estão, em sentido amplo, no escopo da atuação do GT, devendo o referido processo estar integrado aos demais.

Ataques cibernéticos à Justiça Eleitoral têm como alvo principal o sistema eletrônico de votação, ou seja, como a "joia da coroa". Os dias/semanas que antecedem as Eleições, bem como o dia da realização do pleito são períodos críticos. Nestes dias podem surgir importantes ameaças indiretas e diretas ao sistema de votação (como ataques aos sistemas de apoio ou aos sistemas de atendimento aos eleitores, conectados à internet).

São improváveis ataques diretos às urnas eletrônicas, haja vista elas não possuírem conexão externa. No entanto, convém manter uma robusta segurança também sobre os aspectos relativos a código fonte e artefatos utilizados no processo de construção e desenvolvimento dos softwares e hardwares utilizados no processo eleitoral.

Sugere-se, portanto, a criação de um subgrupo para providenciar uma análise crítica do ambiente computacional da Justiça Eleitoral que terá também a missão de elaborar medidas específicas, como a formação antecipada da Sala de Gestão de Crises (War Room), a elaboração do Plano de Recuperação de Desastres (PRD), bem como outras ações necessárias à disponibilidade e à integridade do processo eleitoral.

Na Sala de Gestão de Crises, os envolvidos devem poder acessar informações em tempo real relativas ao andamento de todos os procedimentos de custódia, dos sistemas específicos para o funcionamento das urnas eletrônicas e outros relacionados ao processo eleitoral. Além de uma infraestrutura apartada da infraestrutura utilizada pelo Tribunal.

Por fim, também é imperativo que o responsável pela Gestão da Crise tenha autonomia e acesso direto ao Alto Comando da Justiça Eleitoral (Corte do Tribunal Superior Eleitoral e dos Tribunais Regionais), para que eventuais procedimentos urgentes ou emergenciais sejam prontamente decididos, determinados e executados.

4 - Segurança de Aplicações

A proteção das aplicações eleitorais, sazonais ou utilizadas no dia a dia, expostas ou não na internet, requer soluções de proteção adequadas e multicamadas. Firewalls, proteções aos bancos de dados, autenticação de múltiplos fatores e monitoramento pelo SOC (Security

Operation Center), são necessários para a manutenção da reputação de segurança do sistema eletrônico de votação. Sugere-se a utilização de ferramentas adequadas à diminuição desses riscos, até haver uma estratégia definida de como serão tratados os sistemas legados.

5 - Operações e Infraestrutura

Este tópico é um dos pontos fundamentais em um projeto de arquitetura de cibersegurança. Ele concentra a maior quantidade de aquisições e processos de trabalho, bem como está entrelaçado com outros eixos e à necessidade de investimentos em pessoas, processos e tecnologias. Um centro de operações de segurança (SOC) é uma das iniciativas que propiciará o acompanhamento no dia a dia da saúde do ambiente computacional, bem como o monitoramento de anomalias e ataques cibernéticos ao ambiente computacional da Justiça Eleitoral.

6 - Gestão de Ativos

A gestão dos ativos é um ponto base, pois todo ativo, antes de ser protegido, precisa estar catalogado, ter nominalmente seu "dono" (product owner) definido e seu nível de criticidade levantado. Convém que esta gestão seja automatizada e gerenciada observando o nível de criticidade do ativo. A gestão de ativos deve incluir a classificação dos ativos que contenham dados pessoais e dados pessoais sensíveis. Por isso, convém que o encarregado de dados (DPO) seja envolvido no processo.

7 - Gestão de Identidade e Acessos

É o novo perímetro a ser protegido. Compõe-se fundamentalmente de medidas de proteção aos colaboradores que utilizam os sistemas informatizados desta Justiça Especializada e é a principal vulnerabilidade explorada por criminosos digitais.

Carece de fatores adicionais para identificação, autenticação e controle do acesso de usuários e pode ser utilizado como forma de comprometer os ambientes computacionais desta Justiça Especializada. É a maior vulnerabilidade computacional no contexto da Justiça Eleitoral e representa um ponto nevrálgico que deve ser abordado com bastante precisão.

Os usuários do ambiente computacional devem estar devidamente identificados, tendo suas permissões de acessos monitoradas e revisadas rotineiramente, além de serem autenticados de maneira mais segura, preferencialmente com múltiplos fatores de autenticação.

A atual estrutura de servidores de diretórios AD (Active Directory), carece de revisão

urgente, pois possui muitas bases de usuários, dificultando enormemente os controles. Constitui-se, ainda, em alto risco às operações de segurança da informação da Justiça Eleitoral a existência de máquinas na rede que utilizam apenas autenticação local (standalone), principalmente nas zonas eleitorais, justamente o core business desta Justiça Especializada.

Para mitigar esses riscos e resolver este problema, convém que os controladores de domínio sejam unificados, eliminando-se a autenticação local e atualizando-se a versão do sistema operacional Windows Server mais atualizada disponível no mercado, bem como a implantação de duplo fator de autenticação.

A aplicação de políticas e a adequada gestão dos usuários dependem diretamente dessa reestruturação dos controladores de domínios, bem como da unificação das bases de identificação e autenticação de colaboradores.

Sugere-se, inicialmente, a contratação de consultoria da própria Microsoft para remodelar o serviço de diretórios de toda a Justiça Eleitoral, com um domínio único criado a partir do zero e empregando-se as boas práticas de segurança.

Tal proposta foi feita por um subgrupo de servidores de vários regionais, os quais analisaram a situação atual e os melhores caminhos a seguir. Tal proposta conta com o consenso técnico do GT-SI e deve ser viabilizada de modo a aprimorar a segurança dos ambientes computacionais desta Justiça Especializada.

Convém ainda que sejam realizadas contratações de licenças de Windows Servers, CALs de acesso, suporte Premier da Microsoft e licenças para Desktops, de modo a manter toda a base computacional da Justiça Eleitoral atualizada e segura.

8 - Controles Criptográficos

Este tópico aborda a gestão de todos os controles criptográficos, desde certificados digitais do tipo e-CPF A3 (certificados utilizados por usuários), certificados para servidores web, certificados usados na criptografia de bases de dados e em sistemas.

Sugere-se a implementação de uma Autoridade Certificadora Nacional, utilizando infraestrutura dedicada com HSM (Hardware Security Module) ou TPM (Trusted Platform Module) distribuída em vários datacenters e equipamentos. Estas tecnologias permitirão o gerenciamento eficiente e seguro dos certificados digitais para todos os regionais e TSE.

Convém que seja criado um subgrupo para tratar desse tema, avaliar o tipo de solução a ser adquirida e a interoperabilidade com a infraestrutura existente.

Sugestão para Contratação das Ferramentas

Convém que seja realizado um levantamento junto aos Tribunais Eleitorais (TSE e TREs) para verificar quais soluções cada um já possui e quais estão sendo adquiridas e em qual fase do processo de contratação (contratações em andamento).

Com o levantamento realizado, será possível identificar a possibilidade de agrupamento de Tribunais para compras conjuntas. O GT-SI sugere que as contratações ocorram por registro de preços.

Como informado anteriormente, sugere-se que a planilha 5W2H seja preenchida e acompanhada no dia a dia por um grupo multidisciplinar designado formalmente pela Alta Gestão de cada Tribunal Eleitoral (TSE e TREs), haja vista que deverão constar formalmente os nomes dos responsáveis, datas e custos para entrega das soluções. Cada Tribunal deverá preencher a planilha, mesmo que venha a ser partícipe da contratação de outro Tribunal, pois cada tribunal deve acompanhar suas entregas.

Priorização das Contratações - 2021

Sugerimos fortemente que parte das soluções de criticidade 1, listadas abaixo, sejam adquiridas ainda em 2021.

- **Solução de proteção de endpoints (antivírus/EDR)** – Esta solução protege os endpoints (desktops, notebooks, servidores) da ação de malwares. Essa aquisição já está em andamento no TSE para contratação centralizada, abrangendo TSE e TREs, mas convém que os requisitos técnicos sejam revistos para atingir o maior nível de proteção possível. Junto com a atualização de sistemas operacionais, esta solução diminui sensivelmente o risco de ataques aos usuários, principalmente relacionados a ransomware.
- **Solução de backup** - Ferramentas capazes de fazer cópias de segurança de todos os ativos, além de criptografar e deduplicar os dados armazenados. Trata-se de ponto crítico para a recuperação de incidentes, necessitando que todos os tribunais possuam uma solução robusta e com o suporte técnico adequado. Convém ainda que todos os tribunais possuam política de cópias de segurança atualizada e sejam realizados testes de restauração periódicos, para garantir a integridade destas cópias.
- **Solução de SIEM –** Ferramentas utilizadas na centralização, correlação e análise de logs, com capacidade de suportar os diversos tipos de ativos de informação. Convém que esta solução seja profissional e com suporte técnico adequado. Esta é uma das principais ferramentas utilizadas no tratamento de incidentes pelas ETIRs e pelo SOC.
- **Antispam (TSE) –** Ferramenta de filtro de e-mails, cuja aquisição já está em andamento pelas equipes do TSE e atenderá todos os Tribunais que utilizam solução de e-mail on-premises. Os ataques de phishing são um dos maiores vetores de ataques em redes corporativas, por isso o aumento da segurança do serviço de e-mail é imprescindível.

- **WAF (TSE) –** Solução que analisa e protege o tráfego de entrada das aplicações web. Já foi contratada pelo TSE e está em operação parcial. Convém agilizar a configuração de todas as aplicações web publicadas na Internet pelos regionais e pelo TSE para que possam passar pela solução. Existe um grau de dificuldade técnica no monitoramento e na adequação das aplicações para utilizar esta solução, por isso sugere-se que seja priorizado junto às equipes técnicas. As aplicações web são a parte mais exposta da infraestrutura.

Sugere-se que as soluções de criticidade 1 e 2, sejam adquiridas e estejam minimamente operacionais até as eleições, em 2022, assim como os processos de DRP (Plano de recuperação de desastres) e War Room (sala de crise) estejam implementados e testados.

Convém verificar se as equipes de contratação do TSE que estão tratando dos projetos acima (antispam, proteção de endpoints e WAF), carecem de algum apoio técnico. Os servidores do GT-SI, dos regionais e terceirizados podem ser acionados para contribuir.

No caso da ferramenta de SIEM, o GT-SI sugere que, dado o custo, complexidade, dificuldade de implantação e intrusividade da ferramenta, a aquisição seja pelo prazo mínimo de 60 meses, de modo a diluir o alto investimento, bem como haja um grupo técnico capacitado e dedicado a sua operação em todos os Tribunais Eleitorais.

O GT-SI entende que deve ser criado um subgrupo específico para tratar das soluções eventualmente necessárias à operação do Centro de Operações de Segurança (SOC). Preliminarmente, é consenso do GT-SI que a utilização de software livre aumentará a curva de aprendizagem de uso da ferramenta, bem como o esforço de operação, o que poderá ocasionar em eficácia bem aquém da desejada, principalmente considerando o pleito eleitoral de 2022 que se avizinha.

Marcos a serem acompanhados por cada Tribunal

A complexidade e o custo das aquisições que envolvem a estratégia de cyber, de modo a garantir seu sucesso devem passar por controle gerencial/administrativo, os quais, sugere-se, devem controlar algumas datas macro:

- Data limite de formação do grupo;
- Data de início da prospecção técnica;
- Data de início do documento de oficialização da demanda;
- Data de início dos estudos técnicos preliminares;
- Data de consolidação dos estudos técnicos preliminares;
- Data de consolidação do termo de referência;
- Data de publicação do edital;
- Data de assinatura do contrato;
- Data de início da implantação;
- Pagamento do fornecedor;
- Data de início de operação;

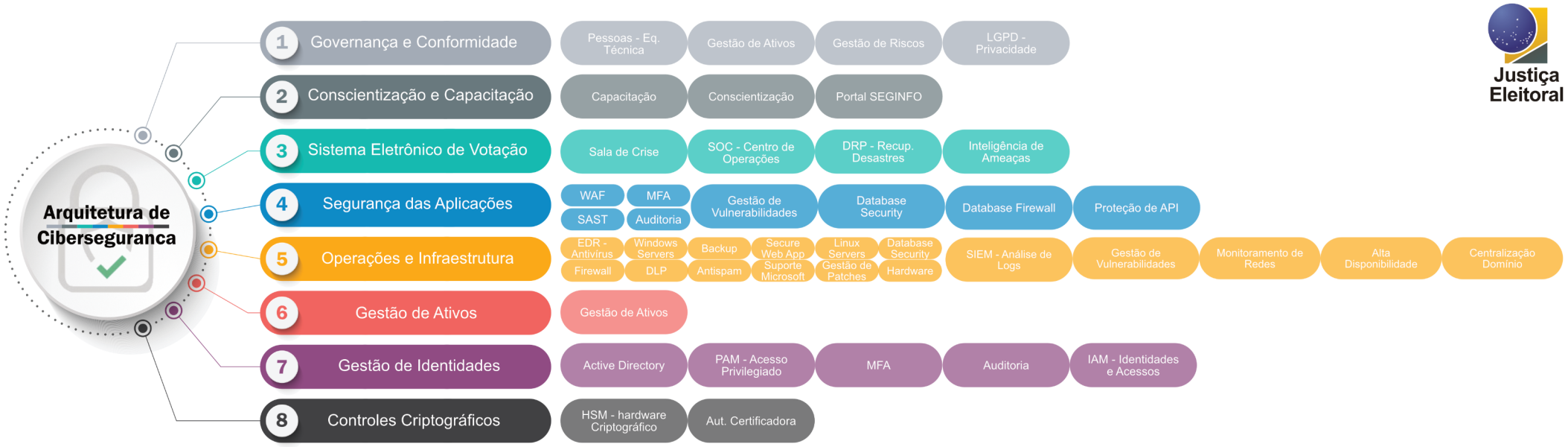
O objetivo é maximizar os fatores críticos de sucesso das aquisições.

Considerações Finais

O GT-SI reuniu o máximo de informações para subsidiar a arquitetura de cibersegurança da JE, bem como as contratações, processos e planejamentos. Vários desafios estão lançados, seja na reformulação do ambiente Windows, seja na implementação de um serviço de SOC. É imprescindível, neste contexto, que todas as ações sejam adequadamente gerenciadas, para que possam surtir efeitos práticos nas Eleições 2022.

Outro ponto que gostaríamos de ressaltar é que não existe uma "bala de prata". O planejamento precisa ser seguido de ações e avaliações constantes.

Agradecemos a oportunidade de utilizar o conhecimento técnico do GT-SI para contribuir com o aumento da resiliência da Justiça Eleitoral e desejamos a todos os nossos colegas um enorme sucesso na condução das iniciativas.



Justiça Eleitoral

Ver. 1.0 2021