ATA DE REUNIÃO
COMITÊ DE GOVERNANÇA DE TIC
PROAD 8314/2025

Data e horário: 21 de mai. de 2026 17:00 BRT

Local: Telepresencial

Lista de Presença			
NOME DO INTEGRANTE OU CONVIDADO	DESIGNAÇÃO	PRESENÇA	AUSÊNCIA JUSTIFICADA
Des. João Pedro Silvestrin	*Magistrado / Presidente do Comitê*	☑	☐
Desª. Carmen Izabel Centena Gonzalez	*Magistrada*	☑	☐
Desª. Tânia Regina Silva Reckziegel	*Magistrada*	☑	☐
Juiz Luiz Antonio Colussi	*Magistrado / Diretor do Foro de Porto Alegre*	☐	☑
Juiz Renato Barros Fagundes	*Magistrado*	☑	☐
Juíza Carolina Quadrado Ilha	*Magistrado / Representante da Secretaria da Corregedoria*	☑	☐
Enilda Souza de Andrade	Secretário-Geral da Presidência	☐	☑
Rejane Carvalho Donis	Diretora-Geral	☐	☑
Aldo da Silva Jardim	Secretário-Geral Judiciário	☑	☐
Natacha Moraes de Oliveira	Secretária-Geral de Tecnologia e Inovação	☑	☐
André Soares Farias	Diretor da Secretaria de Sistemas de Informação	☑	☐
José Cláudio da Rosa Riccardi	Representante da Secretaria de Auditoria	☑	☐
Paulo Mendes Ribeiro Junior	Diretor da Secretaria de Infraestrutura e Serviços	☑	☐
Paulo Roberto do Carmo	Coordenador de Desenvolvimento de Sistemas	☑	☐
Lucas Pozatti	Coordenador de Segurança da Informação e Proteção de Dados	☑	☐
Denilson Ribeiro de Quadros	Coordenador de Serviços de TIC	☑	☐
Pablo Paulo Lopes Barros	Coordenador de Implantação de Sistemas	☑	☐

Alberto Daniel Muller	Coordenador de Gestão e apoio à Governança de TIC	☑	☐

Unidade de apoio executivo: SETIC

Secretária: Deise Alexandra Koerber, Chefe da Divisão de Projetos e Assessoramento Adm de TIC

PAUTA

1. Relato sobre o Galileu
2. Bloqueio do encaminhamento automático de mensagens para e-mails particulares e uso de tokens.
3. Proibição da utilização de canais privados para a recuperação de credenciais (Portaria Presidência CNJ 158/2026)
4. Plano de Contratações 2026 - Demanda Nova
5. Aprovação da revisão de processos de TIC
6. Assuntos Gerais

O Desembargador João Pedro Silvestrin, Presidente do CGTIC, deu as boas-vindas aos presentes e passou a palavra para a Secretária-Geral de Tecnologia e Inovação, Natacha Moraes de Oliveira.

DELIBERAÇÕES E RESULTADOS

1 - Relato sobre o Galileu: Natacha informou que o Tribunal está passando por uma auditoria operacional do TCU focada no sistema Galileu. O trabalho foi descrito como uma "construção coletiva", e os auditores demonstraram satisfação com a organização e os controles de segurança da ferramenta. Além disso, discutiu-se a repercussão de caso ocorrido no TRT8 em que o Galileu detectou um "prompt injection" em peça processual e sobre o risco de ocorrências similares com uso de outras ferramentas de IA. Foi sugerido que o Centro de Inteligência e a Corregedoria expeçam orientações aos magistrados sobre como proceder ao identificar peças trazidas aos autos com a presença de informações inseridas de modo a não serem visíveis a olho nú, configurando injeção de instruções para sistemas de inteligência artificial.

2. Implementação de duplo fator de autenticação na Plataforma Digital do Poder Judiciário. Código gerado em aplicativo autenticador.
Em atendimento ao Ofício 40/2026/SG do CNJ, foi implementado em 18 de maio de 2026 a extinção do envio de tokens de autenticação por e-mail, tornando o uso de aplicativos de OTP (segundo fator de autenticação) no celular como meio oficial para o recebimento dos tokens.

Natacha relatou que alguns usuários estão utilizando extensões de navegadores como Authenticator.cc para geração desses códigos, o que deixaria de exigir o uso dos celulares. No entanto, essa solução traz vulnerabilidades e não atende a demanda do CNJ, que se refere não apenas a existência de um aplicativo gerador de chaves, mas que também garanta a segregação efetiva entre os fatores de autenticação, da

proteção das “sementes” usadas para geração desses tokens e da resistência a ataques de phishing e malwares. Assim, o TRT não pode sugerir essa solução.
A Desembargadora Tânia relatou que magistrados, em diversos grupos de comunicação, têm apresentado fortes reclamações sobre a obrigatoriedade de utilizar seus aparelhos celulares particulares para o recebimento de chaves de autenticação. Esclareceu que, individualmente, não se opõe ao uso do celular e até considera a mais prático, mas sentiu a necessidade de reportar o descontentamento coletivo para que a Administração pudesse decidir como proceder. Como alternativa futura para quem não deseja usar o celular, o comitê discutiu a possibilidade de uso de chaves físicas (UbiKeys) ou outras soluões .Por fim, Natacha esclareceu que está sendo conduzido projeto já autorizado pelo Comitê de Governança de TIC para contratação de solução chamada ZTNA - Zero Trust Network Access, que poderá ser utilizada também nesse contexto. O Ofício do CNJ e o relatório de análise de segurança do uso de extensões seguem anexos à presente ata.

3. Proibição da utilização de canais privados para a recuperação de credenciais (Portaria Presidência CNJ 158/2026)

Ainda na linha da segurança do processo de autenticação e segurança, o Tribunal precisa atender ao que restou definido na Portaria citada, de abril de 206, que determinou aos órgãos do Poder Judiciário a proibição da utilização de canais privados para a recuperação de credenciais e demais elementos de autenticação, sendo vedados, nesse processo, dentre outros, o uso e-mails pessoais (Gmail, Hotmail, Yahoo, etc.), evitando o envio de códigos ou links de recuperação para infraestruturas externas aos órgãos. Ainda, a Portaria citada determinou a revisão e eventual substituição de mecanismos de autoatendimento que não assegurem a identificação inequívoca do usuário. Por fim, determinou a proibição do redirecionamento ou encaminhamento automático de e-mails institucionais para provedores pessoais (Gmail, Hotmail, Yahoo, etc.), evitando o bypass de controles de segurança e o enfraquecimento de mecanismos de autenticação institucionais. Deu, por fim, prazo de 60 (sessenta) dias para a implementação das medidas. **Nesse contexto, o Comitê aprova, nessa oportunidade, a eliminação de qualquer redirecionamento de e-mails institucionais a provedores privados, definindo que os usuários serão avisados e instruídos sobre como reverter tal configuração das caixas postais sob sua responsabilidade, sendo concedido prazo de dez dias para a interrupção desse redirecionamento.** A Portaria referida segue em anexo.

4. Plano de Contratações 2026 - Demanda Nova: Natacha apresentou a necessidade de inclusão no plano de contratações da renovação da garantia da *Tape Library* (equipamento de armazenamento de backups permanentes). O valor estimado é de R$17.974,00, que será remanejado dentro do orçamento atual enquanto se aguarda uma suplementação orçamentária para TI. Demanda aprovada por todos.

ID	Descrição	Justificativa	Valor Estimado	Valor PCA (24 meses)
88	Renovação Tape Library LTO-8	Extensão de garantia das bibliotecas de fitas LTO-8 por 2 anos. Esses equipamentos são responsáveis pela gravação dos backups históricos dos dados	R$ 17.974,11 (mensal de R$ 5.991,37)	R$ 143.792,88

		do TRT, especialmente os processos judiciais, cujas fitas são guardadas em cofres.		

5. Aprovação da revisão de processos de TIC: Foi apresentada e, ao final aprovada pelo Comitê, a revisão de dois processos dois processos de trabalho da TI:

1. **Gerenciamento de Disponibilidade e Capacidade:** Atualização técnica de fluxos internos.
2. **Gerenciamento da Central de Serviços:** Adequação do fluxo de atendimento de chamados à ferramenta Qualitor.

6. Assuntos Gerais:

- **Incidente de Privacidade em Reuniões Virtuais (Read AI):** A Desembargadora Tânia relatou um incidente grave em que uma ferramenta de IA de terceiros (Read AI) ingressou em uma reunião para atendimento a um advogado. Relatou que recebeu e-mail com a transcrição da reunião e que percebeu que a ferramenta continuou a transcrever as conversas mesmo após a saída do advogado externo que a inseriu na reunião. A TI esclareceu que esses "transcritores" entram como convidados e que tal comportamento já foi bloqueado na plataforma Google do TRT. Entrentanto, se os usuários entrarem na videoconferência utilizando e-mails pessoais, esse controle não estará presente. A TI comprometeu-se a validar se houve falha no bloqueio técnico realizado e a emitir uma orientação para que os organizadores verifiquem sempre a lista de participantes e removam participantes estranhos.

- **Evolução do Galileu e Minuta de Embargos de Declaração (ED):** O Juiz Renato apresentou um relato sobre a nova versão do Galileu, que agora permite a **elaboração de minutas completas de decisões de ED**. A ferramenta busca o histórico de decisões do próprio juiz para manter o estilo de escrita e permite a edição de tópicos específicos, sendo superior, nessa funcionalidade,a outras ferramentas de mercado. A funcionalidade está em teste por um grupo restrito de magistrados e será expandida para o primeiro e segundo graus, simultaneamente, em breve.
- **Data da Próxima reunião:** A próxima reunião foi agendada para o dia 18 de junho, às 10h30

Nada mais havendo a tratar, o Desembargador João Pedro Silvestrin agradeceu a presença de todos e declarou encerrada a reunião.

Ata validada por e-mail pelos(as) participantes.

Poder Judiciário
Conselho Nacional de Justiça

Ofício Circular nº 40/2026/SG

Brasília, *data da assinatura eletrônica*.

A Sua Excelência o Senhor
Desembargador Alexandre Corrêa da Cruz
Presidente do Tribunal Regional do Trabalho da 4ª Região
Porto Alegre - RS

Assunto: **Implementação de duplo fator de autenticação na Plataforma Digital do Poder Judiciário. Código gerado em aplicativo autenticador.**

Senhor Presidente,

Informo a Vossa Excelência que, em continuidade às ações do Conselho Nacional de Justiça voltadas a reforçar a segurança e a confiabilidade dos serviços digitais do Poder Judiciário, e em atenção à Portaria Presidência nº 140/2024, foi revista a forma de autenticação em múltiplos fatores (MFA) para todos os usuários da Plataforma Digital do Poder Judiciário.

Em substituição ao mecanismo anteriormente adotado para envio de códigos temporários (OTP) por correio eletrônico, passa a ser utilizado o procedimento de geração de códigos por meio de aplicativo autenticador instalado em dispositivo móvel do usuário. A atualização tem por objetivo aprimorar o processo de autenticação dos usuários internos do Poder Judiciário, conferindo maior robustez, disponibilidade e segurança ao acesso às aplicações integradas à Plataforma Digital do Poder Judiciário.

Sob uma perspectiva operacional, o fluxo de autenticação com certificado digital ou mediante uso de usuário/senha passará a funcionar da seguinte forma:

1. o usuário se autentica no Portal Jus.br ou sistema processual integrado à PDPJ-Br, por meio de certificado digital ou login/senha;

2. no primeiro acesso, será exibido um **QR Code** para configuração de um aplicativo autenticador (Google Authenticator, FreeOTP ou similar);

3. o usuário deverá informar o **código temporário de 6 dígitos** gerado pelo aplicativo para concluir o acesso; e

4. nos acessos seguintes, o usuário seguirá os passos 1 e 3.

Serão afetados todos os usuários que utilizem aplicações integradas à PDPJ, Portal Jus.br e ao SSO. Recomendo ampla divulgação aos usuários acerca do novo procedimento e da obrigatoriedade de configurar o aplicativo autenticador.

Esse novo modelo elimina a dependência de envio de códigos por *e-mail*, garantindo maior disponibilidade e segurança no processo de autenticação, e **entrará em vigor em 18/05/2026.**

Nesse sentido, solicito a cooperação dos Dirigentes de Tecnologia da Informação e Comunicação, sendo essa comunicação essencial para que a mudança possa ocorrer sem maiores impactos.

A Central de Atendimento aos Usuários deste CNJ está disponível para eventuais esclarecimentos, pelo *link* https://suporteti.cnj.jus.br .

Juíza **Clara Mota**
Secretária-Geral

Documento assinado eletronicamente por **CLARA DA MOTA SANTOS PIMENTA ALVES**, **SECRETÁRIA-GERAL - SECRETARIA-GERAL**, em 19/03/2026, às 15:13, conforme art. 1º, §2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no portal do CNJ informando o código verificador **2534812** e o código CRC **39984CE0**.

Atenção: Ao responder este ofício, favor citar o SEI nº 13667/2025. A resposta deverá ser encaminhada por meio do sistema Malote Digital ou Protocolo Eletrônico (https://www.cnj.jus.br/formularios/protocolo-eletronico/).

Poder Judiciário
Conselho Nacional de Justiça

PORTARIA PRESIDÊNCIA Nº 158 DE 13 DE ABRIL DE 2026.

Determina a proibição da utilização de canais privados para a recuperação de credenciais e demais elementos de autenticação no âmbito dos órgãos do Poder Judiciário brasileiro.

O PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ), no uso de suas atribuições legais e regimentais e considerando o disposto no processo SEI/CNJ nº 05800/2026,

RESOLVE:

Art. 1º Determinar aos órgãos do Poder Judiciário Brasileiro, com exceção do Supremo Tribunal Federal, a proibição da utilização de canais privados para a recuperação de credenciais e demais elementos de autenticação, sendo vedados, nesse processo, o uso de:

I - mensagens do tipo SMS, evitando o ataque do tipo *SIM Swap; e*

II - *e-mails* pessoais (Gmail, Hotmail, Yahoo, etc.), evitando o envio de códigos ou links de recuperação para infraestruturas externas aos órgãos.

§ 1º Consideram-se credenciais e demais elementos de autenticação: usuário, senha, mecanismo de autenticação multifator, dispositivo confiável, QR code e outros.

§ 2º A proibição abrange usuários institucionais internos (magistrados e servidores) ativos.

Art. 2º Determinar a revisão e eventual substituição de mecanismos de autoatendimento que não assegurem a identificação inequívoca do usuário.

Parágrafo único. A identificação inequívoca deve ser feita independentemente do canal sendo utilizado pelo usuário (*Internet*, telefone, totens, etc.).

Art. 3º Determinar a proibição do redirecionamento ou encaminhamento automático de e-mails institucionais para provedores pessoais (Gmail, Hotmail, Yahoo, etc.), evitando o *bypass* de controles de segurança e o enfraquecimento de mecanismos de autenticação institucionais.

Art. 4º Fixar o prazo de 60 (sessenta) dias para a implementação das medidas desta Portaria.

Art. 5º Esta Portaria entre em vigor na data de sua publicação.

Ministro **Edson Fachin**

Documento assinado eletronicamente por **LUIZ EDSON FACHIN**, **PRESIDENTE**, em 23/04/2026, às 19:27, conforme art. 1º, §2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no portal do CNJ informando o código verificador **2566707** e o código CRC **D6CE5674**.

CSIPD - Uso de Autenticadores na PDPJ e MFA Baseado em OTP

A transição do **PDPJ (Plataforma Digital do Poder Judiciário)** para o uso exclusivo de **OTP (One-Time Password)** como segundo fator de autenticação (MFA) eleva o patamar de segurança institucional. Contudo, a eficácia dessa medida depende diretamente do método de custódia das chaves secretas (seeds).

Abaixo, apresento uma análise técnica consolidada, categorizada pelos riscos inerentes a cada abordagem tecnológica.

1. Contextualização

Com a adoção de autenticação multifator (MFA) exclusivamente baseada em OTP/TOTP para acesso ao ecossistema do Processo Judicial Digital Brasileiro (PDPJ), torna-se necessário avaliar os riscos de segurança associados às diferentes abordagens de aplicativos autenticadores.

Embora o uso de OTP represente avanço significativo em relação a mecanismos mais frágeis — como autenticação baseada apenas em senha ou envio de códigos por SMS — o nível efetivo de segurança depende diretamente de:

- onde o segredo TOTP (seed) é armazenado;
- como ocorre a segregação do segundo fator;
- qual o nível de proteção do dispositivo autenticador;
- a resistência da solução a phishing, malware e comprometimento do endpoint;
- os mecanismos de governança e controle institucional disponíveis.

No contexto do Poder Judiciário, tais aspectos assumem criticidade elevada em razão:

- do acesso a dados sigilosos;
- da possibilidade de prática de atos processuais;
- da existência de perfis privilegiados;
- da integração nacional entre sistemas judiciais;
- do potencial impacto institucional de comprometimentos de credenciais.

Dessa forma, esta análise avalia os riscos associados às principais categorias de autenticadores atualmente utilizadas.

2. Princípio de Segurança do MFA

O MFA baseia-se no princípio de que o comprometimento de um fator não deve implicar comprometimento automático dos demais.

Idealmente:

- a senha deve estar em um ambiente;
- o segundo fator em outro;
- e ambos devem possuir mecanismos independentes de proteção.

Quanto maior a segregação entre:

- dispositivo autenticado;
- navegador;
- sessão;
- e autenticador,

maior a efetividade do MFA.

Quando senha, sessão autenticada e OTP coexistem no mesmo endpoint, ocorre redução substancial da efetividade do segundo fator.

3a. Extensões de Navegador (Ex: Authenticator.cc)

Embora ofereçam conveniência e código aberto, as extensões são o elo mais frágil na cadeia de confiança do MFA.

- **Violação do Princípio de Posse:** O MFA ideal exige um dispositivo físico separado. Ao usar uma extensão no mesmo navegador do acesso ao PDPJ, os dois fatores de autenticação (senha e OTP) residem no mesmo ambiente de software.
- **Comprometimento do Host:** Se a estação de trabalho for infectada por um *infostealer* ou *Remote Access Trojan* (RAT), o atacante terá acesso simultâneo às credenciais e à ferramenta que gera os códigos.
- **Exposição de Sementes (Seeds):** Sem uma senha mestre robusta configurada na extensão, as chaves secretas ficam vulneráveis no armazenamento local do navegador, podendo ser exportadas por usuários mal-intencionados ou scripts.

3b. Aplicativos Móveis (Google, Microsoft, Aegis)

Representam o equilíbrio entre segurança e custo, utilizando o isolamento de processos (*sandboxing*) dos sistemas iOS e Android.

- **Risco de Sincronização em Nuvem:** Aplicativos que realizam backup automático (como o Microsoft Authenticator) transferem o risco para a conta pessoal do usuário.

Se o e-mail pessoal (Gmail/Outlook) for invadido, o acesso ao PDPJ pode ser comprometido via restauração de backup.

- **Ameaça de Engenharia Social:** O atacante pode induzir o usuário a digitar o código em um site de *phishing* em tempo real. O aplicativo gera o código corretamente, mas não possui inteligência para validar se o destino é o portal oficial do Judiciário.

3c. Gerenciadores de Senhas Integrados (Bitwarden, 1Password)

Soluções que armazenam tanto a senha quanto o segredo TOTP no mesmo cofre digital.

- **Centralização de Falha:** O risco principal é o "tudo ou nada". O comprometimento da senha mestra do gerenciador anula completamente o benefício do segundo fator, pois o invasor obtém ambos os componentes de uma só vez.
- **Vantagem Operacional:** Reduz a perda de acesso por falha de hardware e permite auditoria de acesso em ambientes corporativos.

3d. Chaves de Segurança de Hardware (YubiKey, Google Titan)

Consideradas o "Padrão Ouro" de segurança (NIST AAL3), pois a chave criptográfica nunca deixa o dispositivo físico.

- **Imunidade a Ataques Remotos:** Ao contrário do authenticator.cc, não há malware capaz de "copiar" a semente de uma chave física via rede.
- **Risco de Perda Física:** O maior risco é logístico. A perda do token exige processos de recuperação de conta que podem ser morosos em uma estrutura complexa como o Poder Judiciário.

Análise Comparativa de Riscos

Solução	Vetor de Risco Principal	Nível de Isolamento	Confiabilidade Institucional
Extensões (Navegador)	Malware no PC / Sequestro de Sessão	Baixo	**Baixa**
Mobile Apps	Invasão de Nuvem Pessoal / Phishing	Médio-Alto	**Média-Alta**
Gerenciadores de Senha	Quebra da Senha Mestra	Médio	**Média**
Hardware Tokens	Perda Física do Dispositivo	Máximo	**Alta (Crítica)**

4. Recomendações Técnicas

Para garantir a integridade do ecossistema PDPJ, recomenda-se uma estratégia de segurança em camadas, estratificada pelo perfil de acesso:

Para Magistrados e Administradores de TI

- **Uso de Hardware Tokens:** Implementar chaves físicas (FIDO2/TOTP). O impacto de um vazamento nestas contas é catastrófico, justificando o custo do hardware.
- **Backup:** Manter uma segunda chave física de backup guardada em local seguro (cofre).

Para Servidores e Usuários em Geral

- **Migração para Mobile:** Substituir extensões de navegador por aplicativos móveis (como o **Aegis** para Android ou **Raivo** para iOS), que permitem backups criptografados localmente.
- **Proibição de "Segredos em Texto Claro":** Bloquear via política institucional o armazenamento de sementes de OTP em arquivos TXT, planilhas ou e-mails.

Governança sobre o Authenticator.cc

- Caso o uso da extensão seja a única via possível em determinados terminais, é **obrigatória** a configuração de uma senha mestre única para a extensão e a desativação da sincronização com nuvens pessoais (Google/Dropbox).

A segurança do MFA no PDPJ não é apenas sobre *ter* um código, mas sobre *onde* esse código nasce e como ele é protegido antes de chegar à tela.

5. Conclusão

No contexto do PDPJ, a segurança do MFA não depende apenas da existência de um aplicativo gerador de OTP, mas principalmente:

- da segregação efetiva entre fatores;
- da proteção das seeds;
- da resistência da solução a phishing e malware;
- da governança institucional disponível.

Soluções baseadas em extensões de navegador, como o Authenticator.cc, apresentam limitações estruturais importantes por reduzirem significativamente a independência do segundo fator.

Aplicativos mobile autenticadores representam o nível mínimo recomendável de maturidade.

Entretanto, para ambientes judiciais críticos, o modelo mais aderente às boas práticas modernas de identidade e Zero Trust é a adoção de mecanismos FIDO2/passkeys e tokens físicos resistentes a phishing.

Anexo - Análise dos Riscos por Abordagem

1. Extensões de Navegador (Authenticator.cc e similares)

Características

Soluções como o Authenticator.cc operam diretamente como extensões do navegador, armazenando localmente as seeds TOTP e gerando os códigos no próprio browser utilizado para autenticação.

Principais riscos

1.1. Quebra da segregação do segundo fator

Este é o principal risco da abordagem.

Quando:

- senha;
- sessão;
- e OTP

estão no mesmo endpoint, o MFA perde grande parte de sua efetividade.

Em caso de comprometimento da estação:

- malware pode capturar credenciais;
- acessar sessões;
- extrair seeds TOTP;
- gerar OTPs válidos;
- e realizar autenticações completas.

Nesse cenário, o MFA deixa de funcionar como barreira adicional relevante.

1.2. Risco inerente a extensões de navegador

Extensões possuem histórico recorrente de:

- supply chain compromise;
- takeover de contas de desenvolvedores;
- atualizações maliciosas;
- permissões excessivas;
- exfiltração de dados.

Mesmo extensões legítimas podem tornar-se vetores de ataque futuramente.

O risco é ampliado no Judiciário porque:

- navegadores acessam sistemas críticos;
- usuários frequentemente possuem privilégios elevados;
- há grande volume de dados sensíveis.

1.3. Exposição das seeds TOTP

As seeds:

- permanecem armazenadas localmente;
- podem ser sincronizadas via perfil do navegador;
- podem ser incluídas em backups;
- podem ser extraídas por malware ou em análise forense da estação.

Uma vez comprometida a seed:

- o atacante passa a gerar OTPs indefinidamente.

1.4. Dependência integral da segurança do endpoint

Toda a segurança passa a depender:

- do hardening da estação;
- do navegador;
- do antimalware/EDR;
- da ausência de comprometimento local.

Assim, ataques como:

- infostealers;
- RATs;
- malware de browser;
- sequestro de sessão;

passam a neutralizar o MFA.

Avaliação de risco

Critério	Avaliação
Segregação do MFA	Fraca
Resistência a malware	Baixa
Resistência a phishing	Baixa
Governança institucional	Baixa

Adequação para perfis privilegiados	Inadequada
Adequação ao PDPJ	Apenas excepcional

2. Aplicativos Mobile TOTP (Google Authenticator, Aegis, FreeOTP)

Características

Nesta abordagem:

- o segundo fator permanece em dispositivo distinto;
- normalmente em smartphone;
- isolado do navegador e da estação de trabalho.

Isso já representa ganho substancial de segurança em relação a extensões browser.

Principais riscos

2.1. Comprometimento do dispositivo móvel

Embora segregado do endpoint principal, o dispositivo móvel ainda pode sofrer:

- malware;
- rooting/jailbreak;
- roubo físico;
- comprometimento de backups.

2.2. Clonagem de seeds no onboarding

Durante o cadastro inicial do QR Code:

- captura indevida da seed;
- screenshots;
- compartilhamentos;

podem comprometer o MFA permanentemente.

2.3. Dependência de boas práticas do usuário

Riscos operacionais incluem:

- ausência de backup;
- perda do dispositivo;
- troca de aparelho;

- uso de dispositivos pessoais inseguros.

Avaliação específica das principais soluções

Google Authenticator

Google Authenticator

Pontos positivos

- simplicidade;
- ampla compatibilidade;
- segregação do segundo fator;
- baixa complexidade operacional.

Limitações

- poucos recursos corporativos;
- governança limitada;
- histórico de dificuldades de recuperação e backup.

Aegis Authenticator

Aegis Authenticator

Pontos positivos

- open source;
- forte foco em privacidade;
- backup criptografado;
- controle local das seeds;
- excelente proteção técnica.

Limitações

- ausência de gestão enterprise robusta;
- curva operacional maior;
- disponível apenas para Android.

Avaliação consolidada

Critério	Avaliação
Segregação do MFA	Boa
Resistência a malware	Média

Resistência a phishing	Média
Governança institucional	Média
Adequação ao PDPJ	Boa

3. Microsoft Authenticator e Ecossistemas Corporativos

Microsoft Authenticator

Características

Além do TOTP tradicional, a solução oferece:

- push MFA;
- device binding;
- biometria;
- Conditional Access;
- integração com Entra ID;
- autenticação passwordless.

Principais vantagens

3.1. Melhor governança institucional

Permite:

- integração com MDM;
- políticas corporativas;
- controle centralizado;
- auditoria;
- gerenciamento de dispositivos.

3.2. Redução de ataques de phishing

Recursos como:

- push approval;
- number matching;
- autenticação contextual;

reduzem ataques de:

- MFA fatigue;

- replay;
- phishing tradicional.

3.3. Melhor aderência a Zero Trust

A solução suporta:

- autenticação contextual;
- avaliação do dispositivo;
- identidade forte;
- políticas adaptativas.

Limitações

- dependência do ecossistema Microsoft;
- solução parcialmente proprietária;
- eventual preocupação com telemetria.

Avaliação de risco

Critério	Avaliação
Segregação do MFA	Boa
Resistência a malware	Boa
Resistência a phishing	Boa
Governança institucional	Alta
Adequação ao PDPJ	Muito recomendável

4. Password Managers com TOTP Integrado (Bitwarden, 1Password)

Características

Nessa abordagem:

- senha;
- OTP;
- eventualmente passkeys;

são armazenados no mesmo cofre.

Principal risco

A quebra parcial do conceito de MFA.

Se o cofre for comprometido:

- o atacante obtém simultaneamente:
    - senha;
    - segundo fator.

Isso reduz substancialmente a independência dos fatores.

Cenários aceitáveis

Pode ser aceitável:

- para contas de baixo risco;
- usuários avançados;
- ambientes muito bem protegidos.

No contexto do Judiciário

Não é recomendável para:

- magistrados;
- administradores;
- usuários privilegiados;
- acesso ao PDPJ.

Avaliação de risco

Critério	Avaliação
Segregação do MFA	Parcial
Resistência a malware	Média
Resistência a phishing	Média
Governança institucional	Boa
Adequação ao PDPJ	Restrita

5. Tokens Físicos e FIDO2 (YubiKey, Passkeys, Smartcards)

YubiKey

Características

Representam atualmente o padrão mais robusto de autenticação forte.

Baseiam-se em:

- hardware dedicado;
- segredo não exportável;
- autenticação criptográfica;
- resistência a phishing.

Principais vantagens

5.1. Resistência a phishing

O segredo criptográfico:

- não é compartilhado com o site;
- não pode ser reutilizado;
- é vinculado ao domínio legítimo.

Isso praticamente elimina phishing tradicional de credenciais.

5.2. Segredo não exportável

Mesmo com comprometimento da estação:

- o atacante não extrai o segredo do token.

5.3. MFA efetivamente segregado

O atacante precisa:

- do dispositivo físico;
- da interação do usuário;
- eventualmente de PIN ou biometria.

Limitações

- maior custo;
- logística de distribuição;
- gestão de perda/substituição;

- necessidade de suporte institucional.

Avaliação de risco

Critério	Avaliação
Segregação do MFA	Excelente
Resistência a malware	Muito alta
Resistência a phishing	Excelente
Governança institucional	Alta
Adequação ao PDPJ	Melhor opção

6. Comparativo Consolidado

Solução	Segurança Geral	Segregação do MFA	Resistência a Phishing	Governança	Adequação ao PDPJ
Authenticator.cc	Baixa/Média	Fraca	Baixa	Baixa	Não recomendável
Google Authenticator	Média	Boa	Média	Média	Aceitável
Aegis	Alta	Boa	Média	Média	Muito boa
Microsoft Authenticator	Alta	Boa	Boa	Alta	Muito recomendável
Password Manager + TOTP	Média	Parcial	Média	Boa	Restrita
FIDO2 / YubiKey	Muito alta	Excelente	Excelente	Alta	Melhor opção

7. Recomendações

7.1. Recomendação Estratégica Principal

Para o ecossistema do Poder Judiciário, recomenda-se priorizar mecanismos:

- resistentes a phishing;
- com segregação efetiva do MFA;
- compatíveis com arquitetura Zero Trust;
- e com governança corporativa adequada.

Nesse contexto, a ordem de preferência recomendada é:

1. FIDO2 / Passkeys / Tokens físicos;
2. Microsoft Authenticator;
3. Aegis Authenticator;
4. Google Authenticator.

7.2. Recomendações Operacionais

Para perfis críticos

(magistrados, administradores, perfis privilegiados)

Recomenda-se:

- FIDO2;
- smartcards;
- tokens físicos;
- autenticação resistente a phishing.

Para usuários gerais

Priorizar:

- autenticadores mobile;
- preferencialmente integrados a políticas corporativas.

Evitar como padrão institucional

Não se recomenda:

- extensões browser como Authenticator.cc;
- MFA no mesmo endpoint autenticado;
- TOTP integrado ao mesmo cofre de senhas.

Essas abordagens devem ser tratadas apenas como:

- contingência;

- exceção formal;
- solução transitória.

7.3. Controles Compensatórios

Caso alguma solução de maior risco seja utilizada, recomenda-se:

- hardening de endpoints;
- EDR obrigatório;
- MDM em dispositivos móveis;
- controle de extensões;
- monitoramento comportamental;
- detecção de anomalias;
- políticas formais de exceção;
- revisão periódica de riscos.