Poder Judiciário
Conselho Nacional de Justiça

PORTARIA PRESIDÊNCIA Nº 408 DE 29 DE NOVEMBRO DE 2024.

Disciplina a Gestão de Identidade e Controle de Acesso no âmbito do ambiente tecnológico do Conselho Nacional de Justiça.

O PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ), no uso das atribuições legais e regimentais, e tendo em vista o contido no processo SEI/CNJ nº 00544/2024,

CONSIDERANDO o disposto na Portaria Presidência n° 47/2017, que institui a Política de Segurança da Informação do Conselho Nacional de Justiça;

CONSIDERANDO o disposto na Portaria Presidência n° 197/2023, que dispõe sobre a Política de Cópia de Segurança (*Backup*) e Restauração (*Restore*) de Dados do CNJ;

CONSIDERANDO o disposto na Resolução CNJ n° 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO o disposto na Portaria Presidência n° 162/2021, que aprova o Manual de Referência Gestão de Identidade e de Controle de Acessos (Anexo VI);

CONSIDERANDO que os recursos de Tecnologia da Informação e Comunicação são ativos estratégicos e suportam processos institucionais importantes para os usuários internos e externos ao Conselho Nacional de Justiça;

CONSIDERANDO a necessidade de garantir um ambiente tecnológico controlado, bem como a disponibilidade, integridade, confidencialidade e autenticidade dos recursos de Tecnologia da Informação e Comunicação do CNJ;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1º A Gestão de Identidade e Controle de Acesso no âmbito do ambiente tecnológico do Conselho Nacional de Justiça ficam disciplinados por esta Portaria.

§ 1º Compete ao Departamento de Tecnologia da Informação e Comunicação (DTI) a gestão dos recursos computacionais instalados no ambiente tecnológico do CNJ ou gerenciados por ele, em conformidade com os normativos vigentes e as melhores práticas de segurança da informação.

§ 2º As medidas previstas nesta instrução aplicam-se a todos os usuários do ambiente tecnológico do CNJ, acarretando sua responsabilização em função de descumprimento, nos termos previstos em lei e demais regulamentos.

Art. 2º Para efeitos desta Portaria, considera-se:

I – acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

II – ambiente tecnológico: redes, dispositivos, *softwares*, processos, informação armazenada ou em trânsito, serviços e sistemas que possam ser conectados direta ou indiretamente a redes de computadores;

III – autenticação: processo de identificação das partes envolvidas em um processo;

IV – autenticação multifator: autenticação realizada com a utilização de dois ou mais elementos identificadores (senha, biometria, código de acesso único, entre outros);

V – confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

VI – conta de acesso: identidade digital do usuário, formalmente exercida pelo gestor negocial por meio do processo de gestão de identidade para acesso ao ambiente tecnológico (também conhecida como "usuário" ou "*login*");

VII – conta de serviço: conta de acesso associada a serviço digital ou sistema, e não a usuário;

VIII – controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos;

IX – disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável no momento que for necessária por pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X – gestão de identidade: atividade relacionada à criação, ao bloqueio e a contas de acesso, bem como o gerenciamento e proteção das informações que identificam um usuário no ambiente tecnológico;

XI – gestor negocial: responsável pela execução da atividade finalística no sistema ou conjunto de sistemas de Tecnologia da Informação e Comunicação (TIC), bem como pela definição dos perfis de acesso dos usuários;

XII – gestor técnico: responsável pela sustentação de determinado sistema, conjunto de sistemas ou infraestrutura de TIC, bem como a implementação do perfil de acesso ao usuário;

XIII – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XIV – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XV – perfil de acesso: coleção de atributos e permissões que um usuário ou grupo de usuários têm no ambiente tecnológico;

XVI – senha: conjunto de caracteres (letras, números e símbolos) escolhida e memorizada pelo usuário para realização do processo de autenticação;

XVII – usuário: indivíduo que pode acessar informações, sistemas ou serviços do ambiente tecnológico;

XVIII – usuários externos: magistrados, partes, advogados, membros do Ministério Público, visitantes e demais usuários que não estejam vinculados ao CNJ; e

XIX – usuários internos: conselheiros, magistrados, servidores, estagiários, bem como colaboradores, prestadores de serviço, e demais usuários que estejam formalmente vinculados ao CNJ.

CAPÍTULO II
DA GESTÃO DE IDENTIDADE E CONTROLE DE ACESSO

Seção I
Da Conta de Acesso

Art. 3º O acesso a recursos do ambiente tecnológico do CNJ está condicionado a:

I – identificação do usuário por meio da sua Conta de Acesso (ou Certificado Digital); e

II – autenticação do usuário por meio da senha pessoal ou outros fatores de autenticação.

Art. 4º A criação da Conta de Acesso, condicionada à identificação formal do usuário, será realizada por meio do processo de gestão de identidade, iniciado pelo gestor negocial e operacionalizado pela Central de Atendimento do DTI.

Art. 5º A Conta de Acesso será atribuída a cada usuário, de forma individual e intransferível, para uso exclusivo do seu titular.

§ 1º A Conta de Acesso deve obedecer aos seguintes requisitos:

I – possuir identificação única; e

II – ser gerenciada por sistema de gestão de identidades destinado a esse fim.

§ 2º Os usuários são responsáveis por todos os acessos e por todas as atividades desenvolvidas por meio da sua Conta de Acesso, podendo ser responsabilizados pelos danos decorrentes de sua má utilização.

§ 3º Caso seja detectado acesso ou atividade considerada suspeita, a Conta de Acesso poderá ser bloqueada para fins de segurança e auditoria.

§ 4º Não será permitida a criação de contas de acesso genéricas não associadas a um usuário específico, exceto em casos pontuais devidamente justificados, com duração não superior a 30 (trinta) dias.

§ 5º Caso haja necessidade de criar contas de serviço, essas deverão estar vinculadas a Contas de Acesso pertencentes a usuários internos.

Art. 6º As Contas de Acesso poderão ser temporariamente bloqueadas:

I – automaticamente após tentativas fracassadas de acesso;

II – quando houver a suspeita de seu comprometimento;

III – quando identificada inatividade de 60 (sessenta) dias corridos ou conforme determinação do gestor negocial; e

IV – quando a senha não for alterada no prazo determinado nesta Portaria.

Parágrafo único. A Conta de Acesso poderá ser reativada por manifestação do usuário, mediante justificativa endereçada à Secretaria de Gestão de Pessoas (SGP) ou aos gestores negociais.

Seção II
Da senha

Art. 7º A senha associada à Conta de Acesso deve obedecer aos seguintes requisitos:

I – tamanho mínimo de 8 (oito) caracteres quando a autenticação multifator estiver ativada;

II – tamanho mínimo de 14 (quatorze) caracteres quando a autenticação multifator não estiver ativada;

III – incluir, no mínimo, uma letra maiúscula, uma letra minúscula, um dígito e um caractere especial (por exemplo: !@#$%&*+-<>);

IV – não estar presente em bases de dados de vazamentos conhecidos, disponíveis publicamente na internet; e

V – quando da alteração conveniente ou programada de senha, as três senhas anteriores não poderão ser utilizadas.

Art. 8º É vedado a qualquer usuário se apropriar ou compartilhar Conta de Acesso, senha ou Certificado Digital pertencente a terceiros.

Art. 9º As senhas deverão ser mantidas em sigilo e protegidas contra leitura em texto aberto, inclusive no sistema de gestão de identidades e demais bases internas de dados, bem como ter seu tráfego protegido por meio de canal criptografado.

Parágrafo único. O DTI poderá realizar, de forma proativa, auditoria para determinar se as senhas utilizadas pelos usuários permanecem seguras e não estão presentes em bases de dados de vazamentos conhecidos na internet.

Art. 10. A alteração da senha deve ocorrer quando houver suspeita do seu comprometimento.

Seção III

Da Autenticação

Art. 11. O processo de autenticação ocorrerá mediante identificação da Conta de Acesso (ou Certificado Digital) e a correta verificação da senha ou de outros fatores de autenticação exigidos pelo recurso de TIC ao ser acessado.

§ 1º A autenticação multifator é obrigatória para acessar quaisquer recursos de TIC do ambiente tecnológico do CNJ disponibilizados na internet.

§ 2º A autenticação simples (apenas senha) pode ser utilizada quando o usuário interno se encontra conectado à rede do CNJ nos seguintes cenários:

I – usuário presente fisicamente nas dependências do CNJ e utilizando recursos de microinformática disponibilizados pelo DTI; e

II – usuário em teletrabalho acessando remotamente o ambiente tecnológico do CNJ por meio de canal criptografado seguro disponibilizado pelo DTI.

Art. 12. É facultado ao gestor negocial utilizar a autenticação única do Governo Federal (acesso.gov.br) desde que a autenticação multifator esteja habilitada.

Seção IV

Da concessão do perfil de acesso

Art. 13. Os gestores negociais deverão enviar à Central de Atendimento do DTI informações que impliquem na criação, no bloqueio temporário e na inativação de Contas de Acesso de usuários, bem como permissões e atributos referentes ao perfil de acesso desses usuários.

§ 1º A SGP ocupará a condição de gestor negocial para conselheiros, magistrados, servidores e estagiários do CNJ;

§ 2º Os gestores de contratos administrativos e de termos de cooperação técnica deste Conselho ocuparão a condição de gestores negociais para colaboradores e prestadores de serviços;

§ 3º Os gestores dos serviços digitais constantes do Portfólio de Soluções de Tecnologia da Informação e Comunicação do CNJ ocuparão a condição de gestores negociais para os usuários afetos aos seus serviços.

§ 4º Os gestores negociais definirão os perfis de acesso para cada usuário, sendo o gestor técnico responsável por operacionalizá-los.

Art. 14. Após aprovação do gestor técnico ou gestor negocial, a Central de Atendimento do DTI, no prazo de 24 (vinte e quatro) horas a contar do recebimento da comunicação, promoverá a adequação da conta e do perfil de acesso do usuário.

§ 1º Em caso de desligamento, as contas de acesso serão inativadas no ambiente corporativo do CNJ, bem como em todos os sistemas internos, incluindo sistemas licenciados, e ainda nos sistemas nacionais sob administração do CNJ.

§ 2º Magistrados e servidores requisitados para atuação junto ao CNJ deverão, a partir do desligamento, obter junto aos administradores regionais dos respectivos tribunais de origem, a restauração de seus perfis de acesso, conforme lotação e necessidade negocial.

§ 3º O DTI assegurará a retenção de arquivos pessoais de usuários desligados pelo prazo de 30 (trinta) dias, a contar da data de desligamento, durante o qual disponibilizará cópia de segurança ao interessado, mediante provocação.

Art. 15. Ao final de cada semestre, gestores técnicos e negociais deverão, conjuntamente, promover auditoria nos sistemas de gestão de identidades, a fim de remover contas de acesso obsoletas e adequar os perfis de acesso dos usuários ativos.

Seção V

Do sistema de gestão de identidades

Art. 16. O DTI deverá adotar sistema de gestão de identidades centralizado por meio do qual serão geradas as contas e senhas, e criados os perfis de acesso ao ambiente tecnológico do CNJ, cujos objetivos são:

I – eliminar a necessidade de uso de Contas de Acesso genéricas, com perfil especial ou perfil de administrador;

II – autorizar o acesso somente aos recursos necessários, observando-se a regra de privilégio mínimo; e

III – eliminar Contas de Acesso redundantes, eventualmente presentes nos sistemas descentralizados ou em outros recursos de TIC independentes.

§ 1º O sistema de que trata o *caput* deste artigo deverá atender, ao menos, os seguintes requisitos:

I – permitir cadastramento de informações do usuário;

II – suportar acesso embasado em papeis ou na função "*Role Based Access*" (RBAC);

III – definir diferentes níveis de privilégio de acesso para um usuário;

IV – vincular um usuário a um ou a mais papeis;

V – possuir interface gráfica de gerenciamento;

VI – suportar protocolos seguros de comunicação para transporte de dados de autenticação; e

VII – gerir os acessos conforme seu ciclo de vida: ativo, inativo, revogado e cancelado.

§ 2º Mediante solicitação formal, o DTI poderá conceder, em caráter excepcional e de forma temporária, Conta de Acesso com perfil especial ou de administrador para a execução de atividade pontual tecnicamente fundamentada.

§ 3º O DTI poderá manter dois sistemas de gestão de identidades independentes, um para usuários internos e outro para usuários externos.

Seção VI

Do acesso à rede cabeada, sem fio e remota

Art. 17. A utilização da rede cabeada e sem fio do CNJ é permitida por meio de dispositivos eletrônicos providos e homologados pelo DTI, após o usuário se submeter ao procedimento autenticação.

§ 1º O DTI poderá autorizar o ingresso na rede cabeada e sem fio de dispositivos eletrônicos particulares de usuários internos do CNJ.

§ 2º O DTI poderá proceder verificação técnica de segurança nos dispositivos eletrônicos que ingressarem na rede cabeada e sem fio, podendo negar o acesso aos dispositivos que representem potencial risco ao ambiente tecnológico do CNJ.

Art. 18. Somente será permitido o acesso remoto ao ambiente tecnológico do CNJ por meio de autenticação multifator, de acordo com as configurações e exigências do DTI.

§ 1º O acesso remoto ao ambiente tecnológico do CNJ deve ser provido por meio de canal criptografado seguro.

§ 2º O DTI poderá proceder verificação técnica de segurança nos dispositivos eletrônicos que ingressarem remotamente, sendo negado o acesso remoto aos dispositivos que representem potencial risco ao ambiente tecnológico do CNJ.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 19. O uso inapropriado dos recursos pelos usuários é passível de apuração de responsabilidade, nos termos da legislação aplicável, podendo o DTI suspender imediatamente o acesso concedido.

Parágrafo único. A suspensão será comunicada pelo DTI para o usuário e, quando for o caso, para o titular da unidade orgânica a qual o usuário é associado esclarecendo os detalhes da ocorrência.

Art. 20. A inobservância dos dispositivos constantes desta Portaria pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 21. As situações não previstas nesta Portaria deverão ser resolvidas pelo Comitê de Governança de Tecnologia da Informação e Comunicação.

Art. 22. Esta Portaria deverá ser revisada bianualmente ou quando necessário.

Art. 23. Ficam revogadas:

I – a Portaria Presidência nº 99, de 30 de agosto de 2016.

II – a Instrução Normativa nº 95, de 4 de maio de 2023; e

Art. 24. Esta Portaria entra em vigor 180 (cento e oitenta) dias após a sua publicação.

Ministro **Luís Roberto Barroso**

Documento assinado eletronicamente por **Luís Roberto Barroso**, **PRESIDENTE**, em 22/01/2025, às 16:44, 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 **2042112** e o código CRC **6B8EB0DB**.