INSTRUÇÃO NORMATIVA Nº 302, DE 09 DE JULHO DE 2024

Dispõe sobre o controle de acessos à informação e aos serviços de tecnologia da informação do Supremo Tribunal Federal.

***O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso das atribuições que lhe confere o art. 41, inciso X, alínea b, do Regulamento da Secretaria de 2024;*

***CONSIDERANDO** a Resolução 773, de 29 de abril de 2022, que institui a Política de Segurança da Informação do Supremo Tribunal Federal;*

***CONSIDERANDO** a Norma Complementar 7 DSIC/GSI/PR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e das Comunicações nos órgãos e entidades da Administração Pública Federal;*

***CONSIDERANDO** a Resolução 693, de 17 de julho de 2020, que regulamenta o processo judicial eletrônico no âmbito do Supremo Tribunal Federal;*

***CONSIDERANDO** a Instrução Normativa 203, de 27 de novembro de 2015, que estabelece as rotinas e os procedimentos para utilização do Sistema Eletrônico de Informações (SEI) no âmbito do Supremo Tribunal Federal;*

***CONSIDERANDO** o direito fundamental à autodeterminação informativa (art. 5º, LXXIX, da Constituição de 1988 e a entrada em vigor da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);*

***CONSIDERANDO** que a LGPD estabelece as condições sob as quais os dados pessoais podem ser tratados, define um conjunto de direitos para os titulares dos dados e impõe obrigações específicas aos controladores dos dados;*

***CONSIDERANDO** a Resolução 759/2021, que institui a Política de Privacidade e de Proteção de Dados;*

***CONSIDERANDO** que todos os usuários de serviços de tecnologia da informação são corresponsáveis pela segurança da informação e pela proteção dos dados pessoais dos titulares;*

***CONSIDERANDO** o contido no Processo Administrativo eletrônico 003386/2022;*

R E S O L V E:

Art. 1º O controle de acessos à informação e aos serviços de tecnologia da informação (TI) do Supremo Tribunal Federal (STF) fica regulamentado por esta instrução normativa.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2º Para os efeitos desta instrução normativa, aplica-se o glossário de termos de segurança da informação definido e publicado no Repositório Digital do STF (https://bibliotecadigital.stf.jus.br/xmlui/).

Art. 3º O controle de acessos se alinha às estratégias da Política de Segurança da Informação do STF (PSI/STF) e à Política de Privacidade e de Proteção de Dados, tendo como princípios norteadores:

I – a identificação única do usuário com acesso aos serviços de TI;

II – o uso exclusivo da identificação única pelo seu usuário-proprietário;

III – a concessão de acesso ao usuário apenas aos recursos mínimos necessários ao desempenho de suas atribuições laborais;

IV – a possibilidade de auditoria em todas as atividades realizadas nos serviços de TI.

Art. 4º São objetivos desta instrução normativa:

I – estabelecer as diretrizes, as responsabilidades e as competências para o controle de acessos à informação e aos serviços de TI do STF;

II – preservar os ativos de informação;

III – assegurar a confidencialidade, a integridade e a disponibilidade dos ativos de informação sob responsabilidade do STF;

IV – garantir que os acessos à informação e aos serviços de tecnologia da informação do Tribunal estejam em conformidade com a LGPD.

Art. 5º Esta instrução normativa se aplica a todos os usuários que acessam os serviços internos de TI disponibilizados pelo STF para desempenhar suas atribuições, incluindo ministros, servidores, aposentados, estagiários, empregados de empresas de serviços terceirizados e demais usuários previamente autorizados.

CAPÍTULO II

DA GESTÃO DA CREDENCIAL DE ACESSO

Seção I

Do Credenciamento

Art. 6º Cada usuário dos serviços de TI do STF receberá um identificador único, que o vinculará à sua atuação no STF.

Art. 7º São tipos de contas concedidas pela Secretaria de Tecnologia e Inovação (STI):

I – de pessoa física: pessoa natural que utiliza os serviços de TI;

II – administrativa: restrito àqueles que, pela função que desempenham na STI, necessitam de privilégios administrativos aos ativos de informação que compõem os serviços de TI;

III – de serviço: reservada aos sistemas informatizados, cuja credencial é concedida à pessoa física responsável pelo sistema ou ativo de informação.

Art. 8º O nome de usuário será estruturado a partir do padrão de nomenclatura "<primeira letra do sobrenome>+<seis dígitos aleatórios>".

§ 1° A cada conta de usuário será facultada a criação e a vinculação de um nome de e-mail.

§ 2º O nome de e-mail será estruturado a partir do padrão de nomenclatura "nome.sobrenome@stf.jus.br", sendo que o nome e o sobrenome são, respectivamente, o primeiro e o último nome.

§ 3º Excepcionalmente, com a devida justificativa, poderá ser adotado outro nome ou sobrenome, dentro do mesmo formato disposto no § 2º deste artigo.

§ 4° É vedada a utilização do e-mail institucional em cadastros de serviços não relacionados com as atividades do usuário.

Art. 9º A solicitação para criar credenciais de acesso é realizada, exclusivamente:

I – pela Secretaria de Gestão de Pessoas (SGP), no caso de ministros, juízes auxiliares, juízes instrutores, servidores do Quadro Efetivo do STF, ocupantes de cargo em comissão sem vínculo efetivo com a Administração Pública, servidores cedidos ao STF e requisitados, servidores em exercício provisório no STF e estagiários;

II – pela Secretaria de Orçamento, Finanças e Contratações (SOC), quando se tratar de empregados de empresas prestadoras de serviços terceirizados;

III – pelos fiscais de contratos e seus respectivos substitutos, no caso de empregados terceirizados que estejam em substituição ao titular;

IV – pela Secretaria de Tecnologia e Inovação (STI), no caso dos usuários constantes dos incisos II e III do art. 7º desta instrução normativa.

§ 1º O pedido de criação da credencial deve ser realizado no início das atividades no STF, ocasião em que serão informados à STI os seguintes dados:

I – nome completo;

II – provável unidade de lotação;

III – telefone de contato;

IV – data da entrada em exercício ou início das atividades;

V – tipo de vínculo;

VI – nome da empresa contratada e do gestor do contrato, no caso de empregado de empresa prestadora de serviço terceirizado.

§ 2º Criada a credencial, é de responsabilidade da STI comunicar o usuário.

§ 3º Fica vedada a criação de credenciais por mera cópia de credenciais conferidas a outro usuário, sendo necessário validação da unidade de lotação.

Art. 10. A interrupção do vínculo com o STF será informada à STI:

I – pela SGP, no caso das pessoas mencionadas no inciso I do art. 9º desta instrução normativa;

II – pelos fiscais de contrato, quando se tratar das pessoas descritas nos incisos II e III do art. 9º desta instrução normativa.

§ 1º Tão logo informada sobre a interrupção de vínculo, a STI revogará os acessos vinculados à conta e desabilitará as credenciais de acesso, mantendo os registros necessários para fins de auditoria.

§ 2º As contas desabilitadas serão mantidas pelo período indicado no art. 32 desta instrução normativa, para os registros dos logs de auditoria.

§ 3º O disposto neste artigo também se aplica, no que couber, às mudanças de lotação interna.

Seção II

Da Autenticação

Art. 11. As senhas de acesso do usuário, tokens e outros fatores de autenticação são de uso pessoal e intransferível.

Art. 12. As senhas devem ser secretas e atender aos seguintes requisitos:

I – ter o tamanho mínimo de 12 (doze) caracteres;

II – conter todos os tipos de caracteres listados a seguir:

a) letra maiúscula;

b) letra minúscula;

c) caractere especial (!, @, #, &,...);

d) número;

III – não coincidir com as 6 (seis) últimas senhas utilizadas.

Art. 13. O prazo de expiração das senhas é de 3 (três) meses.

Art. 14. A conta de usuário será bloqueada temporariamente após 5 (cinco) tentativas de acesso inválidas.

Art. 15. A STI proverá mecanismos que permitam aos usuários a atualização de sua senha de acesso.

Parágrafo único. Em casos excepcionais, quando justificada a impossibilidade de atualização da senha pelo próprio usuário, essa ação poderá ser realizada pela STI.

Art. 16. As senhas de acesso devem ser armazenadas e os seus tráfegos na rede, protegidos, utilizando-se algoritmos criptográficos reconhecidamente seguros.

Art. 17. Além da autenticação por senha, o usuário deverá fazer uso de um segundo fator de autenticação (2FA/MFA).

§ 1º Por meio de procedimento interno a STI fornecerá meios para que todas as credenciais de acesso tenham múltiplo fator de autenticação, adotando-se, além da senha, método adicional para verificação da identidade do proprietário.

§ 2º A credencial de acesso administrativa deve, obrigatoriamente, fazer uso de múltiplo fator de autenticação, além de outros mecanismos adicionais de segurança, salvo quando houver impeditivo técnico justificado.

Seção III

Da Utilização da Credencial de Acesso

Art. 18. A credencial de acesso aos serviços de TI é utilizada tão somente pelo seu proprietário.

Parágrafo único. Os proprietários das contas dos usuários administrativo e de conta de serviço são as pessoas físicas a elas vinculadas.

Art. 19. A credencial de acesso administrativa não é usada para navegação na internet, correio eletrônico ou outras atividades não vinculadas diretamente à administração do serviço de TI.

Art. 20. Não é permitida a definição de credencial de acesso genérica e de uso compartilhado, devendo cada uma ser vinculada a uma pessoa física específica ou a um único serviço.

Art. 21. As credenciais de acesso sem uso por mais de 60 (sessenta) dias são bloqueadas automaticamente.

CAPÍTULO III

DA AUTORIZAÇÃO DE ACESSO

Art. 22. O acesso às funcionalidades de sistemas e de outros serviços de TI é autorizado de modo a permitir a realização das atividades atreladas aos processos de trabalho em que o usuário atua no STF.

Art. 23. As solicitações de inclusão ou de exclusão de acesso, bem como a alteração dos níveis de acesso aos sistemas de TI, devem ser formalizadas à STI pelo gestor da unidade ou por seu substituto, ou, ainda, por pessoa designada.

Art. 24. É responsabilidade dos gestores das unidades autorizar estritamente os acessos mínimos necessários à realização do trabalho.

§ 1º A STI deverá, sempre que possível, prover meios para que os próprios gestores possam atualizar o perfil de acesso dos usuários sob sua gestão.

§ 2º Os gestores devem ser notificados pela STI sobre as solicitações de acesso a funcionalidades dos sistemas adotados em sua unidade que não tenha autorizado previamente e deliberar sobre o caso.

Art. 25. As autorizações de acesso dos usuários administrativos e de conta de serviço serão revisadas pelos gestores responsáveis em intervalos de até 6 (seis) meses.

Art. 26. A mudança de unidade de lotação enseja a revogação imediata dos acessos autorizados ao usuário, cabendo ao novo gestor definir e solicitar à STI as permissões necessárias, observado o disposto no art. 25 desta instrução normativa.

Art. 27. Manterão acesso apenas ao portal do servidor do STF para obtenção de informações financeiras e relacionadas à vida funcional:

I – os servidores efetivos do STF:

a) em licença por motivo de afastamento do cônjuge ou companheiro;

b) em licença para tratar de interesses particulares;

c) em exercício provisório em outros órgãos;

d) cedidos a outros órgãos da Administração Pública;

II – os servidores aposentados;

III – os pensionistas do STF.

CAPÍTULO IV

DA PROTEÇÃO CONTRA ACESSO NÃO AUTORIZADO

Art. 28. O usuário é responsável por zelar pelo acesso seguro aos sistemas e serviços de TI, de modo a protegê-los contra a obtenção não autorizada de informações.

Art. 29. A tela dos computadores e terminais deve ser bloqueada por senha, token ou mecanismo de autenticação similar, sempre que o usuário se afastar de sua estação de trabalho.

Art. 30. Informações com restrição de acesso não devem ser armazenadas em mídias eletrônicas que não disponham de mecanismos de controle de acesso ou mantidas impressas sobre mesas de trabalho e devem ser inutilizadas antes de seu descarte, seja em meio eletrônico ou em papel.

Art. 31. Sempre que houver suspeita de comprometimento da segurança do equipamento utilizado para realizar acesso, bem como da senha ou de outro recurso de autenticação, o usuário realizará sua imediata alteração, neste último caso, e comunicará a ocorrência à Coordenadoria de Segurança Cibernética da STI.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 32. Os serviços de TI devem registrar as ações dos usuários no ambiente computacional, de forma a permitir a recuperação de trilhas de auditoria, que serão mantidas por, no mínimo, 12 (doze) meses.

§ 1º A gestão dos registros de auditoria (logs) seguirá as diretrizes de normativo específico.

§ 2º As auditorias de acessos só poderão ser solicitadas pelos gestores das unidades, por meio de processo no SEI, diretamente à STI.

Art. 33. O controle de acesso aos sistemas em nuvem deve obedecer a este normativo, no que couber.

Art. 34. Os casos omissos serão resolvidos pelo(a) titular da Secretaria de Tecnologia e Inovação.

Art. 35. Esta instrução normativa entra em vigor na data de sua publicação.

EDUARDO S. TOLEDO

Publicado no DJE/STF em 10/7/2024.