TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

PORTARIA PRESI - 10918140

Regulamenta, no âmbito da Justiça Federal da 1ª Região, o documento acessório diferenciado "Política de Controle de Acesso Lógico".

O **PRESIDENTE DO TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO**, no uso de suas atribuições legais e regimentais e tendo em vista o constante nos autos do PAe 0000654-14.2019.4.01.8000,

CONSIDERANDO:

a) a Resolução 6, de 7 de abril de 2008, do Conselho da Justiça Federal, que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus e sobre a elaboração de uma política de controle de acesso lógico como documento acessório diferenciado;

b) a Portaria CJF-POR-2013/00279 de 19 de agosto de 2013, que define a Política de Controle de Acesso Lógico do Conselho da Justiça Federal;

c) a Norma Complementar GSI/PR 7, de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelece as diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta;

d) a Resolução Presi 600-007, de 19 de julho de 2007, que regulamenta o uso dos equipamentos e programas de informática disponibilizados na Justiça Federal de 1º e 2º graus da 1ª Região;

e) a Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização;

f) a Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação;

g) a necessidade de manter a segurança dos ativos de informação, buscando a disponibilidade, confidencialidade, autenticidade e integridade das informações custodiadas e que trafegam nos diversos meios de responsabilidade dos órgãos da Justiça Federal da 1ª Região;

h) a unicidade de sistemas de informação e a utilização de um domínio comum em toda a Justiça Federal da 1ª Região,

RESOLVE:

Seção I

Disposições preliminares

Art. 1º Regulamentar, no âmbito da Justiça Federal da 1ª Região, a Política de Controle de Acesso Lógico como documento acessório diferenciado da Política de Segurança da Informação instituída pela Resolução 6, de 7 de abril de 2008, do Conselho da Justiça Federal.

§ 1º A Política de Controle de Acesso Lógico de que trata o *caput* é de caráter obrigatório

em todos os órgãos da Justiça Federal da 1ª Região.

§ 2º As seções judiciárias poderão definir regras complementares às definidas na política estabelecida por esta Portaria, contanto que sejam mais restritivas e possuam nível maior de segurança.

Art. 2º A política estabelecida nesta Portaria define as normas relativas ao acesso lógico a ativos de informação no âmbito da Justiça Federal da 1ª Região – JF1, de modo a possibilitar o controle de acesso à rede, aos sistemas, às configurações de ativos e às informações produzidas e armazenadas nos órgãos da JF1, de caráter público ou privativo.

Parágrafo único. Deverão ser observadas, além das regras gerais estabelecidas nesta Portaria, normas complementares que vierem a ser editadas nos termos do art. 19 desta Portaria, conforme previsto no item 9.3.1 do Anexo I da Resolução CJF 6/2008.

Art. 3º Esta norma se aplica a todos os usuários e agentes públicos que tenham qualquer tipo de contato com informações produzidas ou custodiadas pela Justiça Federal da 1ª Região, bem como a seus sistemas informatizados e ativos de informação.

Seção II

Das definições

Art. 4º Para os efeitos desta Portaria, considera-se:

I – ataque de força bruta: ataque em que se tenta obter a senha de um usuário utilizando combinações aleatórias ou listas de senhas frequentemente utilizadas;

II – ativo: aquilo que tem valor, tangível ou intangível, para a JF1;

III – ativo de informação: qualquer componente, tangível ou intangível (humano, tecnológico, geográfico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio;

IV – credencial: chave lógica que consiste em um par único, pessoal e intransferível, de nome de usuário e senha utilizado para realizar acesso lógico a ativos;

V – credenciamento: processo de validação das informações cadastrais da credencial com documentos oficiais;

VI – critérios de complexidade: definição de um padrão mínimo de quantidade de caracteres e conjunto de símbolos que formarão a senha da credencial dos usuários;

VII – perfil de acesso: conjunto de permissões comuns e necessárias ao desempenho de determinado perfil de atividade, a exemplo de desenvolvedor de *software*, secretária, manutenção;

VIII – princípio de privilégio mínimo: obrigatoriedade de se atribuir ao usuário o conjunto mais restritivo possível de permissões suficiente para realização de suas tarefas;

IX – registro de acesso: conjunto de informações de auditoria que contenha informação suficiente para identificar univocamente um acesso lógico, também referenciado como "*log* de acesso";

X – sistema de gerenciamento de identidades: conjunto de ferramentas e processos que suportam as atividades de credenciamento, descredenciamento, autenticação e controle da titularidade e privilégios dos usuários de determinada organização.

Seção III

Da gestão das credenciais

Art. 5º As unidades de tecnologia da informação de cada órgão da JF1 são responsáveis pela implantação e manutenção de um sistema de gerenciamento de identidades nos seus órgãos.

Art. 6º A gestão das credenciais deve preferencialmente estabelecer um modelo de autenticação centralizado, no qual os diversos sistemas utilizam um mesmo ponto de autenticação para autenticar acessos e permissões.

Parágrafo único. Na impossibilidade de se utilizar um modelo de autenticação centralizado, por limitações tecnológicas, deve-se tomar providências para que os níveis de segurança e privilégios de acesso das contas de uma mesma pessoa sejam compatíveis com as determinações contidas nesta Portaria.

Art. 7º Os titulares das contas são responsáveis, em todas as esferas, pelo uso e manutenção de suas credenciais, cabendo-lhes observar as boas práticas de segurança da informação, descritas em termo de responsabilidade, que deverá ser por eles assinado.

Parágrafo único. Toda credencial fornecida aos usuários é pessoal e intransferível.

Art. 8º O acesso a recursos e sistemas só deve ser concedido a usuários previamente credenciados e autorizados.

Art. 9º Todo o tipo de concessão de acesso deve seguir o princípio de privilégio mínimo.

Art. 10. Os ativos de informação, quando tecnicamente possível, devem manter registros de acesso.

Art. 11. As senhas utilizadas em todas as credenciais devem possuir critérios de complexidade para evitar ataques de força bruta.

Parágrafo único. Os critérios de complexidade mínimos devem ser definidos pela área de tecnologia da informação do Tribunal e atualizados conforme seja necessário.

Art. 12. O acesso a conteúdos inseguros ou maliciosos deve ser bloqueado pela área de tecnologia da informação, quando conhecidos e tecnicamente possível, devendo a área informar posteriormente o motivo do bloqueio ao usuário afetado.

Art. 13. O Tribunal e as seções judiciárias devem designar formalmente uma área responsável pelas atividades de credenciamento de magistrados, servidores, prestadores de serviço, visitantes ou qualquer outra pessoa que necessite de acesso lógico aos ativos de informação da JF1.

Seção IV

Das responsabilidades

Art. 14. A área responsável pela atividade de credenciamento tem por responsabilidades:

I – verificar os dados informados para cadastro e credenciamento, que devem ser validados com documentos oficiais;

II – providenciar a criação de credenciais de acesso para os usuários;

III – adequar o perfil inicial de acesso do usuário, levando em consideração o princípio do privilégio mínimo;

IV – providenciar a atualização dos dados quando necessário, mantendo a mesma validação necessária ao credenciamento;

V – revogar o acesso ao fim do vínculo dos usuários.

Art. 15. A definição dos critérios de bloqueio a conteúdos maliciosos é de responsabilidade da área de segurança da informação dos órgãos da JF1, podendo se basear em definições utilizadas por ferramentas de mercado.

Seção V

Disposições gerais

Art. 16. A política estabelecida por esta Portaria deve ser atualizada sempre que necessário, de modo a refletir as necessidades da JF1 e a evolução tecnológica dos ativos de informação.

Art. 17. As atualizações desta Portaria poderão ocorrer no todo ou em partes, tendo em vista a modularidade da política por ela estabelecida.

Art. 18. As seções judiciárias da JF1 deverão, no prazo de 60 (sessenta) dias, a contar da publicação desta Portaria, indicar ao Tribunal cronograma com atividades que serão realizadas para

adequação a esta norma.

Art. 19. A política de que trata esta Portaria será detalhada em normas complementares, que deverão ser elaboradas e publicadas pela Secretaria de Tecnologia da Informação, após aprovação pelo Comitê Gestor de Tecnologia da Informação do Tribunal Regional Federal da 1ª Região – COGETI-TRF1.

Art. 20. Esta Portaria entra em vigor na data de sua publicação.

Desembargador Federal **I'TALO FIORAVANTI SABO MENDES**

Presidente

ANEXO I

NORMA DE CONTROLE DE ACESSO À REDE LOCAL E SISTEMAS INTERNOS

1 Descrição

Esta norma integra a Política de Controle de Acesso Lógico da Justiça Federal da 1ª Região e estabelece os procedimentos de concessão de acesso à rede dos órgãos que a compõem. Suas diretrizes devem ser observadas em todas as atividades que envolvam a concessão de acesso à rede da JF1 ou a criação de novas credenciais para colaboradores.

2 Finalidade

Definir as regras a serem seguidas no âmbito da JF1 relativas à criação de credenciais para acesso à rede local e sistemas internos.

3 Abrangência

Aplica-se a todo tipo de criação de credencial e concessão de acesso lógico à rede local e sistemas internos da JF1.

4 Público alvo

Agentes públicos que necessitem de acesso à rede local ou aos sistemas internos da JF1 para a execução de suas tarefas institucionais.

5 Credenciamento e descredenciamento

5.1 A atividade de credenciamento deve incluir a validação das informações cadastrais com documentos de identificação válidos no território brasileiro e ser anterior à criação de contas de acesso.

5.1.1 Caso seja necessário alterar informações que tenham sido validadas com documentos oficiais, essas novas informações devem passar pelo processo de conferência documental novamente.

5.1.2 Deve-se definir um processo específico para alteração de dados de contato, como telefone e informações identificadoras que sejam utilizadas para acesso às contas, como CPF e *e-mails*, a fim de sempre validar a identidade do solicitante.

5.2 O acesso dos usuários à rede local e aos sistemas internos da JF1 se dará por meio de uma credencial pessoal e intransferível, devendo cada usuário possuir uma única credencial.

5.2.1 Regras de negócio que determinem a utilização de mais de uma credencial por usuário devem ser apreciadas pelo gestor do sistema afetado quanto à sua adequação à segurança da informação.

5.3 A criação de uma credencial única para uma equipe ou grupo deve ser evitada e, caso seja comprovadamente necessária, deve-se garantir que existam meios de identificação do agente público que

esteja fazendo uso da credencial.

5.4 A criação ou exclusão de novas contas deve ocorrer da seguinte maneira:

a) o setor formalmente responsável deve proceder, após devido credenciamento e conferência documental, à criação de contas para os usuários quando necessitarem de acesso à rede local ou sistemas internos;

b) os órgãos poderão definir setores de credenciamento distintos para públicos distintos, como magistrados, servidores, estagiários, visitantes ou prestadores de serviço;

c) as contas devem obrigatoriamente obedecer aos critérios de privilégio mínimo, devendo qualquer privilégio adicional ser formalmente solicitado pela autoridade ou chefia competente;

d) o setor formalmente responsável pelo credenciamento deve proceder ao descredenciamento ou exclusão das credenciais quando as regras de negócio o determinarem.

5.5 As contas de magistrados e servidores devem possuir prazo de validade indeterminado, sendo encerradas no momento da perda de seu vínculo com o órgão.

5.6 As contas de usuários eventuais, como visitantes ou prestadores de serviços, devem possuir prazo de validade definido no ato de sua criação, compatível com a sua necessidade, sendo encerrada imediatamente após o vencimento do mencionado prazo.

5.7 A área responsável pelo credenciamento deve suspender imediatamente as contas de usuários que perderem vínculo com a JF1.

5.8 A área responsável pelo credenciamento deve ajustar as permissões das contas de acordo com as movimentações internas dos servidores no organograma do órgão, devendo retirar os privilégios da lotação anterior.

5.9 Contas que infrinjam qualquer norma ou política de segurança serão suspensas até averiguação do fato pelas autoridades responsáveis.

5.10 A suspensão de contas e o motivo de tal procedimento devem ser imediatamente reportados ao titular e ao responsável por sua unidade de lotação.

6 Contas de acesso

6.1 O modelo de controle de acesso deve preferencialmente ser do tipo centralizado.

6.2 A área de tecnologia da informação do Tribunal deve definir uma nomenclatura padronizada para a as contas dos usuários.

7 Concessão de privilégios de acesso

7.1 Os seguintes tipos de acesso podem ser alvo de restrição:

a) acesso a diretórios na rede;

b) acesso a sistemas internos e externos;

c) acessos a configurações de ativos;

d) acessos a conteúdos de internet;

e) demais configurações em que seja possível segregar o tipo de usuário do sistema ou ativo.

7.2 As contas devem ser inicialmente criadas com um conjunto de privilégios de acesso mínimo.

7.3 O titular da unidade de lotação do magistrado, servidor, prestador de serviços ou estagiário deverá justificar e solicitar formalmente os privilégios adequados às atribuições do agente público, respeitando uma política de privilégios mínimos.

ANEXO II

NORMA DE CRITÉRIOS DE COMPLEXIDADE DE SENHAS

1 Descrição

Esta norma é parte da Política de Controle de Acesso Lógico da Justiça Federal da 1ª Região e estabelece os critérios de complexidade na formação das senhas que são utilizadas nas credenciais da JF1. Suas diretrizes devem ser observadas em todo tipo de criação ou alteração de senha de acesso.

2 Finalidade

Definir as regras a serem seguidas no âmbito da JF1 relativas aos critérios mínimos de complexidade de senhas de acesso.

3 Abrangência

Aplica-se a todo tipo de criação ou alteração de senhas de acesso lógico de usuários da rede local e sistemas internos da JF1.

4 Público alvo

Agentes públicos que necessitem de acesso à rede local ou aos sistemas internos da JF1 para a execução de suas tarefas institucionais.

5 Disposições gerais

5.1 As senhas utilizadas pelos usuários da rede e sistemas internos da JF1 terão sua formação baseada nos seguintes critérios:

a) histórico de senhas: controle sobre quando o usuário pode utilizar uma senha já utilizada no passado;

b) comprimento de senhas: quantidade mínima de caracteres que uma senha deve ter;

c) tempo de vida máximo da senha: período de tempo máximo em que uma senha pode ser utilizada até que o sistema solicite sua troca automaticamente;

d) tempo de vida mínimo da senha: período de tempo mínimo para que uma senha seja trocada novamente;

e) restrições de conteúdo: impossibilidade de que a senha tenha, em seu conteúdo, informações de fácil obtenção como o nome do próprio usuário;

f) utilização abrangente de caracteres: obrigação de que a senha contenha, em sua formação, caracteres de tipos distintos como letras maiúsculas, minúsculas, numerais e/ou símbolos especiais.

5.2 As senhas utilizadas na JF1 devem ter os seguintes critérios mínimos em sua formação:

a) histórico de senhas: não repetição das últimas 3 senhas;

b) comprimento de senhas: mínimo de 8 caracteres;

c) tempo de vida máximo da senha: 6 meses;

d) tempo de vida mínimo da senha: 1 dia;

e) restrições de conteúdo: ativadas, caso disponível no sistema utilizado;

f) utilização abrangente de caracteres: ativada, caso disponível no sistema utilizado.

5.3 A impossibilidade técnica de definição de critério mínimo de senha deve ser reportada à área de TI do órgão, que deve implementar medidas para a adequação do respectivo sistema a esse requisito de segurança.

1ª Região, em 21/08/2020, às 17:45 (horário de Brasília), conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://portal.trf1.jus.br/portaltrf1/servicos/verifica-processo.htm informando o código verificador **10918140** e o código CRC **1A45F854**.