POLÍTICA DE CONTROLE DE ACESSO LÓGICO

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CÓDIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

Política de Controle de Acesso Lógico

1. Apresentação

Esta política norteará a implementação de medidas para o controle de acesso lógico aos ativos de informação, tanto internos quanto externos, do Tribunal Regional Federal da 5ª Região (TRF5).

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio do Tribunal, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.3.1 – Política de Controle de Acesso Lógico – do Anexo I da Resolução Nº 6, de 7 de abril de 2008, do Conselho da Justiça Federal, que definiu a Política de Segurança da Informação no âmbito do Conselho e da Justiça Federal de Primeiro e Segundo graus.

2. Escopo

O escopo desta Política de Segurança da Informação abrange o Tribunal Regional Federal da 5ª Região.

3. Público Alvo

Esta Política de Controle de Acesso Lógico se aplica aos agentes públicos do Tribunal Regional Federal da 5ª Região e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas com a administração.

4. Termos e Definições

Confidencialidade – Sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-la.

Criptografia – Arte e ciência de esconder o significado de uma informação de receptores não desejados.

Disponibilidade – Uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

Download - É a transferência de dados de um computador remoto para um computador local.

Fator de Autenticação – Informação que um cliente/usuário sabe (ex: *senha*), tem (ex.: *smartcard*) ou é (ex: impressão digital), necessária para completar sua autenticação em um sistema.

Integridade – A preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original.

Log – Registro de dados que armazena informações de auditoria.

OTP – *One Time Password*. É uma senha que perde a validade após um processo de autenticação. Geralmente uma nova senha é gerada de forma aleatória e em intervalos de tempo regulares.

Privilégio Mínimo – conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

Recursos de TI – Recursos de Tecnologia da Informação. Softwares e hardwares que geram, processam, recebem ou transmitem informações, como desktops, notebooks, sistemas operacionais, processadores de texto, *smartphone*, *pendrive* etc.

Redes Ponto-a-Ponto – Redes caracterizadas por dispositivos (nós) que têm a capacidade de atuar simultaneamente como servidor e receptor de dados.

Smartcard - é um cartão que geralmente assemelha-se em forma e tamanho a um cartão de crédito convencional. Muito utilizado para armazenar informações relativas a certificados digitais.

Smartphone – Telefone móvel dotado de grande capacidade computacional, cumprindo funções de telefone celular, agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e redes de computação.

SSH – *Secure Shell*. É simultaneamente um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede, de forma a executar comandos de uma unidade remota.

SSID – *Service Set Identifier*. É um nome que identifica uma rede sem fio em particular.

Upload - É a transferência de dados de um computador local para um computador remoto.

VPN – *Virtual Private Network*. É uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, implementada em cima de uma rede de comunicações pública (como, por exemplo, a Internet).

5. Identificação dos usuários

5.1 A inclusão e a exclusão de agentes públicos, estagiários, aprendizes, funcionários de empresas contratadas e de outros órgãos conveniados, doravante denominados de forma geral como usuários, nos recursos de rede e sistemas, inclusive correio eletrônico, do TRF5 deve ser realizada pela Subsecretaria de Informática (SI), por solicitação formal da autoridade competente.

5.1.1 Em relação aos funcionários de empresas contratadas e de outros órgãos conveniados, a autorização será solicitada pelo servidor responsável direto pela elaboração de parcerias e pela Diretoria Geral (DG), no caso de clientes.

5.1.2 Os casos omissos serão tratados pela diretoria da SI, juntamente com a DG.

5.2 O acesso aos recursos de tecnologia da informação somente deve ser permitido aos usuários previamente autorizados, mediante identificação.

5.3 As autorizações devem ser definidas de acordo com a necessidade de condução das tarefas institucionais e considerando o princípio de privilégio mínimo.

5.4 Nenhum usuário que não pertença ao corpo técnico da SI deverá possuir privilégio de administrador de computadores/sistemas, inclusive de dispositivos móveis, como notebooks. As exceções ocorrerão apenas caso a SI não consiga alternativas que permitam o desenvolvimento das atividades do usuário. Nestes casos, caberá à DG, diante de parecer técnico emitido pela SI, a autorização, após a devida solicitação, justificada, da autoridade competente.

5.5 Os usuários da SI deverão possuir privilégio de administrador de computadores/sistemas apenas se necessário para o cumprimento de suas atividades, obedecido o princípio de privilégio mínimo.

5.6 Sempre que possível, o controle de acesso aos recursos de tecnologia da informação deverá possuir, pelo menos, dois fatores de autenticação.

5.7 As credenciais de identificação, como dispositivos *OTP*, login/senhas e *smartcards,* são únicas, pessoais e intransferíveis, não devendo ser compartilhadas, sendo sua utilização ou as conseqüências decorrentes do seu uso indevido de responsabilidade do usuário. Nenhum usuário deve identificar-se como outro usuário.

5.8 As alteração de credenciais do usuário, como logins e senhas de acesso a sistemas e à rede local, quando não disponíveis nos próprios sistemas, deverão ser feitas de forma presencial pelo usuário, com a apresentação de documento oficial com foto deste ou memorando da autoridade competente, junto ao setor responsável da SI.

5.9 Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer da SI acerca da possibilidade de aceitação dos riscos associados.

5.10 As senhas de sistemas do usuário devem ser escolhidas seguindo orientações contidas no sistema de controle de acesso a ser definido pela SI. Tal sistema deverá possuir mecanismos para impedir a geração de senhas fracas ou óbvias, conter definições sobre conjunto de caracteres permitidos, tamanho, tempo de vida, forma de troca e restrições específicas para as senhas, garantir a segurança da distribuição de senhas (inicial ou não), bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal-sucedidas, dentre outros.

5.11 Fica assegurado à Comissão Local de Resposta a Incidentes, a qualquer tempo, decidir pela suspensão temporária do acesso do usuário ao recurso computacional do TRF5, quando evidenciados os riscos à segurança da informação.

5.12 É proibida a utilização de senhas sem nenhum processo criptográfico aplicado, excetuando-se os casos em que não houver alternativa.

5.13 O juiz convocado para substituir Desembargador neste Tribunal terá direito, assim como seus assessores, a uma conta de acesso à rede e a uma caixa postal de e-mail para a utilização, que serão desativadas findado o período de convocação.

5.13.1 Os gabinetes deverão encaminhar à SI a informação sobre o período de convocação referido no item anterior, para que a mesma efetue os procedimentos necessários.

6. Processo de desligamento ou movimentação de usuário

6.1 Será proibido o acesso de ex-servidores, ex-desembargadores, ex-estagiários e ex-contratados aos sistemas de informação do TRF5.

6.2 Será restrito o acesso de desembargadores federais aposentados, bem como de servidores aposentados, cedidos ou que mantenham vínculo efetivo com esta corte aos sistemas de informação do TRF5.

6.3 As credenciais, identificações, crachás, equipamentos, mecanismos e acessos lógicos devem ser revogados e/ou inutilizados quando do desligamento do usuário.

6.4 A Subsecretaria de Pessoal será responsável pelo envio imediato à SI da informação de desligamento, aposentadoria ou movimentação de desembargadores, funcionários, estagiários e aprendizes integrantes do TRF5, para o procedimento dos devidos ajustes das credenciais de acesso, em face dos itens 5.1 e 5.2.

7. Acesso à rede local

7.1 É vedada a utilização de microcomputadores ou dispositivos eletrônicos particulares, portáteis ou não, na rede do TRF5, exceto em casos de comprovada necessidade, mediante solicitação por escrito do dirigente responsável pela unidade à DG, justificando a necessidade e o prazo de utilização. Caberá à DG a autorização, diante de parecer técnico emitido pela SI. Nestes casos, deverão ser obrigatoriamente adotados os padrões de configuração, softwares e segurança compatíveis com o disposto nesta política, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, além da manutenção e suporte aos sistemas não homologados pela SI.

7.2 É vedada a conexão de equipamentos conectados à rede corporativa do TRF5 a outros sítios através da utilização de linha discada, rede sem fio ou quaisquer outros meios, exceto os autorizados pela DG, diante de parecer técnico emitido pela SI.

8. Acesso remoto ao TRF5

8.1 O item 7 desta política se aplica às conexões de acesso remoto ao TRF5 utilizadas para serviço.

8.2 As implementações de acesso remoto que são cobertas incluem DSL, VPN e SSH, mas a estas não se limitam.

8.3 É proibido o acesso remoto à rede corporativa do TRF5 por meios que não implementem criptografia do tráfego durante o acesso.

8.4 O acesso remoto à rede corporativa do TRF5 deverá se precedido de solicitação formal à DG, pela autoridade competente, explicitando os motivos de tais necessidades, o período de utilização e os serviços que necessita utilizar na rede corporativa. A DG poderá proceder com a autorização, diante de parecer técnico prévio emitido pela SI.

8.4.1 As conexões de acesso remoto deverão ser precedidas da assinatura do Acordo de Requisitos a Acesso Remoto, documento a ser mantido e atualizado pela SI.

8.5 O usuário com privilégio de acesso remoto é responsável por impedir que qualquer pessoa com acesso, físico ou lógico, ao dispositivo que está efetuando o acesso viole política do TRF5, execute atividades ilegais e/ou utilize o acesso para desenvolver atividades pessoais. O usuário detém a responsabilidade pelas conseqüências do mau uso do acesso remoto.

8.6 A segurança do acesso remoto deve ser estritamente controlada. O controle deverá ser feito através de autenticação forte, de preferência com utilização de autenticação de no mínimo dois fatores e de regras de filtragem que reforcem o princípio do privilégio mínimo.

8.7 As credenciais de acesso remoto são pessoais e intransferíveis, sendo o usuário responsável pela segurança das informações.

8.8 Estações de trabalho ou dispositivos móveis que serão utilizados para o acesso remoto deverão, de preferência, ser disponibilizados pela SI ou ter suas configurações aprovadas - por tal Subsecretaria.

8.9 Todos os dispositivos conectados remotamente à rede corporativa do TRF5 devem, obrigatoriamente, utilizar, no mínimo, software antivírus atualizado até a última definição do fabricante do mesmo.

8.10 As informações de controle dos acessos remotos (*logs*) deverão ser registradas e auditadas periodicamente pela SI, para apuração de eventuais violações de segurança e contabilização do uso de recursos.

9. Utilização de sistema de mensageria corporativa

9.1 O sistema de correio eletrônico do TRF5 não deve ser utilizado para a criação ou distribuição de quaisquer mensagens que não sejam compatíveis com as atribuições dos usuários, incluindo as que contêm ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade, mas a estas não se limitando.

9.2 Todos os e-mails armazenados, transmitidos ou recebidos pelo sistema de correio eletrônico do TRF5 são passíveis de auditoria, podendo ser rastreados por softwares específicos para a verificação e adequação às normas estabelecidas em toda a Política de Segurança da Informação do Conselho e da Justiça Federal e na legislação brasileira.

9.3 O envio de mensagens a todos os componentes da lista de endereços do Tribunal se restringe a assuntos de interesse geral dos servidores e magistrados e é de responsabilidade da Divisão de Comunicação Social e Cerimonial.

9.4 É proibido o envio de *spam* ou mensagens que contenham qualquer tipo de software malicioso por parte dos usuários do sistema de correio eletrônico do TRF5.

9.5 O TRF5 proverá mecanismos para a identificação de mensagens que possuam conteúdo infectado por softwares maliciosos ou que ofereçam risco à segurança da informação. Tais mensagens, quando detectadas, poderão ser excluídas automaticamente ou armazenadas em quarentena.

9.6 Cabe à DG, diante de parecer técnico emitido pela SI, estipular as regras de utilização do correio eletrônico que se façam necessárias para o bom funcionamento do serviço e para a segurança das informações, aí incluídas as de quantidade de destinatários, tamanho máximo das caixas postais, mensagens enviadas e recebidas e tipos permitidos de arquivos anexados às mensagens.

10. Utilização de sistema de mensageria instantânea

10.1 O TRF5 poderá prover sistemas de mensageria instantânea para a comunicação entre os usuários internos e outros órgãos.

10.2 A SI definirá o cliente e o protocolo de mensageria instantânea homologado para utilização pelo TRF5.

10.3 A utilização ou conexão com sistemas de mensageria instantânea de uso público, como MSN Messenger, Yahoo!, Messenger, dentre outros, deverá ser

precedida de solicitação formal da autoridade competente, explicitando a necessidade de utilização de tais serviços, e da conseqüente autorização da DG.

10.4 O sistema de mensageria instantânea do TRF5 não deve ser utilizado para a criação ou distribuição de quaisquer mensagens e/ou arquivos que não sejam compatíveis com as atribuições dos usuários, como os que contêm ofensas e comentários sobre raça, idade, deficiência, orientação sexual, pornografia, crença e religião, política ou nacionalidade.

11. Acesso à Internet

11.1 O acesso aos serviços disponibilizados na Internet será provido pelo TRF5 aos usuários para o cumprimento de suas atribuições e obedecendo ao princípio de privilégio mínimo.

11.2 O acesso a serviços que não sejam comuns a todos os usuários, como, por exemplo, acesso a sítios, deverá ser precedido de solicitação formal, com a devida justificativa, e da respectiva autorização da Diretoria Geral, diante de parecer técnico emitido pela SI.

11.3 É proibido o acesso a sítios de conteúdos diversos dos compatíveis com as atribuições do usuário, incluindo aqueles que tratem de propaganda comercial ou política, sexo, pornografia, pedofilia, erotismo e assuntos correlatos, técnicas e ferramentas para invasão e evasão de sistemas, racismo, compartilhamento de arquivos, bem como de qualquer conteúdo de natureza duvidosa ou ofensiva ou que possa prejudicar o acesso legítimo a sítios utilizados para a devida prestação jurisdicional.

11.4 A SI utilizará softwares específicos que efetuarão o registro de todos os acessos aos serviços providos na Internet, assim como o bloqueio aos sítios especificados no item 11.3.

11.5 Em caso da necessidade de liberação de algum sítio, deverá ser enviada solicitação formal à SI, justificando a necessidade do desbloqueio**.**

12. Conexão e Acesso a Extranets

12.1 Conexões entre o TRF5 e terceiros que necessitam de acesso a recursos não públicos, independente da tecnologia de circuito de telecomunicação ou de VPN, devem seguir as seguintes exigências:

12.1.1 Toda nova conexão a ser estabelecida como extranet deve ser analisada previamente sob a perspectiva de segurança da informação pela SI. A análise deverá garantir que todos os acessos estão de acordo com as necessidades do serviço da melhor maneira possível e que o princípio do privilégio mínimo está sendo seguido.

12.1.2 Toda nova requisição de conexão entre terceiros e o TRF5 necessita que seus representantes concordem e assinem o Acordo de Conexão de Extranet, documento mantido e atualizado pela SI. Todo o processo de estabelecimento da extranet deverá ser documentado e armazenado pela SI.

12.1.3 O requisitante deverá designar um representante para servir de Ponto de Contato (PC) para a conexão de extranet. No caso de mudança de PC, o requisitante deverá informar essa mudança imediatamente ao TRF5.

12.1.4 Todas as mudanças no Acordo de Conexão de Extranet deverão ser justificadas e serão objeto de uma revisão de análise de segurança.

12.1.5 Todos os usuários do TRF5 que necessitem acessar serviços providos por extranets deverão ser identificados e autorizados pela autoridade competente.

12.1.6 Os Acordos de Conexão de Extranet deverão, sempre que possível, possuir prazo de término definido.

12.1.7 A SI deverá, periodicamente, conduzir auditorias em todas as conexões de extranet, para garantir que elas ainda são necessárias e que o acesso provido atinge as necessidades da conexão. Eventuais modificações para atender aos requisitos de negócio e/ou segurança da informação do TRF5 deverão ser comunicadas ao PC, para que o requisitante as providencie.

13. Acesso à rede sem fio

13.1 As exigências que se seguem atingem todos os dispositivos de comunicação de dados sem fio (como, por exemplo, notebooks, smartphones e microcomputadores) conectados à rede corporativa do TRF5. Dispositivos de comunicação de dados sem fio que não estão conectados à rede corporativa do TRF5 não são atingidos.

13.1.1 Todos os pontos de acesso sem fio conectados à rede corporativa do TRF5 deverão ser registrados e aprovados pela SI. Esses pontos de acesso serão objeto de periódicos testes de penetração e auditoria. Todas as

interfaces de rede sem fio utilizadas nos microcomputadores e notebooks do TRF5 deverão ser registradas na SI.

13.1.2 É proibido o acesso de dispositivos particulares de comunicação de dados sem fio à rede corporativa do TRF5, excetuando-se os casos devidamente justificados e autorizados formalmente pela Diretoria Geral, após parecer técnico emitido pela SI.

13.1.2.1 A autorização deverá estabelecer o período de utilização, que, findado, ensejará o bloqueio do acesso pela SI.

13.1.2.2 Os dispositivos particulares, mesmo autorizados, só deverão obter o acesso se possuírem todas as configurações de segurança exigidas dos equipamentos do próprio TRF5, as quais são definidas pela SI. A SI deverá proceder a vistoria nos dispositivos para garantir que os mesmos cumprem todas as exigências e estão livres de ameaças e softwares que possam comprometer a segurança das informações do TRF5.

13.1.3 Todas as conexões à rede sem fio deverão ser aprovadas em relação aos requisitos de segurança e deverão atender ao princípio do privilégio mínimo.

13.1.4 Todos os dispositivos conectados à rede corporativa do TRF5 através de conexão sem fio devem utilizar as configurações de criptografia estabelecidas pela SI para eliminar o tráfego de dados não criptografado.

13.1.5 Toda tecnologia de acesso sem fio implementada no TRF5 deverá suportar autenticação forte, com possibilidade de efetuar checagens em bancos de dados externos, como RADIUS ou similar. Deverá ser dada preferência a tecnologias que possibilitem autenticação de, pelo menos, dois fatores.

13.1.6 Toda identificação de rede sem fio ou SSID deverá ser configurada de maneira a não conter qualquer informação que identifique o TRF5 ou o produto utilizado.

14. Transferência de arquivos

14.1 A transferência de arquivos deve ocorrer somente quando utilizada para o cumprimento das atividades de interesse do TRF5, sendo regulada pela SI, que poderá proibir o *download* ou *upload* de arquivos que representem risco potencial.

14.2 No caso de *download* de interesse comum a várias áreas, o mesmo deve ser feito pela SI e disponibilizado aos usuários.

14.3 Os arquivos advindos de *download* podem sofrer varredura da ferramenta antivírus disponibilizada para o usuário.

14.4 É proibida a utilização de programas de compartilhamento e transferência de arquivos que utilizem redes Ponto-a-Ponto (P2P), incluindo Emule, Kazaa e Bittorrente.

15. Periodicidade de Revisão

15.1 Esta política deverá ser revista anualmente pelo Comitê Local de Segurança da Informação, com vistas a adequar a mesma às necessidades atuais.

15.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.