Justiça Federal 61 Tribunal Regional Federal - 2ª Região

ANEXO Nº TRF2-ANE-2014/00076

Anexo ao documento

Data de revisão:	Revisão nº
Data de criação: 25/09/2014	DAR-TRF2-PolíticaControleAcessoLógico-1.00-2014

Política de Controle de Acesso Lógico

1. Apresentação

Este documento acessório à Política de Segurança da Informação da Justiça Federal trata da Política de Controle de Acesso Lógico.

2. Escopo

Esta Política, bem como os eventuais respectivos documentos anexos, têm abrangência regional, ou seja, se aplicam no âmbito do Tribunal Regional Federal da 2ª Região e das Seções Judiciárias da Justiça Federal da 2ª Região.

3. Público-alvo

Esta Política, bem como os eventuais respectivos documentos anexos, se aplicam a todas as pessoas naturais e jurídicas na qualidade de agentes públicos em sentido amplo (ou seja, em sentido estrito ou equiparados), que exercem ou exerceram atividades na Justiça Federal da 2ª Região ou para ela, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, seja em cargo, emprego, função, mandato ou com mero múnus ou atribuição pública ou de interesse público, encontrando-se na atividade ou inatividade, o que inclui, dentre outras similares:

- servidores;

- empregados;

- magistrados;

- estagiários e aprendizes;

- partes em quaisquer contratos, convênios, acordos, ajustes, termos de parceria e outros instrumentos congêneres, bem como seus eventuais agentes (tais como empregados, prepostos, estagiários e aprendizes de "terceirizados");

- pensionistas de servidores e magistrados.

Esta Política, bem como os eventuais respectivos documentos anexos, também se aplicam a todos aqueles que, mesmo exercendo ou tendo exercido atividades na Justiça Federal da 2ª Região ou para ela sem qualquer forma de investidura ou vínculo, também possam eventualmente ter acesso lógico, o que inclui, dentre outros similares:

- advogados (inclusive estagiários) e outras espécies de mandatários, bem como seus clientes;

- membros de outras instituições públicas (tais como OAB, AGU, DPU, MPF, DPF, CJF, CNJ, TCU, CEF e BB);

- visitantes.

4. Conceituação

Para os efeitos desta Política, considera-se acesso lógico toda forma de ingresso (*sign-in, login* ou *logon*), circulação, permanência ou saída (*sign-out, logoff* ou *logout*) de computadores, aplicativos, sistemas, *sites* e *e-mails*,

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 62 Tribunal Regional Federal - 2ª Região

presentes em redes internas (Intranet), virtualmente internas (seja *VNC - virtual network computing* ou *VPN - virtual private network*) ou externas (Internet), conectadas com ou sem fio (via onda infravermelha, *Wi-Fi*, *Bluetooth*, outras espécies de ondas de rádio, *3G*, *4G* etc.), e com ou sem o intermédio de ferramenta eletrônica de comunicação de dados de qualquer espécie, que integre a qualquer título o patrimônio da Justiça Federal da 2ª Região como ativo tecnológico informático, tangível ou intangível, ou que, mesmo não o integrando, seja utilizado nela ou para ela.

5. Objetivos

Os objetivos desta Política são, essencialmente, assegurar os simultâneos acesso e proteção da informação com seus principais requisitos de segurança (ou seja, confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade), levando em consideração as vulnerabilidades exploráveis por ameaças e agressões com risco de impacto negativo, e tendo ênfase no aspecto da segurança lógica, descrita no item 8.1 do Anexo I da Resolução nº 6, de 7 de abril de 2008, do CJF.

Esta Política é complementada pelos demais documentos acessórios à Política de Segurança da Informação da Justiça Federal, com ênfase em outros aspectos.

6. Documentos de referência

Os documentos de referência desta Política são, principalmente, os seguintes:

- art. 13 da Resolução nº 90, de 29 de setembro de 2009, do CNJ;

- Anexo da Resolução nº 103, de 23 de abril de 2010, do CJF;

- art. 1º, § ún., da Resolução nº 176, de 10 de junho de 2013, do CNJ;

- Anexo da Resolução nº 91, de 29 de setembro de 2009, do CNJ;

- Anexos da Resolução Conjunta nº 4, de 28 de setembro de 2005, do CJF;

- "Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário" elaboradas pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário;

- "Boas Práticas em Segurança da Informação" elaboradas pelo TCU;

- publicações do DSIC - Departamento de Segurança da Informação e Comunicações do GSI - Gabinete de Segurança Institucional da Presidência da República;

- Resolução nº 22, de 30 de maio de 2011, do Tribunal;

- Anexo da Portaria nº 124, de 10 de abril de 2013, do CJF.

Além desses, os documentos de referência desta Política são, especialmente, os seguintes:

- art. 2º, c/c os itens 4.2 e 9.3.1 do Anexo I, da Resolução nº 6, de 7 de abril de 2008, do CJF;

- Lei nº 12.965, de 23 de abril de 2014;

- Decreto nº 8.135, de 4 de novembro de 2013;

- Resolução Conjunta nº 3, de 16 de abril de 2013, do CNJ;

- Orientação nº 3, de 5 de março de 2007, da Corregedoria Nacional de Justiça;

- Resolução nº 2, de 23 de janeiro de 2013, do Tribunal;

- Resolução nº 13, de 30 de junho de 2014, do Tribunal;

- art. 195, § 1º, da Consolidação de Normas da Corregedoria-Regional;

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 63 Tribunal Regional Federal - 2ª Região

- Consolidação de Normas da Diretoria do Foro da SJ/RJ;

- Norma Interna nº 7-01, de 13 de setembro de 2007, da Diretoria do Foro da SJ/ES;

- publicações do CGI.br, NIC.br, Registro.br, CETIC.br, CEPTRO.br e W3C.br.

7. Disposições gerais

7.1. Dos que podem ter acesso lógico

7.1.1. Poderá ter acesso lógico todo o público-alvo desta Política, definido no item 3 da mesma, sendo necessária sua anuência tácita ou expressa, de qualquer forma, à Política de Segurança da Informação implantada no âmbito da Justiça Federal da 2ª Região.

7.2. Do acesso lógico passível de concessão

7.2.1. Para integrarem a qualquer título o patrimônio da Justiça Federal da 2ª Região, bem como para terem expandida sua utilização, as formas de acesso lógico deverão se submeter previamente, conforme o caso, a:

- contratação;

- teste, avaliação e homologação, pela unidade responsável pela TI, em conjunto com o respectivo GN, com ênfase nos requisitos de segurança da informação, principalmente o nível de impacto negativo; e

- autorização ou aprovação, pela Presidência, com assessoramento por parte do CODITI e da CLSI, com ênfase nos mesmos requisitos.

7.2.2. Deverão ser utilizadas na Justiça Federal da 2ª Região ou para ela as formas de acesso lógico que integrem a qualquer título seu patrimônio.

7.2.3. Também poderão ser utilizadas na Justiça Federal da 2ª Região ou para ela, excepcionalmente, as formas de acesso lógico que não integrem seu patrimônio, inclusive na linha do *"BYOD - bring your own device"* (ou seja, "traga seu próprio dispositivo") ou da computação em nuvem (*cloud computing*), principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item 7.2.1 desta Política.

7.2.4. Os computadores que não integrem o patrimônio da Justiça Federal da 2ª Região poderão estar presentes em redes internas apenas se conectados sem fio, ou com fio, situação em que deverão ter configuração idêntica à previamente estabelecida para as estações de trabalho.

7.2.5. O acesso lógico deverá se dar a partir da prévia autorização ao serviço, sucedida, preferencialmente, pela concomitante autenticação do usuário.

7.2.6. A autorização ao serviço deverá se dar por meio da concessão, pelo GN, de permissão ao usuário ou grupo, para agir de determinadas maneiras (tais como ler, modificar etc.), conforme a anterior definição, também pelo GN, dos diferentes perfis, baseados na forma de vínculo, atribuições, unidade ou níveis de acesso, criticidade ou prioridade da informação.

7.2.7. A permissão deverá ser individual e intransferível, sendo possíveis, no entanto, a herança de permissão e o regime de expressa substituição eventual.

7.2.8. Como preceito geral, deverão ser definidos um perfil comum, para a grande maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas relevantes, e determinados perfis especiais (tais como para administradores, técnicos, *designers*, editores, estagiários, empregados de "terceirizados", magistrados, advogados, inspetores e auditores), com máximo ou mínimo privilégio, para as unidades e usuários que exercem atividades com peculiaridades técnicas relevantes.

7.2.9. O administrador deverá ter a possibilidade de modular entre o perfil comum e o perfil especial para administradores, estritamente conforme a ação pretendida.

7.2.10. Todas as formas de acesso lógico deverão ter uma configuração previamente estabelecida, pela unidade responsável pela TI, principalmente quanto aos processos técnicos passíveis de automação (tais como os que envolvem *cookie*, *script*, *plug-in*, *pop-up*, *download*, *upload*, macro, notificação etc.), ressalvada a possibilidade de

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 64 Tribunal Regional Federal - 2ª Região

ajustes de menor proporção por parte do próprio usuário.

7.2.11. A autenticação do usuário deverá se dar por meio de sua identificação, conforme seu anterior credenciamento (*sign-up*), pelo GN, em *ACL - access control list* (ou seja, lista de controle de acesso), na forma de conta de serviços, baseada na credencial completa, composta:

- pelo que se sabe em termos de informação (tal como identidade, senha, dados pessoais etc.); e

- pelo que se tem em termos de tecnologia (tal como *token*, *smartcard* etc.); ou

- pelo que se é em termos de características biométricas (tal como mediante impressão digital, impressão palmar, caligrafia, formação da íris, voz, perfil genético etc.).

7.2.12. A credencial deverá ser individual e intransferível.

7.2.13. Não poderá existir conta de serviços genérica ou compartilhada, exceto se houver outro modo de identificação do usuário, bem como se for baixo o risco de impacto negativo, constatado pelo GN.

7.2.14. Sempre que tecnicamente possível:

- o credenciamento (*sign-up*) deverá compartilhar dados com o registro de incidentes de segurança da informação;

- a autenticação do usuário deverá ser acompanhada da transcrição de caracteres de imagem dinâmica com geração automática (*"CAPTCHA - Completely Automated Public Turing Test to Tell Computers and Humans Apart"*, ou seja, "teste de Turing público completamente automatizado para diferenciação entre computadores e humanos"), em razão de tentativa errônea de autenticação do usuário;

- a autenticação do usuário deverá ser forte, enquanto baseada na credencial completa e limitada quanto a número de sucessivas tentativas;

- a autenticação do usuário não poderá ser automática ou se submeter a preenchimento automático em formulário;

- a conta de serviços deverá ter um prazo de validade, conforme a forma de vínculo ou as atividades exercidas;

- a conta de serviços deverá ser suspensa ou interrompida, em razão de sucessivas tentativas errôneas de autenticação do usuário ou inatividade trimestral;

- a identidade, a senha e os dados pessoais verificados na forma de perguntas e respostas deverão se submeter a padronização quanto a serviço a que são destinados, tamanho mínimo e máximo em número de caracteres, formato em tipos de caracteres e efeitos, e periodicidade de efetiva troca, sem prejuízo dos dados pessoais utilizados apenas para lembrar a senha;

- a geração, entrega e alteração da senha deverão se dar de modo a garantir a manutenção do respectivo sigilo;

- a senha deverá ser forte, enquanto dotada de muitos caracteres de todos os tipos (alfanumérica), em caixa alta e baixa, não idêntica à eventualmente anterior, difícil de adivinhar, e sujeita a efetiva troca no mínimo semestral, principalmente para as formas de acesso lógico que envolvem alto risco de impacto negativo, constatado pela unidade responsável pela TI;

- a senha para o primeiro ingresso (*sign-in, login* ou *logon*) deverá ter um prazo de expiração;

- a senha preenchida em formulário deverá ser invisível e, para acessibilidade por parte de portadores de necessidades especiais de audição, não poderá ser falada;

- a senha deverá se submeter a imediata e efetiva alteração no primeiro ingresso (*sign-in, login* ou *logon*), bem como quando houver anormalidade quanto à permissão ou credencial, ou suspeita de perda do respectivo sigilo, sem prejuízo da efetiva troca periódica;

- a sessão da específica forma de acesso lógico deverá ter um prazo de expiração (*time-out*).

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

7.2.15. As finalidades, conteúdos e práticas de acesso lógico não poderão comprometer o desempenho técnico dos computadores, aplicativos, sistemas, *sites*, *e-mails* e redes, bem como o desempenho funcional de seu usuário, se for o caso.

7.2.16. Qualquer conduta deverá ter sua relevância avaliada independentemente de ser comissiva ou omissiva, dolosa ou culposa, consumada ou tentada.

7.3. Das finalidades do acesso lógico

7.3.1. O acesso lógico deverá se dar em atividades imediatamente relacionadas ao serviço prestado na Justiça Federal da 2ª Região, por lhe serem necessárias, e poderá se dar em atividades mediatamente relacionadas ao serviço nela prestado, por lhe serem úteis.

7.3.2. O acesso lógico também poderá se dar em atividades não relacionadas ao serviço prestado na Justiça Federal da 2ª Região, desde que tratem de conteúdos e configurem práticas permitidas ou não proibidas.

7.4. Dos conteúdos passíveis de acesso lógico

7.4.1. O acesso lógico, com destaque para os computadores, aplicativos, sistemas, *sites*, *e-mails* e redes, deverá se dar para tratar de informações necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região.

7.4.2. O acesso lógico também poderá se dar para tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado na Justiça Federal da 2ª Região, sejam concernentes, dentre outros temas, a educação, saúde, trabalho, comunicação, cidadania, serviços públicos ou de interesse público, governo e poderes estatais, o que inclui, dentre outros correlatos:

- instituições de ensino ou pesquisa;

- planos de saúde;

- entidades sindicais ou associativas;

- meios de comunicação social;

- transporte e trânsito;

- segurança;

- previsão do tempo;

- provedores de *e-mails* não institucionais;

- murais, fóruns, grupos de discussão, grupos de notícias (*newsgroups*), *newsfeeds* e *pushes* profissionais;

- *blogs*, redes e mídias sociais profissionais ou institucionais estatais;

- páginas, perfis e canais institucionais estatais em redes ou mídias sociais.

7.4.3. O acesso lógico não poderá se dar para tratar de informações ilícitas, imorais, abusivas, inconfiáveis, inseguras, anônimas ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, bem como que sejam concernentes a temas muito distantes dos descritos no item 7.4.2 desta Política, enquanto desnecessárias ou inúteis ao serviço prestado na Justiça Federal da 2ª Região, o que inclui, dentre outros similares:

- conteúdos que sejam objeto de crime, contravenção, improbidade administrativa, infração disciplinar ou ética, ato jurídico ilícito ou qualquer outra espécie de infração;

- pornografia;

- violência;

- assuntos pessoais, inclusive relacionamentos;

- jogos e qualquer outra espécie de entretenimento;

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 66 Tribunal Regional Federal - 2ª Região

- concursos de prognósticos (tais como sorteios de números, loterias e apostas);

- salas de bate-papo (*chat*) não profissionais;

- páginas, perfis e canais não institucionais estatais em *blogs*, redes ou mídias sociais.

7.5. Das práticas de acesso lógico

7.5.1. O acesso lógico, com destaque para os computadores, aplicativos, sistemas, *sites, e-mails* e redes, deverá se dar de modo necessário ou útil ao serviço prestado na Justiça Federal da 2ª Região.

7.5.2. O acesso lógico não poderá se dar de modo ilícito, imoral, abusivo, inconfiável, inseguro, anônimo ou com alto risco de impacto negativo, constatado pela unidade responsável pela TI, o que inclui, dentre outros similares:

- práticas que configurem crime, contravenção ou qualquer outra espécie de infração;

- interceptação, invasão, subtração, adulteração, prejuízo ou destruição de informações ou formas de acesso lógico, mediante violação ou desativação de mecanismos de controle de segurança da informação (*hacking*);

- proliferação de *softwares* maliciosos (*malwares*) ou exploradores de vulnerabilidades (*exploits*) de qualquer espécie (tais como vírus, *worms*, "Cavalos de Tróia" e *keyloggers*);

- obtenção de informações mediante fraude (*"phishing"*), ou de qualquer outra espécie de vantagem mediante fraude, num contexto de "engenharia social";

- adulteração de *site* (*cracking*, *defacement* ou "pichação");

- sobrecarregamento, congestionamento ou derrubada de formas de acesso lógico mediante ação em massa de qualquer espécie (*broadcast*);

- difusão de informação institucional falsa;

- difusão de informações de qualquer espécie (texto, imagem estática, imagem dinâmica ou som) não solicitadas (*"SPAM - sending and posting advertisement in mass"*, ou seja, "enviar e postar publicidade em massa"), principalmente com caráter comercial, político, partidário, eleitoral etc.;

- difusão de boatos (*"hoaxes"*);

- difusão de correntes;

- utilização de serviço *proxy* de acesso lógico.

7.5.3. Sempre que tecnicamente possível, todo documento criado por meio de específica forma de acesso lógico deverá ter assinatura eletrônica.

7.5.4. Os dados deverão trafegar, conforme os níveis de acesso, criticidade ou prioridade, em canais:

- apropriados;

- com limite de capacidade adequado;

- preferencialmente internos;

- preferencialmente estatais;

- com criptografia baseada em algoritmo de Estado.

7.5.5. Os dados também poderão trafegar, excepcionalmente, conforme os níveis de acesso, criticidade ou prioridade, em canais:

- externos;

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 67 Tribunal Regional Federal - 2ª Região

- particulares, individuais ou compartilháveis;

- sem criptografia;

- mediante redirecionamento (via *forwarders* ou *aliases*).

7.5.6. Se vierem a estar fora da vigilância de seu proprietário, possuidor ou detentor, inclusive em trânsito, independentemente de estar sendo utilizado em teletrabalho, bem como se vierem a deixar de ser utilizados, o computador, bem como todas as específicas formas de acesso lógico, deverão se submeter a desligamento, bloqueio ou saída (*sign-out, logoff* ou *logout*), preferencialmente de modo automático.

7.6. Do efetivo controle de acesso lógico

7.6.1. O efetivo controle de acesso lógico, pela unidade responsável pela TI:

- poderá ser preventivo, detectivo ou reativo, dando-se prévia, simultânea ou posteriormente, priorizando-se o primeiro;

- deverá ser previamente avisado e agendado, exceto se for alto o risco de impacto negativo, constatado pela unidade responsável pela TI;

- poderá ser ordinário ou extraordinário, gerando relatório.

7.6.2. Poderão ser utilizados os seguintes mecanismos de efetivo controle:

- efetuação de registros (tais como *log*) e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave;

- monitoramento de tráfego constante (tal como mediante *sniffer*);

- rastreamento, varredura ou verificação periódica;

- implantação de filtro (*firewall*);

- implantação de sensores, bem como de alertas sonoros e visuais, com funcionamento constante;

- realização de teste (tal como *pentest*, inclusive mediante *honeypot* ou *honeynet*) periódico;

- bloqueio de conteúdo;

- limitação de prática;

- restrição de propriedades (tais como tipo e tamanho);

- submissão a quarentena ou suspensão;

- invalidade ou expiração;

- remoção ou interrupção;

- inspeção periódica.

7.6.3. Os mecanismos de efetivo controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de *software* anti-vírus e anti-*malware*), sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício, pelo GN; e resguardada a inviolabilidade do sigilo das comunicações de dados.

7.6.4. A inviolabilidade referida no item 7.6.3 desta Política não impede a coleta, uso, armazenamento e tratamento de registros estritamente para o fim de manutenção preventiva, adaptativa, evolutiva ou corretiva.

7.6.5. De modo complementar, os arquivos recebidos por meio de acesso lógico, quando abertos pela primeira vez, deverão se submeter a utilização de *software* anti-vírus.

7.6.6. Aplicam-se subsidiariamente o processo de gestão de riscos e o Catálogo de Fraudes do CAIS -

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 68 Tribunal Regional Federal - 2ª Região

Centro de Atendimento a Incidentes de Segurança da RNP - Rede Nacional de Ensino e Pesquisa.

7.6.7. Qualquer incidente que, envolvendo acesso lógico, aparentemente tenha relevante risco de impacto negativo, deverá ser imediatamente reportado, por quem tomar conhecimento, ou mesmo de modo automatizado, ao respectivo GN e, daí, à CLRI, para os devidos fins.

8. Disposições finais

8.1. As unidades responsáveis deverão providenciar os pertinentes registros e divulgação das informações de que trata esta Política, incluindo a ciência ao CSI-Jus e a consolidação das mesmas na página da segurança da informação, constante no portal eletrônico da Justiça Federal da 2ª Região, sem prejuízo dos pertinentes meios oficiais de publicação.

Elaborado por: Comissão Local de Segurança da Informação	Aprovado por: Presidência	Próxima revisão: 25/09/2016
DAR-TRF2-PolíticaControleAcessoLógicoTI-1.00-2014		Página 8 de 8

.

SERGIO SCHWAITZER
PRESIDENTE

TRF2ANE201400076B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1100336-2362 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action