Justiça Federal 69 Tribunal Regional Federal - 2ª Região

ANEXO Nº TRF2-ANE-2014/00075

Anexo ao documento

Data de revisão:	Revisão nº
Data de criação: 25/09/2014	DAL-TRF2-PolíticaUtilizaçãoRecursosTI-1.00-2014

Política de Utilização de Recursos de TI

1. Apresentação

Este documento acessório à Política de Segurança da Informação da Justiça Federal trata da Política de Utilização de Recursos de TI.

2. Escopo

Esta Política, bem como os eventuais respectivos documentos anexos, têm abrangência local, ou seja, se aplicam exclusivamente no âmbito do Tribunal Regional 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 recurso de TI todo equipamento (*hardware*) ou programa (*software*) com tecnologia da informação, bem como qualquer dado acessível por meio desse equipamento ou programa,

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 70 Tribunal Regional Federal - 2ª Região

agregado ou não na forma de estação de trabalho, que integre a qualquer título o patrimônio do Tribunal como ativo tecnológico informático, tangível ou intangível, ou que, mesmo não o integrando, seja utilizado nele ou para ele, o que inclui, dentre outros similares:

- os computadores de mesa (*desktops*) de qualquer espécie (inclusive os *all-in-ones*);

- os computadores portáteis de colo (*laptops*) de qualquer espécie;

- os computadores portáteis de mão (*palmtops*) de qualquer espécie (inclusive os *smartphones*);

- os terminais de autoatendimento (quiosques);

- os dispositivos periféricos de qualquer espécie (inclusive para acessibilidade por parte de portadores de necessidades especiais) destinados a conexão em computadores (tais como monitores, teclados, *mouses*, caixas de som, fones de ouvido, microfones, leitoras, *hubs*, gravadoras, *HDs* externos, *pen drives*, cartões de memória, *chips*, câmeras, *scanners*, impressoras, multifuncionais, cartuchos, *toners*, *tokens*, *smartcards*, *HSM - hardware security module*, equipamentos de biometria, equipamentos de videoconferência, projetores, *touch boards*, mesas digitalizadoras, *modems*, roteadores, cabos, adaptadores, estabilizadores, filtros e *no-breaks*);

- os equipamentos que compõem o *data center*;

- os equipamentos de redes internas (Intranet), bem como a rede de comunicação de dados que as interliga e as liga a redes externas (Internet), com ou sem fio (via onda infravermelha, *Wi-Fi*, *Bluetooth*, outras espécies de ondas de rádio etc.);

- os programas de computador de qualquer espécie (tais como aplicativos e sistemas);

- os endereços e correios eletrônicos (tais como *sites*, *e-mails*, calendários, agendas, catálogos de contatos e gerenciadores de tarefas);

- as ferramentas eletrônicas de comunicação de dados de qualquer espécie;

- os dados de qualquer espécie armazenados em computadores, dispositivos periféricos e outros equipamentos, bem como em *CDs*, *DVDs* e outras mídias, dispostos ou não em banco de dados (tais como arquivos e certificados digitais).

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 física, 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;

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 71 Tribunal Regional Federal - 2ª Região

- "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, essencialmente, os seguintes:

- art. 2º, c/c os itens 4.2 e 9.3.2 do Anexo I, da Resolução nº 6, de 7 de abril de 2008, do CJF;

- Instrução Normativa nº 6-01, de 22 de maio de 1995, do CJF;

- Lei nº 12.682, de 9 de julho de 2012;

- arts. 3º, *caput*, VI, 4º, *caput*, VIII, e 10, *caput*, II, da Resolução nº 182, de 17 de outubro de 2013, do CNJ;

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

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

- Instrução Normativa nº 24-14, de 30 de setembro de 2008, do Tribunal.

7. Disposições gerais

7.1. Dos usuários dos recursos de TI

7.1.1. Poderá ser usuário dos recursos de TI todo o público-alvo desta Política, definido no item 3 da mesma, sendo necessário, com sua anuência tácita ou expressa, de qualquer forma, o respectivo termo de responsabilidade, conforme a Política de Segurança da Informação implantada no âmbito do Tribunal.

7.2. Dos recursos de TI passíveis de utilização

7.2.1. Para integrarem ou deixarem de integrar a qualquer título o patrimônio do Tribunal, bem como para terem expandida sua utilização, os recursos de TI 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 utilizados no Tribunal ou para ele os recursos de TI que integrem a qualquer título seu patrimônio.

7.2.3. Também poderão ser utilizados no Tribunal ou para ele, excepcionalmente, os recursos de TI 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. Se for o caso, os recursos de TI deverão ser agregados na forma de estações de trabalho conforme um padrão comum, para a grande maioria das unidades e usuários, que exerce atividades sem peculiaridades técnicas relevantes, ou conforme determinados padrões especiais (tais como para administradores, técnicos, designers, editores, estagiários, empregados de "terceirizados", magistrados, advogados, inspetores e auditores), com máximo ou mínimo

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 72 Tribunal Regional Federal - 2ª Região

privilégio, para as unidades e usuários que exercem atividades com peculiaridades técnicas relevantes, ou para acessibilidade por parte de portadores de necessidades especiais.

7.2.5. A estação de trabalho deverá ser individual e intransferível, sendo possível, no entanto, o regime de expressa substituição eventual.

7.2.6. A impressora poderá ser compartilhada, enquanto baixo o risco de impacto negativo.

7.2.7. Todos os componentes das estações de trabalho deverão ter uma configuração previamente estabelecida, pela unidade responsável pela TI, principalmente quanto aos processos técnicos passíveis de automação, ressalvada a possibilidade de ajustes de menor proporção por parte do próprio usuário.

7.2.8. As finalidades, conteúdos e práticas dos recursos de TI não poderão comprometer o desempenho técnico dos próprios recursos, bem como o desempenho funcional de seu usuário, se for o caso.

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

7.3. Das finalidades dos recursos de TI

7.3.1. Os recursos de TI deverão ser utilizados em atividades imediatamente relacionadas ao serviço prestado no Tribunal, por lhe serem necessárias, e poderão ser utilizados em atividades mediatamente relacionadas ao serviço prestado no Tribunal, por lhe serem úteis.

7.3.2. Os recursos de TI também poderão ser utilizados em atividades não relacionadas ao serviço prestado no Tribunal, desde que tratem de conteúdos e configurem práticas permitidas ou não proibidas.

7.4. Dos conteúdos dos recursos de TI

7.4.1. Os recursos de TI, com destaque para os computadores, impressoras, *softwares* e arquivos, deverão tratar de informações necessárias ou úteis ao serviço prestado no Tribunal.

7.4.2. Os recursos de TI também poderão tratar de informações que, embora não sejam necessárias ou úteis ao serviço prestado no Tribunal, sejam concernentes, dentre outros temas, a educação, saúde, trabalho, comunicação, cidadania, serviços públicos ou de interesse público, governo e poderes estatais.

7.4.3. Os recursos de TI não poderão 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 no Tribunal, 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.

7.5. Das práticas com os recursos de TI

7.5.1. Os recursos de TI, com destaque para os computadores, impressoras, *softwares* e arquivos, deverão ser aplicados de modo necessário ou útil ao serviço prestado no Tribunal.

7.5.2. Os recursos de TI não poderão ser aplicados 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 recursos de TI, mediante

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 73 Tribunal Regional Federal - 2ª Região

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";

- 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.

7.5.3. Os dados deverão ser armazenados, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- apropriados;

- com limite de capacidade adequado;

- preferencialmente internos, inclusive, se for o caso, com segregação ("conteinerização");

- preferencialmente estatais;

- com ou sem criptografia baseada em algoritmo de Estado.

7.5.4. Os dados também poderão ser armazenados, excepcionalmente, conforme os níveis de acesso, criticidade ou prioridade, em dispositivos:

- externos;

- particulares, individuais ou compartilháveis;

- sem criptografia.

7.5.5. Todos os dados armazenados, com destaque para os críticos ou prioritários, deverão ou poderão ter cópias de segurança (*backups*) providenciadas, periodicamente, por seu proprietário, possuidor ou detentor, conforme o caso.

7.5.6. Os recursos de TI que integrem o patrimônio do Tribunal poderão ser utilizados, excepcionalmente, fora de suas instalações, independentemente de ser ou não em teletrabalho, principalmente em situações de contingência, desde que previamente submetidos, conforme o caso, às operações descritas no item 7.2.1 desta Política.

7.5.7. 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.

7.5.8. É recomendável que o computador portátil disponha de mecanismos remotos de localização via rede ou *GPS - global positioning system* (ou seja, sistema de posicionamento global), bem como de desligamento, bloqueios, saída (*logoff* ou *logout*), cópia de segurança (*backup*) e apagamento, preferencialmente de modo automático.

7.5.9. O documento impresso que tiver sido definido como controlado, e, assim, que contiver informação classificada em qualquer grau de sigilo, conforme a Lei nº 12.527, de 18 de novembro de 2011, ou em qualquer grau de limitação equivalente, caso a pertinente tecnologia e processos de trabalho adotados no Tribunal ainda não estejam ajustados a essa lei, deverá ser imediatamente recolhido da bandeja de saída da impressora compartilhada, bem como fragmentado ou devidamente rasurado, caso se trate de documento inutilizável, não obstante o art. 15 da Resolução nº 23, de 19 de setembro de 2008, do CJF.

7.6. Do controle da utilização dos recursos de TI

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 74 Tribunal Regional Federal - 2ª Região

7.6.1. O controle da utilização de recursos de TI, 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 controle:

- efetuação de registro (tal como tombamento) e manutenção preferencialmente durante o prazo para aplicar ou buscar a aplicação da penalidade para o tipo de infração mais grave;

- rastreamento, varredura ou verificação periódica (tal como levantamento físico e inventário);

- bloqueio de conteúdo;

- limitação de prática;

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

- submissão a quarentena ou suspensão;

- remoção ou interrupção;

- inspeção periódica.

7.6.3. Os mecanismos de 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 dos dados classificados em qualquer grau de sigilo, conforme a Lei nº 12.527, de 2011, ou em qualquer grau de limitação equivalente, caso a pertinente tecnologia e processos de trabalho adotados no Tribunal ainda não estejam ajustados a essa lei.

7.6.4. De modo complementar, os arquivos armazenados em dispositivos apropriados, quando abertos pela primeira vez, deverão se submeter a utilização de *software* anti-vírus.

7.6.5. Aplicam-se subsidiariamente os mecanismos de controle de todos os recursos materiais.

7.6.6. Qualquer incidente que, envolvendo utilização de recursos de TI, 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 do Tribunal, sem prejuízo dos pertinentes meios oficiais de publicação.

Elaborado por: Comissão Local de Segurança da Informação	Aprovado por: Presidência	Próxima revisão: 25/09/2016
DAL-TRF2-PolíticaUtilizaçãoRecursosTI-1.00-2014		Página 6 de 6

.

SERGIO SCHWAITZER

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal
75
Tribunal Regional Federal - 2ª Região

PRESIDENTE

TRF2ANE201400075B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1093439-169 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action