Justiça Federal 55 Tribunal Regional Federal - 2ª Região

ANEXO Nº TRF2-ANE-2014/00074

Anexo ao documento

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

Política de Segurança de Acesso Físico às instalações envolvidas na guarda das informações

1. Apresentação

Este documento acessório à Política de Segurança da Informação da Justiça Federal trata da Política de Segurança de Acesso Físico às instalações envolvidas na guarda das informações.

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 outros 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 físico às instalações envolvidas na guarda das informações, 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, CJF, CNJ, TCU, CEF e BB);

TRF2ANE2014000074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 56 Tribunal Regional Federal - 2ª Região

- visitantes.

4. Conceituação

Para os efeitos desta Política, considera-se acesso físico às instalações envolvidas na guarda das informações o ingresso, circulação, permanência ou saída de arquivos, sala-cofre, unidades processantes e de protocolo, Gabinetes de magistrados, centrais telefônicas, salas de automação, unidades responsáveis por fonografia e taquigrafia, segurança institucional, saúde, acompanhamento de bens e rendas particulares, processos disciplinares, concursos públicos, licitações e processos criativos, dentre outras similares.

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;

- "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 9.2.1 do Anexo I, da Resolução nº 6, de 7 de abril de 2008, do CJF;

- arts. 13 e ss. da Resolução nº 3, de 10 de março de 2008, do CJF;

- art. 3º da Lei nº 12.694, de 24 de julho de 2012;

- Resolução nº 193, de 8 de maio de 2014, do CNJ;

- Resolução nº 34, de 22 de dezembro de 2010, do Tribunal;

- Instrução Normativa nº 24-06, de 24 de setembro de 2014, do Tribunal;

TRF2ANE201400074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 57 Tribunal Regional Federal - 2ª Região

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

- Norma Interna nº 4-05, de 29 de fevereiro de 2008, da Diretoria do Foro da SJ/ES.

7. Disposições gerais

7.1. Dos que podem ter acesso físico

7.1.1. Poderá ter acesso físico 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 físico passível de concessão

7.2.1. O acesso físico deverá se dar a partir da prévia autorização ao local de guarda, sucedida, preferencialmente, pela concomitante autenticação do usuário.

7.2.2. A autorização ao local de guarda deverá se dar por meio da concessão, pelo GN, de permissão ao usuário ou grupo, para agir de determinadas maneiras (tais como ingressar, circular, permanecer, sair 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.

7.2.3. Aplicam-se subsidiariamente as permissões e os perfis definidos para o acesso físico às instalações comuns (tais como portaria/recepção, *hall* de entrada, escadas, elevadores não privativos, corredores, banheiros, centrais de atendimento ao público externo, balcões/recepções, salas de audiências e sessões de julgamento, ouvidoria, bibliotecas, salas de leitura e cafeterias).

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

7.2.5. 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.

7.2.6. A autenticação do usuário deverá se dar por meio de sua identificação, no local de guarda, perante o GN, conforme seu anterior credenciamento, na portaria/recepção, pela unidade responsável pela infraestrutura ou segurança, em *ACL - access control list* (ou seja, lista de controle de acesso), baseada na credencial completa, composta:

- pelo que se tem em termos de tecnologia (tal como crachá, distintivo, *button*, *pin*, broche, *token*, *smartcard*, selo, cartão de estacionamento 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.).

7.2.7. O crachá é a principal tecnologia que compõe a credencial.

7.2.8. A credencial deverá ser individual e intransferível.

7.2.9. O crachá deverá:

- ter especificações (tais como dimensões, cores, impressões etc.) que permitam fácil distinção visual do perfil do usuário;

- ser colocado em local que permita fácil visualização e assim permanecer enquanto no interior das dependências da Justiça Federal da 2ª Região.

7.2.10. Todo local de guarda deverá, conforme os níveis de acesso, criticidade ou prioridade das informações nele guardadas:

- ser dotado de infraestrutura inviolável ou de difícil violação, bem como portas e janelas passíveis de

TRF2ANE201400074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 58 Tribunal Regional Federal - 2ª Região

trancamento;

- ter acesso restrito;

- receber, clara e ostensivamente, em sua entrada e interior, as respectivas sinalizações, porém sem qualquer menção a eventual existência de informação classificada em qualquer grau de sigilo, conforme a Lei nº 12.527, de 18 de novembro de 2011, bem como crítica ou prioritária;

- ser dotado de mobiliário inviolável ou de difícil violação e passível de trancamento, destinado ao armazenamento de suportes físicos de informações.

7.2.11. Todos os locais de guarda deverão se submeter a mapeamento e conseqüentes definições, pelas unidades responsáveis pela infraestrutura ou segurança, TI, documentação e segurança institucional, em conjunto com os respectivos GNs, dos respectivos níveis/perímetros de segurança, bem como dos *PPS - perimeter protection systems* (ou seja, sistemas de proteção de perímetro), baseados nos níveis de acesso, criticidade ou prioridade das informações nele guardadas.

7.2.12. Aplicam-se subsidiariamente o tombamento de todos os recursos materiais, as barreiras próprias da segurança física, as medidas especiais de tratamento de informações e a planilha da força de trabalho.

7.2.13. Sempre que tecnicamente possível:

- o credenciamento deverá compartilhar dados com o registro de incidentes de segurança da informação;

- a autenticação do usuário, em catraca/roleta eletrônica do *hall* de entrada, deverá disparar comando para o elevador ir ao andar a que o usuário pretende se dirigir, bem como notificação para o respectivo local de guarda, conforme seu anterior credenciamento, sem prejuízo de posterior acesso a outros andares e locais de guarda;

- o crachá e o cartão de estacionamento deverão ser dotados de fotografia digitalizada com alta resolução e colorida, diretamente gravada ou impressa e colada;

- o crachá e o cartão de estacionamento deverão ser dotados de *transponder* (transmissor) para *RFID - radio-frequency identification* (ou seja, identificação por radiofreqüência) e, ao mesmo tempo, as dependências da Justiça Federal da 2ª Região deverão ser dotadas dos respectivos *readers* (leitores), tanto para ingresso quanto para circulação, permanência e saída;

- o crachá e o cartão de estacionamento deverão ter um prazo de validade, conforme a forma de vínculo ou as atividades exercidas;

- todo local de guarda deverá ser dotado de porta com fechadura e chave eletromecânicas eletrônicas, bem como de mobiliário passível de trancamento da mesma espécie;

- a geração, entrega e alteração de segredo de cofre deverão se dar de modo a garantir a manutenção do respectivo sigilo.

7.3. Das finalidades do acesso físico

7.3.1. O acesso físico 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 físico também poderá se dar em atividades não relacionadas ao serviço prestado na Justiça Federal da 2ª Região, desde que configurem práticas permitidas ou não proibidas.

7.3.3. Aplica-se subsidiariamente a lista de práticas permitidas ou não proibidas própria da segurança física.

7.4. Das práticas de acesso físico

7.4.1. O acesso físico deverá se dar de modo necessário ou útil ao serviço prestado na Justiça Federal da 2ª Região.

7.4.2. O acesso físico não poderá se dar de modo ilícito, imoral, abusivo, inconfiável, inseguro, anônimo ou com alto risco de impacto negativo, constatado pelo GN, o que inclui, dentre outros similares:

TRF2ANE201400074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

Justiça Federal 59 Tribunal Regional Federal - 2ª Região

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

- interceptação, invasão, subtração, adulteração, prejuízo ou destruição de informações, mediante violação ou desativação de mecanismos de controle de segurança da informação;

- exploração de vulnerabilidades;

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

- sobrecarregamento ou congestionamento de locais de guarda mediante ação em massa de qualquer espécie.

7.4.3. Enquanto o local de guarda estiver aberto, no mínimo dois servidores lotados na respectiva unidade deverão:

- estar presentes e vigilantes, ressalvada a possibilidade de permissão diversa pelo GN, principalmente em situações de contingência, exceto se for alto o risco de impacto negativo;

- supervisionar constantemente a utilização de dispositivos móveis de qualquer espécie destinados a reprodução de informações (tais como telefones, *smartphones*, gravadores, *pen drives*, cartões de memória, *chips*, câmeras, *scanners* e impressoras) ou aptos a eliminação de suportes físicos de informações, bem como o porte de acessórios para carregar objetos (tais como bolsas, sacos, sacolas e maletas) ou o uso de peças de vestuário aptas a carregarem objetos, conforme os níveis de acesso, criticidade ou prioridade das informações nele guardadas;

- evitar situações aptas a prejuízo de sua atenção;

- contar com o auxílio da unidade responsável pela infraestrutura ou segurança.

7.4.4. Se vier a estar inabitado, todo local de guarda deverá se submeter a trancamento, preferencialmente de modo eletrônico, ressalvada a possibilidade de permissão diversa pelo GN, principalmente em situações de contingência, exceto se for alto o risco de impacto negativo.

7.4.5. Se o local de guarda não tiver se submetido a trancamento no fim do expediente, e não for a hipótese da ressalva descrita no item 7.4.4 desta Política, ele deverá se submeter a lacre, pela unidade responsável pela infraestrutura ou segurança, no qual deverão constar o dia e hora de sua aposição.

7.5. Do controle de acesso físico

7.5.1. O controle de acesso físico, pela unidade responsável pela infraestrutura ou segurança:

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

- poderá ser ordinário ou extraordinário, gerando relatório.

7.5.2. Poderão ser utilizados os seguintes mecanismos de controle:

- efetuação de registros (tal 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 a utilização de CFTV - circuito fechado de televisão);

- ronda diária;

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

- realização de teste (tal como *pentest*) periódico;

- limitação de prática;

TRF2ANE201400074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action

- suspensão;

- invalidade;

- expulsão;

- inspeção periódica.

7.5.3. Sempre que tecnicamente possível, os mecanismos de controle, sempre atualizados, deverão ser ativados de modo automatizado (tal como mediante a utilização de detectores de metais, *scanners* de raios X, catracas/roletas e cancelas eletrônicas, detectores de abertura, presença e movimento, detectores de ondas eletromagnéticas, bem como *IPS - intrusion prevention system* e *IDS - intrusion detection system*, ou seja, sistemas de prevenção e detecção de intrusão), sem a possibilidade de desativação, ressalvada a possibilidade de revisão do resultado dessa automatização, a pedido ou de ofício, pelo GN; e resguardada a plenitude da liberdade de locomoção.

7.5.4. Aplicam-se subsidiariamente os mecanismos de controle próprios da segurança física e de todos os recursos materiais, bem como o processo de gestão de riscos.

7.5.5. A danificação, extravio ou perda de qualquer chave, bem como a suspeita de perda do sigilo de segredo de cofre, deverão ser imediatamente reportados, pelo GN, à unidade responsável pela infraestrutura ou segurança; e todos esses incidentes, bem como a execução de qualquer serviço de chaveiro (tal como de confecção, cópia ou mestragem de chave), a geração, entrega e alteração de segredo de cofre, e a abertura de qualquer fechadura sem chave ou segredo, deverão ser registrados por esta unidade.

7.5.6. Qualquer incidente que, envolvendo acesso físico, 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-PolíticaSegurançaAcessoFísico-1.00-2014		Página 6 de 6

.

SERGIO SCHWAITZER
PRESIDENTE

TRF2ANE201400074B

Assinado digitalmente por SERGIO SCHWAITZER.
Documento Nº: 1088548-1195 - consulta à autenticidade em https://siga.jfrj.jus.br/sigaex/autenticar.action