Imprimir...

RESOLUÇÃO PRES Nº 294, DE 19 DE AGOSTO DE 2019.

Implantar a Instrução Normativa 37-06, que trata da Política de Segurança de Tecnologia da Informação da Justiça Federal da 3.ª Região.

A PRESIDENTE DO TRIBUNAL FEDERAL DA TERCEIRA REGIÃO, no uso de suas atribuições regimentais,

CONSIDERANDO a Resolução CJF n.º 6, de 7 de abril de 2008, 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;

CONSIDERANDO a necessidade de estabelecer procedimentos de segurança da informação para a Justiça Federal da 3.ª Região, a fim de garantir a segurança dos sistemas informatizados;

CONSIDERANDO o expediente SEI n.º 0017976-66.2014.4.03.8000,

R E S O L V E:

Art. 1.º Implantar, no âmbito da Justiça Federal da 3.ª Região, a Instrução Normativa n.º 37-06, que dispõe sobre a Política de Segurança de Tecnologia da Informação da Justiça Federal da 3.ª Região.

Art. 2.º Esta Resolução entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Documento assinado eletronicamente por **Therezinha Astolphi Cazerta**, **Desembargadora Federal Presidente**, em 21/08/2019, às 22:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

Disponibilizada no Diário Eletrônico da Justiça Federal da 3ª Região em 23/08/2019, Caderno Administrativo, págs. 1-10. Considera-se data de publicação o primeiro dia útil subseqüente à data acima mencionada, nos termos do art. 4º, §§ 3º e 4º, da Lei 11.419/2006.

ANEXO RESOLUÇÃO PRES N.º 294, DE 19 DE AGOSTO DE 2019

IN - 37-06

SISTEMA: **INFORMÁTICA**	Número: **IN-37-06**
SUBSISTEMA: **POLÍTICA DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO DA JUSTIÇA FEDERAL DA 3.ª REGIÃO**	
MÓDULO: **ÍNDICE**	

ASSUNTO	MÓDULO
GENERALIDADES	1
ACESSO AOS DIVERSOS SISTEMAS	2
UTILIZAÇÃO DO CORREIO ELETRÔNICO	3
UTILIZAÇÃO DA INTERNET E INTRANET	4
PROTEÇÃO	5
MANUTENÇÃO	6

MÓDULO 1: **GENERALIDADES**

I - REFERÊNCIAS

a) Decreto n.º 3.505, de 13/7/2000, da Presidência da República - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

b) Decreto n.º 3.996, de 31/10/2001, da Presidência da República - Dispõe sobre a prestação de serviços de certificação digital, no âmbito da Administração Pública Federal.

c) Portaria n.º 104, de 6/3/2015, do Conselho da Justiça Federal - Dispõe sobre a aprovação do documento acessório comum "Política de Segurança para Desenvolvimento, Aquisição e Manutenção de Sistemas", de que trata a Resolução CJF n.º 6/2008.

d) Resolução n.º 293, de 22/5/2012, da Presidência do TRF da 3.ª Região - Institui o Gestor de Sistema de Informação e o Comitê Gestor de Sistema de Informação na 3.ª Região.

e) Resolução n.º 424, de 9/6/2015, da Presidência do TRF da 3.ª Região - Implanta a IN-37-04, que regulamenta o processo de desenvolvimento de software corporativo, no âmbito da Justiça Federal da 3.ª Região.

f) Resolução n.º 279, de 27/12/2013, do Conselho da Justiça Federal - Dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal - MCTI-JF, no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

g) Resolução n.º 255, de 27/7/2011, da Presidência do TRF da 3.ª Região - Padroniza o acesso à internet na Justiça Federal da 3.ª Região.

h) Resolução n.º 6, de 7 de abril de 2008, do Conselho da Justiça Federal - Dispõe sobre a implantação da Política de Segurança e a utilização dos ativos de informática, no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

i) Resolução n.º 278, de 15/2/2012, da Presidência do TRF da 3.ª Região - Regulamenta a utilização do correio eletrônico, no âmbito da Justiça Federal da 3.ª Região.

j) Resolução Conjunta n.º 3, de 16/4/2013, do CNJ - Institui o Modelo Nacional de Interoperabilidade do Poder Judiciário e do Ministério Público e dá outras providências.

k) Ordem de Serviço n.º 6, de 16/6/2016, da Presidência do TRF da 3.ª Região - Dispõe sobre a criação, a alteração e a atualização das páginas do sítio do Tribunal.

l) Resolução n.º 339, de 15/8/2013, da Presidência do TRF da 3.ª Região - Regulamenta a utilização da rede sem fio, no âmbito da Justiça Federal da 3.ª Região.

m) Resolução n.º 52, de 21/9/2016, da Presidência do TRF da 3.ª Região - Regulamenta a utilização da VPN – Virtual Private Network, no âmbito da Justiça Federal da 3.ª Região;

n) Resolução n.º 83, de 16/12/2016, da Presidência do TRF da 3.ª Região - Estabelece as regras para as páginas da *internet* e da *intranet* da Justiça Federal da 3.ª Região.

II - FINALIDADE

Esta Instrução Normativa tem por finalidade reger a Política de Segurança de Tecnologia da Informação da Justiça Federal da 3.ª Região.

III - CONCEITOS

01 - Acesso: capacidade de uma pessoa ingressar em um sistema.

02 - Ambiente de desenvolvimento de sistemas: é o local utilizado pela equipe técnica para desenvolver e testar o sistema e realizar suas manutenções, incluindo todos os itens necessários para isso, como base de dados, programas-fonte e ferramentas de apoio.

03 - Ambiente de produção: é o local onde o sistema é instalado e disponibilizado para utilização pelos usuários finais, incluindo a aplicação (código executável), a base de dados e quaisquer outras ferramentas de apoio necessárias.

04 - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização.

05 - Assinatura digital: código usado para comprovar a autenticidade e a integridade de uma informação.

06 - Ativos de Tecnologia da Informação: quaisquer equipamentos, *softwares*, recursos, informações ou bens de Tecnologia da Informação.

07 - Autenticidade: visa garantir para o receptor de uma mensagem que ela realmente pertence ao emissor legítimo da comunicação.

08 - Autorizadores: servidores públicos da Justiça Federal da Terceira Região, com delegação superior para aprovar demandas e necessidades.

09 - *Backup*: cópia de segurança das informações, armazenada em um meio separado do original, de forma a proteger esse dados de qualquer eventualidade. Essencial para dados importantes.

10 - Callcenter: sistema de chamados relacionado com o catálogo de serviços de Tecnologia da Informação.

11 - CD/DVD: o *Compact Disc* (abreviado como CD) é um disco ótico digital de armazenamento de dados; o *Digital Versatile Disc* (abreviado como DVD) é um formato digital para arquivar ou guardar dados, som e voz, que possui maior capacidade de armazenamento comparativamente ao CD.

12 - Certificado digital: registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um site Web) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

13 - CLRI: Comissão Local de Resposta a Incidentes de Segurança da Informação, criada pela Portaria PRES n.º 7.847/2015 e com atribuições definidas pela Resolução CJF n.º 6/2008.

14 - CLSI: Comissão Local de Segurança da Informação, criada pela Portaria PRES n.º 98/2016 e com atribuições definidas pela Resolução CJF n.º 6/2008.

15 - Confidencialidade: propriedade que garante não estar a informação disponível ou não ser revelada a pessoa física, sistema, órgão ou entidade não autorizados nem credenciados.

16 - Configurações: opções e parâmetros de um equipamento ou software que podem ser definidas previamente à utilização.

17 - Console: terminal ou periférico utilizado para comunicação entre o operador de computador e o computador, que permite a intervenção, por métodos manuais, no controle da máquina e nos processamentos que estão sendo por ela efetuados.

18 - Conta de usuário: também chamada de "nome de usuário" e "nome de login", corresponde à identificação única de um usuário em um computador ou serviço.

19 - Controle de versão: procedimento, automatizado ou não, que permite manter e disponibilizar cada versão produzida de um determinado programa, evitando sobreposição e mantendo histórico de alterações.

20 - Credenciais de acesso: conjunto composto pelo nome da conta de usuário e pela respectiva senha utilizados para ingresso ou acesso (login) em equipamentos, rede ou sistema.

21 - Criptografia: disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo.

22 - Criticidade: possibilidade de que a redução ou perda de funcionalidade de um determinado ativo cause impacto ao negócio, de acordo com sua gravidade.

23 - Dados estruturados: dados que contêm uma organização lógica, para serem recuperados. De forma geral, armazenados em bancos de dados.

24 - *Desktops*: termo internacionalmente usado para se referir aos computadores de mesa; quando os componentes são separados: mouse, teclado, gabinete, monitor, impressora etc.).

25 - Disponibilidade: garantia de que a informação estará disponível aos seus usuários legítimos, sempre que ela for necessária.

26 - Dispositivo móvel: equipamento com recursos computacionais que, por ter tamanho reduzido, oferece grande mobilidade de uso, podendo ser facilmente carregado pelo seu dono. Exemplos: notebooks, netbooks, tablets, PDAs, smartphones e celulares.

27 - *Download*: é a transferência de arquivos de um computador remoto/site para o computador "local" do usuário. No sentido contrário, ou seja, do computador do usuário para o computador remoto, a transferência de arquivos é conhecida como *upload.*

28 - Engenharia reversa: é o processo de descobrir os princípios tecnológicos e o funcionamento de um dispositivo, objeto ou sistema, através da análise de sua estrutura, função e operação.

29 - Espelhamento: é o processo de duplicação de recursos (discos, fontes de energia, equipamentos), mantendo seus conteúdos ou configurações equivalentes à matriz, de forma que possa assumir o funcionamento, em caso de falha do equipamento matriz.

30 - Estação de trabalho: computador de uso pessoal.

31- Estratégia de *site-backup*: estrutura de operação que replica os dados em mais de um local.

32 - Extranet: extensão segura de uma intranet, que permite aos usuários internos de uma organização acessarem recursos de rede interna privada, utilizando-se de um acesso externo controlado.

33 - *Freeware*: é qualquer programa de computador cuja utilização não implica pagamento de licenças de uso ou de royalties.

34 - Gerador elétrico: é um dispositivo utilizado para a conversão da energia mecânica, química ou de qualquer outra natureza em energia elétrica.

35 - *Hardware*: a parte física, material, do computador (unidades centrais de processamento, microcomputadores, impressoras e demais periféricos).

36 - Homologação: procedimento que consiste na averiguação de conformidade com os requisitos especificados.

37 - Impacto: grau do prejuízo que a concretização de uma determinada ameaça causará. Exemplo: o impacto causado em um computador devido à contaminação por um vírus.

38 - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação.

39 - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

40 - Integridade: garantia de que uma informação não foi modificada, desde a origem até o destino.

41 - Internet: é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos (*Internet Protocol Suite* ou *TCP/IP*), com o propósito de servir progressivamente usuários no mundo inteiro.

42 - Intranet: rede de comunicação interna privada de uma organização, baseada em protocolos da internet, utilizada para compartilhar e trocar informações, mas com acesso restrito aos usuários internos.

43 - Irretratabilidade: garantia de que o autor de uma informação não possa negar a sua autoria, controlada pela existência da assinatura digital que somente ele pode gerar, sem negar a própria efetividade de todo o sistema de segurança.

44 - Licenciamento de *softwares*: direito legal de instalar, exibir, acessar, executar e interagir com um programa.

45 - *Login*: código de identificação do usuário para acesso a sistema ou a equipamento.

46 - Melhoria: solicitação para aperfeiçoar *software* aplicativo (ou parte dele) já implantado, sem alteração em regra de negócio, conforme IN-37-04.

47 - Metadados: são dados sobre outros dados. Um item de um metadado pode dizer do que trata aquele dado, geralmente uma informação inteligível por um computador.

48 - *Modem*: equipamento que converte sinais digitais derivados de um computador ou de outro aparelho digital em sinais analógicos, para transmiti-los por uma linha tradicional de telefone, de forma a serem lidos por um computador ou por outro aparelho.

49 - *Nobreak*: sistema de alimentação secundário de energia elétrica, que entra em ação, alimentando os dispositivos a ele ligados, quando há interrupção no fornecimento de energia primária.

50 - *Notebook* institucional: computador portátil pertencente ao patrimônio da Justiça Federal da 3.ª Região.

51 - Nova funcionalidade: solicitação para implementar novas regras de negócio em *software* aplicativo já implantado, conforme IN-37-04.

52 - *Open source*: *software* cujos códigos-fonte são distribuídos livremente, de forma que qualquer pessoa possa consultá-lo, examiná-lo ou modificá-lo.

53 - Pasta compartilhada na rede: área de armazenamento na rede de computadores, que pode ser acessada por usuários de outras unidades.

54 - *Pen drive*: dispositivo móvel de armazenamento de dados que utiliza memória *flash* e uma entrada *USB*.

55 - Periféricos: qualquer equipamento ou acessório que seja ligado à *CPU* (unidade central de processamento) ou, num sentido mais amplo, ao computador.

56 - Personificação: ato de atuar como se fosse outro.

57 - Personificação de páginas da Justiça Federal: fenômeno que ocorre quando um terceiro publica páginas próprias no sítio da Justiça Federal da 3.ª Região.

58 - Plano de contingência: medidas a serem tomadas, incluindo a ativação de processos manuais, para fazer os processos vitais voltarem a funcionar plenamente ou num estado minimamente aceitável, o mais rápido possível, evitando uma paralisação prolongada que possa gerar maiores prejuízos.

59 - Plano de continuidade: desenvolvimento preventivo de um conjunto de estratégias e de planos de ação, de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados, após a ocorrência de um desastre, até o retorno à situação normal de funcionamento.

60 - Política de *backup*: define a estratégia e a periodicidade de realização de cópias de segurança.

61 - Política de segurança: define os direitos e as responsabilidades de cada um em relação à segurança dos recursos computacionais que utiliza e as penalidades às quais está sujeito, caso não a cumpra.

62 - Processadores: dispositivos responsáveis pelos cálculos, decisões lógicas e execuções de tarefas do computador.

63 - Programas-fonte: conjunto de instruções escrito em linguagem de programação, de forma ordenada e em sequência lógica.

64 - *Proxy*: em redes de computadores, um *Proxy* (procurador) é um servidor (sistema de computação ou de aplicação) que age como um intermediário para requisições de usuários, solicitando recursos de tecnologia da informação.

65 - *Proxy* do Correio Eletrônico: recurso que permite a um usuário de sistema de correio eletrônico acesso identificado e controlado a outra conta, de usuário ou corporativa.

66 - *Rack*: estrutura utilizada para acondicionar equipamentos de rede de computadores.

67 - Recursos de hibernação: o computador fica completamente desligado, usa menos energia que a suspensão, entretanto, o início do dispositivo é mais lento, pois os programas e os documentos abertos ficam armazenados no disco rígido.

68 - Recursos de suspensão: colocam o computador em estado de economia de energia, permitem o início do dispositivo mais rápido que a hibernação, pois os programas e os documentos abertos ficam armazenados na memória *RAM.*

69 - Recursos de Tecnologia da Informação: *softwares*, equipamentos ou dispositivos que utilizem tecnologia da informação, bem como quaisquer recursos ou informações que sejam acessíveis através desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, acessos à rede local, internet, *VPN*, *pendrives*, *smartcards, tokens, smartphones, modems* sem fio, *desktops* e pastas compartilhadas na rede.

70 - Repositório de informação: local de armazenamento de informações.

71 - Risco: probabilidade de uma ameaça ocorrer, juntamente com o impacto que trará.

72 - Segurança: medidas de controle que visam assegurar a proteção de sistemas. Exemplo: treinamento em segurança da informação para os usuários de uma instituição.

73 - Senha: conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser e que possui o direito de acessar o recurso em questão.

74 - Serviços de Tecnologia da Informação: quaisquer recursos de *softwares* e *hardwares* disponibilizados aos usuários da Justiça Federal da 3.ª Região pela Secretaria de Tecnologia da Informação, tais como sistemas de informação, serviços de mensageria eletrônica, navegação extranet, internet e intranet, pastas de rede e correio eletrônico.

75 - Sistema de Informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, com o fim de otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação.

76 - Sistema operacional: programa ou conjunto de programas e aplicativos que servem de interface entre o usuário e o computador.

77 - *Smartcard*: cartão assemelhado, em forma e tamanho, a um cartão de crédito convencional, possui capacidade de processamento, pois embute um microprocessador e memória (que armazena vários tipos de informação na forma eletrônica), ambos com sofisticados mecanismos de segurança.

78 - *Smartphone*: celular que combina recursos com computadores pessoais, com funcionalidades avançadas que podem ser estendidas por meio de programas executados por seu sistema operacional, chamados de aplicativos ou *apps* (diminutivo de *"Applications"*).

79 - *Software*: parte não física - são os programas (instruções) que fazem o computador funcionar.

80 - *Switch*: dispositivo utilizado em redes de computadores para reencaminhar pacotes (*frames*) entre os diversos nós.

81 - *Token*: dispositivo eletrônico gerador de senhas, geralmente sem conexão física com o computador, podendo também, em algumas versões, ser conectado a uma porta *USB*.

82 - Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo, tornando-se parte de outros programas e arquivos. O vírus depende da execução do programa ou do arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

83 - *VPN* (*Virtual Private Network*): termo usado para se referir à construção de uma rede privada utilizando redes públicas (como a internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança, para garantir que somente usuários autorizados possam ter acesso à rede privada e nenhum dado seja interceptado enquanto estiver passando pela rede pública.

84 - Vulnerabilidade: condição que, quando explorada por um atacante, pode resultar em violação da segurança. Exemplo: um antivírus desatualizado.

IV - CONVENÇÕES

SETI: Secretaria de Tecnologia da Informação

TI: Tecnologia da Informação

V - OBJETIVOS

01 - Estabelecer normas, procedimentos e controles de acesso de usuários aos recursos de Tecnologia da Informação.

02 - Orientar ações de segurança tecnológica, a fim de reduzir riscos associados à informação, bem como garantir a integridade, a autenticidade, a confidencialidade e a disponibilidade dos ativos de Tecnologia da Informação da Justiça Federal da 3.ª Região.

03 - Permitir a adoção de soluções de segurança da Tecnologia da Informação e servir de referência para auditoria, apuração e avaliação de responsabilidades.

VI - USUÁRIOS

01 - Usuários internos: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos e, desde que previamente autorizados, empregados de empresas prestadoras de serviços, estagiários e outras pessoas que se encontrem a serviço do Poder Judiciário, ainda que em caráter temporário.

02 - Usuários externos: magistrados e servidores aposentados, bem como pessoas não pertencentes ao quadro de pessoal, tais como advogados e jurisdicionados.

VII - ABRANGÊNCIA

01 - A referência feita à Justiça Federal da 3.ª Região nesta Instrução Normativa abrange o Tribunal Regional Federal da 3.ª Região, bem como a Justiça Federal de 1.º grau das Seções Judiciárias de São Paulo e de Mato Grosso do Sul.

02 - Esta política se aplica, no que couber, às atividades de todos os usuários de que trata o Título VI - Usuários, deste Módulo, ou quem venha a ter acesso a dados ou a informações protegidos pela presente Instrução Normativa.

VIII - DIRETRIZES E PRINCÍPIOS

01 - Celeridade: ações de respostas a incidentes e de correções de falhas serão adotadas o mais rápido possível.

02 - Conhecimento: administradores e usuários de um sistema de informação devem ter ciência de todas as normas e procedimentos de segurança necessários.

03 - Integração: os processos de segurança devem ser coordenados e integrados entre si e com os demais procedimentos e práticas da organização, objetivando um sistema coerente de segurança da informação.

04 - Legalidade: os processos de segurança da TI devem levar em consideração as leis, as normas e as políticas organizacionais, administrativas, comerciais, técnicas e operacionais.

05 - Responsabilidade: as responsabilidades primárias e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas.

06 - Revisão: os sistemas de segurança devem ser reavaliados periodicamente, conforme a evolução tecnológica.

07 - Continuidade dos serviços de TI: os processos de segurança da Tecnologia da Informação devem contribuir para a resiliência dos serviços de TI da Justiça Federal da 3.ª Região.

08 - Alinhamento estratégico: os processos de segurança da TI devem estar alinhados à visão, aos objetivos e à missão da Justiça Federal da 3.ª Região, expressos em seu Planejamento Estratégico Organizacional e em seu Planejamento Estratégico de Tecnologia da Informação.

MÓDULO 2: **ACESSO AOS DIVERSOS SISTEMAS**

01 - O acesso aos serviços de TI da 3.ª Região deve ser realizado por meio de credenciais individuais e exclusivas, sendo expressamente vedado o compartilhamento de credenciais em qualquer situação.

02 - A SETI atenderá todos os chamados do callcenter referentes à concessão ou à remoção de direito de acesso à rede, à concessão de credenciais, à concessão de conta de e-mail institucional e ao acesso a pastas compartilhadas em rede.

02.1 - Não se aplica o disposto neste item para os casos em que a concessão ou a remoção do acesso estiverem automatizadas por integração entre os sistemas de gestão de pessoas e de gerenciamento de identidades.

02.2 - Nos chamados do callcenter para concessão de credenciais de acesso a estagiários e a terceirizados, deverá ser informada a data prevista de encerramento do contrato, limitada a dois anos, a qual será utilizada para remoção de acesso à rede de forma automatizada.

02.2.1 - Havendo renovação do contrato, nova concessão de credenciais deverá ser solicitada, nos termos do subitem 02.2.

03 - Não será permitida a alteração de credencial de acesso, a fim de se preservarem os registros históricos de uso dos sistemas.

04 - O usuário deverá, toda vez que concluir seu trabalho ou quando, por qualquer motivo, se afastar da estação de trabalho:

a) desconectar-se ou bloquear o acesso ao sistema;

b) desconectar *tokens, smartcards e arquivos* contendo certificados digitais.

04.1 - As estações de trabalho terão bloqueio de tela automático, ativado após quinze minutos de inatividade.

05 - As autorizações e as permissões de acessos para utilização de recursos de TI são de responsabilidade dos Autorizadores das respectivas unidades.

06 - Cabe ao gestor:

a) solicitar a atualização do cadastro de acesso aos sistemas informatizados da unidade, sempre que houver movimentação de lotação de servidores ou mudança de código da unidade nos sistemas, bem como retirar as autorizações e permissões de acessos atribuídas;

b) providenciar a alteração da senha da conta institucional da unidade, bem como incluir/excluir servidor da lista de acesso ao Proxy do correio eletrônico.

06.1 - Entende-se por movimentação qualquer alteração de vinculação/lotação ou situação de afastamento de usuário, tais como:

a) admissão;

b) desligamento de forma definitiva;

c) mudança de lotação de uma unidade para outra;

d) afastamento temporário;

e) retorno de afastamento temporário.

06.2 - A concessão de acessos deve obedecer ao critério de menor privilégio, ou seja, o acesso pleno restringe-se aos administradores (servidores da área de tecnologia da informação e outros que venham a ser assim designados, em razão de suas atribuições), concedendo-se ao usuário comum acesso limitado aos recursos de informação imprescindíveis para o desempenho das atividades tipicamente judicantes e administrativas, ficando a liberação de níveis de acessos mais avançados condicionada à avaliação da SETI e dos gestores de sistemas, se o caso.

07 - O descadastramento, quando necessário, será sempre lógico, isto é, com inativação de dados e não exclusão, de forma a não implicar perda de registros históricos de uso do sistema.

08 - Nos casos de perda de senha de acesso aos sistemas, não sendo possível recuperá-la automaticamente ou o sistema não disponibilizar tal procedimento, o usuário deverá solicitar ao gestor de sua unidade a abertura de chamado no CallCenter para recuperação de senha.

08.1 - A senha fornecida mediante CallCenter deve ser alterada imediatamente pelo usuário.

08.2 - É vedado à SETI atender os pedidos verbais de alteração de direitos de acesso e senhas, exceto em situações de risco iminente e irreparável à segurança das informações, o que ensejará posterior justificativa.

09 - O acesso do usuário às informações, aos sistemas e aos recursos de TI deve ser realizado em atividades estritamente relacionadas às suas funções institucionais.

09.1 - A utilização dos sistemas é passível de monitoramento, sendo seus registros, quando efetuados, mantidos pela SETI durante o prazo mínimo definido na política de backup.

10 - As informações geradas nos sistemas são propriedade da Justiça Federal da 3.ª Região, independentemente da forma de sua apresentação ou armazenamento, e serão adequadamente protegidas e utilizadas, para fins relacionados às atividades desta Justiça Federal.

11 - É vedada a prática ou tentativa de contornar ou burlar os mecanismos de segurança dos sistemas e recursos de TI, bem como a prática de abusos de privilégios de acesso e a posse indevida de informações.

11.1 - Excetuam-se deste item os procedimentos executados pelos setores técnicos competentes da SETI com o intuito de tornar efetivas medidas defensivas e eliminar eventuais falhas, desde que aprovados pela referida Secretaria.

MÓDULO 3: **UTILIZAÇÃO DO CORREIO ELETRÔNICO**

01 - A utilização do Correio Eletrônico seguirá o disposto na Resolução n.º 278/2012, da Presidência, e suas alterações posteriores.

02 - É recomendável a utilização de assinatura digital para o envio de mensagens que o remetente considerar necessária a garantia de autenticidade, de integridade e de não-repúdio.

MÓDULO 4: **UTILIZAÇÃO DA INTERNET E DA INTRANET**

01 - O acesso à Internet seguirá o disposto na Resolução n.º 255/2011, da Presidência, e suas alterações posteriores.

02 - A disponibilização de informação na intranet e/ou internet seguirá o disposto na Resolução PRES n.º 83/2016, e suas alterações posteriores.

03 - Todo material inserido nas páginas da Internet ou Intranet da Justiça Federal da 3ª Região pertence à Instituição, que possui a exclusividade dos seus direitos. O uso desses recursos é consentido a todos os usuários, desde que o seja para finalidade relacionada às atividades da Instituição. Em todo caso deverá ser sempre citada a fonte do material.

04 - A SETI monitorará os acessos às páginas da internet que possam causar prejuízo à rede, com intuito de manter a disponibilidade do serviço e as atividades da Justiça Federal da 3.ª Região, respeitada a privacidade individual no que esta não colida com as disposições desta política de segurança.

05 - O recebimento de arquivos da Internet (download) deverá ser restrito para assuntos relacionados às atividades laborais e está sujeito ao exame por sistema de detecção de artefatos maliciosos para afastar a presença de ameaças.

06 - Cabe à SETI implantar os controles de acesso e mecanismos de monitoramento que garantam a aplicação deste módulo.

MÓDULO 5: **PROTEÇÃO**

01 - A SETI deverá estabelecer medidas:

a) para proteção dos sistemas, que evitem o acesso indevido e a modificação não autorizada de dados ou informações armazenadas, em processamento ou em trânsito, abrangendo inclusive a segurança das documentações, comunicações e dos equipamentos;

b) visando à adoção de tecnologias e mecanismos que viabilizem a oferta de serviços de sigilo, a validade, a autenticidade, a integridade de dados, a irrevogabilidade e a irretratabilidade das transações eletrônicas que o exigirem e das aplicações de suporte que possam demandar o uso de criptografias, certificados e assinaturas digitais, devidamente credenciadas.

c) para garantir a segurança das instalações, em conjunto com a SSEG.

01.1 - As condições de proteção a serem estabelecidas deverão observar a possibilidade de prevenir, detectar, deter e documentar eventuais ameaças ao longo do ciclo de vida da informação.

02 - Será restrito o acesso:

a) às áreas reservadas para as Centrais de Processamento de Dados ou que abriguem processadores, consoles, periféricos, bem como outros equipamentos pertencentes ao parque de TI, destinadas ao desenvolvimento, à produção e à administração de dados e redes;

b) às salas que abriguem equipamentos de infraestrutura elétrica e lógica que sustentem o processamento e a comunicação de dados, tais como racks, switches, geradores elétricos e nobreaks, bem como os sistemas de climatização e de detecção e de extinção de incêndios das salas.

03 – O acesso será permitido a:

a) servidores autorizados pelos respectivos setores de TI;

b) terceiros autorizados pela SETI, identificados e acompanhados pelos servidores autorizados.

04 - Os técnicos e demais usuários autorizados deverão se desconectar e/ou encerrar a sessão no sistema operacional depois de concluídas suas atividades, observando o mesmo procedimento quando deixarem as salas referidas no item 02.

05 - Dados estruturados e informações extraídas dos sistemas somente podem ser fornecidos mediante aprovação do gestor do sistema.

06 - Todas as estações de trabalho e servidores da Justiça Federal da 3.ª Região, em que o Sistema Operacional seja vulnerável a ataques por vírus, deverão possuir, instalado e atualizado, o antivírus corporativo.

MÓDULO 6: **MANUTENÇÃO**

01 - São condições para garantir a preservação e o funcionamento ininterrupto dos equipamentos:

a) infraestrutura ambiental (temperatura e umidade controladas);

b) infraestrutura elétrica (rede certificada, com dimensionamento adequado e previsão para quedas de energia, com estabilizadores, geradores elétricos e nobreak);

c) plano de execução periódica de backup para todos os repositórios de informação;

d) plano de contingência e plano de continuidade de TI, para controle de interrupções dos sistemas e prevenção da continuidade dos serviços de TI, minimizando riscos e falhas que afetem a operação dos sistemas;

e) replicação de informações, espelhamento, redundância de hardware e estratégia de site-backup;

f) monitoração física, ambiental e de operação; e

g) manutenção adequada e preventiva de todos os componentes de hardware e software.

02 - A manutenção de todo e qualquer recurso de hardware, bem como dos softwares e sistemas instalados, pertencentes ao patrimônio da Justiça Federal da 3.ª Região, somente poderá ser efetuada por técnicos devidamente autorizados pelos respectivos setores de Tecnologia da Informação.

02.1 - Interrupções de energia elétrica, programadas ou não, que impactem o funcionamento de recursos centrais e interfiram na operação de sistemas deverão ser informadas à SETI para as providências necessárias. As interrupções programadas devem ser comunicadas previamente.

02.2 - Fica vedado o suporte, a manutenção, a configuração, a instalação ou qualquer intervenção técnica em recursos de hardware e software não pertencentes ao patrimônio da Justiça Federal da 3.ª Região.

02.3 - O suporte prestado pela SETI aos sistemas disponíveis na internet e extranet ficará restrito à verificação da disponibilidade de funcionamento e operação, bem como orientações sobre os requisitos para utilização dos sistemas.

02.3.1 - Dúvidas quanto às funcionalidades e uso dos sistemas são de responsabilidade do gestor ou comitê gestor do sistema nos termos da Resolução PRES n.º 293/2012, art. 4.º, inciso XVI.

03 - O procedimento de manutenção deverá ser devidamente documentado e aprovado, de acordo com o processo de gerenciamento de mudanças, excetuando-se os equipamentos de microinformática.

MÓDULO 7: **GESTÃO E UTILIZAÇÃO**

01 - Compete à Secretaria de Tecnologia da Informação:

a) providenciar a instalação, configuração e manutenção preventiva e corretiva dos equipamentos de TI, sendo expressamente vedada a realização de tais tarefas por pessoas não autorizadas;

b) controlar e estabelecer procedimentos operacionais para o uso de equipamentos de TI;

c) propor normatização para o uso de equipamentos de TI, com posterior análise da Comissão de Informática e deliberação da Presidência.

02 - A fim de garantir o funcionamento dos sistemas, bem como otimizar o uso dos recursos humanos disponíveis para manutenção e sustentação dos recursos de TI, as estações de trabalho fornecidas devem manter as configurações de hardware e software padronizadas pela SETI.

03 - Fica proibido o acréscimo ou instalação de recursos de hardware e software não pertencentes ao patrimônio da Justiça Federal da 3.ª Região. As exceções deverão ser submetidas à avaliação da SETI, com posterior encaminhamento à Comissão de Informática e aprovação da Presidência.

03.1 - A SETI deverá obter parecer técnico da área de segurança da informação, para encaminhamento à Comissão de Informática.

03.2 - A fim de serem admitidos na rede de dados da Justiça Federal da 3.ª Região, os computadores e dispositivos móveis, pertencentes ou não ao patrimônio da Justiça Federal, serão submetidos ao procedimento de homologação e validação de requisitos mínimos de segurança.

03.2.1 - A SETI providenciará meios para homologação e validação dos requisitos mínimos de segurança.

03.3 - Os softwares, ferramentas e bibliotecas de desenvolvimento e soluções alternativas em fase de homologação, serão instalados pela SETI em ambiente próprio para a homologação.

03.4 - O recebimento, seja por meio de doação ou cessão, de equipamentos de TI, oriundos de órgãos externos, deve ser precedido de análise e manifestação da SETI quanto à viabilidade de uso, integração, administração, gerenciamento e sustentação em relação às tecnologias já empregadas pela Justiça Federal da 3.ª Região.

04 - O descarte de equipamentos e mídias magnéticas ou digitais, assim como a cessão ou doação a terceiros, deve seguir as diretrizes apontadas pela SETI, visando garantir a sanitização prévia, observados os preceitos normativos afetos à gestão de resíduos sólidos.

05 - Quando possível, os recursos de hibernação e de suspensão serão habilitados nas estações de trabalho, de forma a economizar energia elétrica.

MÓDULO 8: **DEVERES DOS USUÁRIOS**

01 - Constituem deveres dos usuários:

a) zelar pela correta utilização dos recursos de TI;

b) utilizar os recursos de TI exclusivamente para atividades desenvolvidas pela Justiça Federal da 3.ª Região, vedado o uso para fins particulares;

c) acatar as normas e os procedimentos operacionais para o uso dos recursos de TI;

d) zelar pela integridade, segurança e vida útil dos equipamentos, evitando quedas, contato com líquidos ou alimentos de qualquer natureza e desligamento de forma brusca, sem necessidade;

e) realizar procedimentos básicos de segurança, tais como backup de arquivos armazenados localmente;

f) manter o sigilo da senha de acesso, proceder frequentemente à sua atualização, seguindo as diretrizes apontadas pela SETI;

g) abrir chamado no callcenter de informática previamente ao deslocamento de equipamentos de TI, exceto para dispositivos móveis, para análise de possíveis impactos;

h) não abrir e-mail ou seus anexos quando a origem ou conteúdo forem duvidosos, enviando-o à CLRI para averiguação;

i) efetuar as atualizações programadas dos sistemas em seus equipamentos, conforme procedimento definido pela SETI;

j) conectar o notebook institucional à rede de dados da Justiça Federal da 3.ª Região no mínimo mensalmente, para que o equipamento receba as atualizações de softwares de antivírus e políticas de segurança, mantendo-o dentro das condições técnicas de uso.

02 - Fica expressamente proibido aos usuários:

a) remover, transferir, emprestar, modificar ou proceder qualquer alteração na característica física ou técnica dos equipamentos;

b) compartilhar unidades de armazenamento local de informações em rede com outros usuários, tais como: disco rígido interno ou externo, CD/DVD, entre outros e impressoras sob o risco de violação de segurança;

c) executar ou configurar os recursos computacionais com a intenção de facilitar o acesso a usuários não autorizados;

d) criar ou propagar vírus, danificar equipamentos, serviços e arquivos;

e) obter acesso não autorizado aos sistemas;

f) copiar, transferir ou emprestar direitos de uso de softwares para qualquer que seja a finalidade sem a devida formalização legal;

g) usar, instalar, executar, copiar ou armazenar aplicativos, programas ou qualquer outro material que não estejam devidamente licenciados ou autorizados pela SETI;

h) ceder ou emprestar o dispositivo que armazena certificados digitais e chaves privadas (*"token"* ou cartão inteligente) e/ou as respectivas senhas a terceiros, ainda que agentes públicos da Justiça Federal.

MÓDULO 9: **AQUISIÇÕES E CONTRATAÇÕES DE SISTEMAS**

01 - As aquisições e contratações de sistemas na Justiça Federal da 3.ª Região deverão seguir o MCTI-JF (Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal), regulamentado pela Resolução n.º 279/2013 do Conselho da Justiça Federal e seus documentos acessórios.

02 - Todo e qualquer sistema ou software, independentemente de seu porte ou de sua complexidade, somente poderá ser adquirido, customizado e/ou instalado após aprovação da SETI, ficando vedado o uso de cópias ilegais ou programas de terceiros (inclusive de servidores), ainda que legalizados.

02.1 - É vedado o uso de softwares não homologados pela SETI, ainda que de licenças gratuitas (freeware, open source, etc.).

MÓDULO 10: **DESENVOLVIMENTO, IMPLANTAÇÃO E MANUTENÇÃO DE SISTEMAS**

01 - O desenvolvimento de melhorias, novas funcionalidades e a manutenção de sistemas, já existentes ou novos, na Justiça Federal da 3.ª Região segue o procedimento estabelecido pela Instrução Normativa 37-04, implantada pela Resolução PRES n.º 424/2015, bem como as diretrizes definidas na Política de Segurança para Desenvolvimento, Aquisição e Manutenção de Sistemas, estabelecida pela Portaria CJF n.º 104, de 6 de março de 2015.

02 - A administração dos sistemas em uso na Justiça Federal da 3.ª Região cabe aos gestores dos sistemas, conforme regulamentado pela Resolução PRES n.º 293/2012.

03 - Os sistemas que vierem a ser criados e que possam interessar à Justiça Federal da 3.ª Região, desenvolvidos por servidores ou terceiros da 3.ª Região, externos à SETI, deverão ser submetidos à análise e aos testes da aludida secretaria.

03.1 - Na análise deverão ser apresentados os respectivos programas-fonte, a documentação técnica e o manual do usuário.

03.2 - O sistema, se aprovado, só terá sua instalação efetivada mediante cessão de uso e autorização de seu(s) autor(es), após o que passarão a pertencer ao acervo da Justiça Federal da 3.ª Região.

03.3 - Nesse caso, sempre que necessário, o(s) autor(es) poderá(ão) ser convocado(s) para possíveis manutenções e/ou instalações dos respectivos sistemas.

04 - Os ambientes lógicos de desenvolvimento de sistemas e de produção deverão ser segregados e possuir acesso controlado e restrito, com o devido controle de versão dos programas.

05 - A cessão de fontes ou documentação de sistemas a órgãos externos somente poderá ser efetuada mediante autorização da Presidência do TRF 3.ª Região.

06 - A implantação de sistemas cedidos por outros órgãos à Justiça Federal da 3ª. Região deve ser precedida de avaliação da futura área gestora do sistema, bem como avaliação técnica da SETI, e, após assinatura de termo de convênio ou acordo de cooperação técnica, com a especificação das responsabilidades das partes envolvidas.

07 - A SETI deverá zelar pela implementação, nos sistemas e na configuração de servidores, de controles de segurança necessários para proteger os ativos de informação, de acordo com a sua criticidade.

07.1 - A criticidade da informação será definida pelo gestor do sistema.

07.2 - Os controles de segurança devem abordar:

a) restrição de acesso às áreas, aos arquivos e conteúdos sensíveis, sem a devida autenticação;

b) impedimento de inserção de comandos de recuperação de dados e metadados para adulteração ou roubo de informação;

c) impedimento de “personificação” de páginas dos sítios da Justiça Federal da 3.ª Região;

d) proteção de senhas, endereços e demais informações sensíveis de forma a impossibilitar engenharia reversa por terceiros; e

e) criptografia das informações trafegadas.

07.3 - A autenticação aos sistemas mediante uso de login e senha deve, preferencialmente, utilizar comunicação segura.

MÓDULO 11: **INTEGRAÇÃO**

01 - A integração com outros órgãos, sempre que possível, seguirá os padrões estabelecidos pelo Modelo Nacional de Interoperabilidade - MNI, definido pelo Conselho Nacional de

Justiça.

02 - O fornecimento contínuo e periódico de dados estruturados a outras instituições somente poderá ser realizado mediante assinatura de termo de convênio/acordo de cooperação entre as instituições.

MÓDULO 12: **MEDIDAS EDUCACIONAIS**

01 - A Justiça Federal da 3.ª Região promoverá ações de divulgação, conscientização e capacitação dos usuários, em especial para os ingressantes em seus quadros, sejam magistrados ou servidores, visando aprimorar a utilização de recursos de TI.

02 - Caberá aos responsáveis das respectivas unidades administrativas incentivar e apoiar às práticas de treinamento e autodesenvolvimento de seus funcionários.

MÓDULO 13: **DISPOSIÇÕES FINAIS**

01 - As avaliações de conformidade em TI serão executadas em periodicidade a ser definida pela SETI, ou a qualquer tempo, levando-se em consideração a complexidade do sistema ou do serviço auditado, a sua importância e os dados que utiliza, sem prejuízo das auditorias da UCON.

02 - As avaliações serão exercidas por profissionais da SETI, podendo ser servidores ou terceiros contratados, especialmente designados para esse trabalho.

02.1 - Poderão ser convocados servidores das demais unidades da Justiça Federal da 3.ª Região para auxiliar nos trabalhos.

03 - Fica autorizada a utilização de software destinado às funções de avaliação, incluindo ferramentas de verificação de vulnerabilidade de segurança.

04 - Os casos omissos serão submetidos à CLSI.

05 - O descumprimento das normas estabelecidas nesta Instrução Normativa implicará responsabilidade civil, penal e administrativa dos que estiverem envolvidos na violação em referência.