PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 231/2013 (*)

Aprova a Norma Complementar de Controles de Acesso Relativos à Segurança da Informação e Comunicações.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais;

CONSIDERANDO as boas práticas de Governança de TI que visam garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a necessidade de sistematizar a concessão de acesso a usuários, a fim de evitar a quebra de segurança da informação e comunicações;

CONSIDERANDO que a identificação, a autorização e o interesse do usuário do serviço são condicionantes prévias para a concessão de acesso aos ativos e aos serviços de Tecnologia da Informação;

CONSIDERANDO a identificação dos controles de acesso lógico e físico como consequência do processo de gestão de riscos de segurança da informação e comunicações;

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 05/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre os controles de acesso relativos à segurança da informação e comunicações, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 29 de maio de 2013.
MARIA ROSELI MENDES ALENCAR
Presidente

(*) Revogado pelo ATO TRT7.GP Nº 65/2020 Disponbilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2989, 08 jun. 2019. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013. Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 1.

~~Anexo~~

Revogado pelo ATO TRT7.GP Nº 65/2020

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação Escritório de Segurança da Tecnologia da Informação	Número da Norma Complementar	Revisão	Emissão	Folha
	05/NC/STI/SESEG	00	00/00/00	1/1
	Controles de Acesso Relativos à Segurança da Informação e Comunicações.			

1 OBJETIVO

Estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações do Tribunal Regional do Trabalho da 7ª Região.

2 CONSIDERAÇÕES INICIAIS

2.1 O objetivo do controle é sistematizar a concessão de acesso, a fim de evitar a quebra de segurança da informação e comunicações.

2.2 A identificação, a autorização, a autenticação, o interesse do serviço e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos Ativos e Serviços de tecnologia da Informação do Tribunal Regional do Trabalho da 7ª Região.

2.3 A identificação dos controles de acesso lógico e físico, do Tribunal Regional do Trabalho da 7ª Região, é consequência do processo de Gestão de Riscos de Segurança da Informação e Comunicações.

2.4 A implementação dos controles de acesso está condicionada à prévia aprovação pela autoridade responsável do Tribunal Regional do Trabalho da 7ª Região.

2.5 Para implementar os controles de acesso aprovados é fundamental a elaboração e divulgação de normas, bem como programas periódicos de sensibilização e conscientização em conformidade com a Política de Segurança Institucional do Tribunal Regional do Trabalho da 7ª Região.

2.6 O Tribunal Regional do Trabalho da 7ª Região, através do Escritório de Segurança de TI, estabelecerá regras específicas para credenciamento de acesso de usuários aos ativos de informação em conformidade com a legislação vigente, e em especial quanto ao acesso às informações em áreas e instalações consideradas críticas.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1 Item I, Art. 3º, do Decreto nº 3.505, de 13 de Junho de 2000, que institui a Política de Segurança da Informação nos Órgãos da Administração Pública Federal, que estabelece "*dotar os órgãos e as entidades da Administração Pública Federal* de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis".

3.2 Cobit 4.1, DS 5.3, Gestão de Identidade, "*Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo.".*

3.3 Cobit 4.1, DS 5.4, Gestão de Contas de Usuários, "*Assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário.".*

3.4 Cobit 4.1, DS 12.2, Medidas de Segurança Física, "*Definir e implementar medidas de segurança física alinhadas com os requisitos de negócio para proteger o local e os ativos físicos.*".

3.5 Cobit 4.1, DS 12.3, Acesso Físico, "*Definir e implementar procedimentos para conceder, limitar e revogar o acesso a instalações, prédios e áreas de acordo com as necessidades do negócio, inclusive em situações de emergências.*

3.6 ABNT NBR ISO/IEC 27002:2005, Código de prática para a gestão de segurança de informação, Capitulo 11, "*Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação. Convém que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação".*

3.7 Art. 10, da Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, estabelece que "*a estrutura organizacional, o quadro de pessoal, a gestão de ativos e os processos do setor responsável pela gestão de trabalho da área de TIC do Tribunal deverão estar adequados às melhores práticas preconizadas pelos padrões nacionais e internacionais para as áreas de governança e de gerenciamento de serviços de TIC".*

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

a) acesso - ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

b) ativo de informação - aquilo que tem valor, seja tangível ou intangível, tais como informações, *software,* equipamentos, instalações, serviços, pessoas e imagem institucional;

c) controle de acesso - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou excluir acesso;

d) credenciamento - processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

e) credenciais ou contas de acesso - permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

f) extranet - ambiente de rede de computadores com acesso permitido aos usuários por meio da Internet;

g) gestão de riscos de segurança da informação e comunicações - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

h) intranet - ambiente de rede de computadores composta pelo conjunto de redes locais e recursos computacionais utilizados para sua formação;

i) necessidade de conhecer - condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação;

j) perfil de acesso - conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

k) quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações;

l) termo de responsabilidade - termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso (Modelo - Anexo A);

m) usuário - magistrados, servidores ocupantes de cargo efetivo ou cargo em comissão, requisitados e cedidos, funcionários de

empresas prestadoras de serviços terceirizados, consultores, estagiários, pensionistas, bem como Magistrados e servidores inativos que estão autorizados a obter acesso a informações e sistemas.

5 CONTROLE DE ACESSO LÓGICO

5.1 Quanto à criação e administração de contas de acesso:

a) quando do primeiro ingresso do usuário no Tribunal Regional do Trabalho da 7ª Região a Secretaria de Gestão de Pessoas deverá abrir uma requisição junto a Central de Serviços da Secretaria de Tecnologia da Informação, para criação de conta de acesso para o usuário que ingressar, informando:

- nome completo,
- nome do cargo,
- lotação,
- CPF;

b) o acesso aos ativos de informação será disponibilizado para usuários autorizados, com a utilização de identificador e senha concedidos por este Tribunal e assinatura de Termo de Responsabilidade (Anexo I) na forma desta Norma Complementar;

c) será adotado no identificador o prenome e o último ou penúltimo sobrenome do usuário, separados pelo sinal do ponto, em letras minúsculas, sem a utilização de agnomes, acentos, cedilhas ou caracteres especiais;

d) é vedada a utilização de apelidos no identificador do usuário, bem como de abreviaturas ou de variações do prenome ou sobrenome que não sejam condizentes com a sua identidade;

e) excepcionalmente, no caso de homônimos ou desde que justificável, poderá ser adotada forma diferente da estabelecida neste artigo no identificador do usuário;

f) o identificador e senha de acesso são pessoais e intransferíveis;

g) a senha de acesso cadastrada pelos usuários terá o tamanho mínimo de oito caracteres alfanuméricos, cabendo à Secretaria de Tecnologia da Informação impedir a utilização daquelas de fácil dedução;

h) a senha de acesso deverá ser alterada a cada noventa dias, ocasião em que um histórico impedirá a repetição das duas últimas senhas utilizadas;

i) a senha de acesso será bloqueada após três tentativas sem sucesso de acesso aos ativos de informação;

j) em caso de bloqueio ou perda da senha por parte do usuário, a sua recuperação somente se dará mediante requisição feita pela chefia imediata à Central de Serviços da Secretaria de Tecnologia da Informação;

k) o acesso de que trata este Item será concedido, segundo o perfil de cada usuário, nos seguintes níveis:

- Nível 1 - acesso à Intranet, o qual compreende a utilização dos sistemas administrativos e judiciários,
- Nível 2 - além da permissão do Nível 1, acesso à Extranet e à Internet, o qual compreende a navegação em documentos de hipertexto,
- Nível 3 - além das permissões dos Níveis 1 e 2, acesso ao Serviço de e-mail,
- Nível 4 - além das permissões dos Níveis 1, 2 e 3, acesso ao Serviço de Mensagens Instantâneas,
- Nível 5 - além das permissões dos Níveis 1, 2, 3 e 4, acesso aos sistemas de desenvolvimento e serviços de administração remota ou local dos recursos de informática;

l) o Nível 1 de acesso será concedido observando-se qual sistema administrativo ou judiciário o usuário necessita utilizar;

m) aos magistrados será concedido o Nível 4 de acesso para o desempenho de suas atividades;

n) o Nível 5 de acesso é restrito à Secretaria de Tecnologia da Informação;

o) o Procurador do Trabalho, durante as Sessões do Tribunal Pleno e das Turmas, terá garantido o acesso à Internet e ao Sistema de Sala de Sessões, observadas, em ambos os casos, as regras estabelecidas nesta Resolução;

p) o identificador e senha de acesso, quando concedidas aos estagiários e empregados terceirizados, serão utilizadas de modo restrito às atividades por eles desenvolvidas e limitadas ao Nível 2 de acesso;

q) poderá ser concedido acesso temporário aos Ativos de Informação a servidores pertencentes a outros Órgãos Públicos ou funcionários de empresas prestadoras de serviços, quando em atividade junto a este Tribunal;

r) responde pelo acesso feito em desacordo com esta Norma Complementar o usuário que o tenha realizado e, solidariamente, o responsável pela unidade organizacional onde ocorrer a infração;

s) a Secretaria de Gestão de Pessoas comunicará mensalmente as aposentadorias, falecimentos, remoções, cessões, promoções, designações e exonerações de magistrados ou servidores para que sejam providenciados pela Central de Serviços os ajustes necessários nos perfis de acesso;

t) compete aos responsáveis pelas Unidades Organizacionais comunicar à Central de Serviço o desligamento de estagiários ou empregados terceirizados sob sua responsabilidade, desde que os mesmos possuam acesso aos Ativos de Informação.

6 CONTROLE DE ACESSO FÍSICO

6.1 Quanto às áreas e instalações físicas:

a) o acesso físico à sala cofre e aos demais espaços destinados aos equipamentos computadores servidores, bastidores ou racks de equipamentos de rede lógica e comunicação deste Tribunal é restrito ao pessoal da Divisão de Infraestrutura de TI, da Secretaria de Tecnologia da Informação;

b) o acesso às áreas referidas neste item por pessoas estranhas à Divisão de Infraestrutura de TI somente poderá ser feito com a necessária autorização e mediante designação de acompanhante;

c) não será permitido o uso de câmeras fotográficas de qualquer espécie e gravadores de vídeo ou áudio nos locais indicados no caput deste artigo, salvo se for autorizado pela Secretaria de Tecnologia da Informação;

d) o Diretor da Secretaria de Tecnologia da Informação poderá limitar, mediante portaria, o acesso de pessoas estranhas à Secretaria de Tecnologia da Informação aos espaços destinados ao desenvolvimento de sistemas de tecnologia da informação e à manutenção de equipamentos de informática.

7 VIGÊNCIA

7.1 Esta Norma Complementar entra em vigor na data de sua publicação.

7.2 Fica estabelecido um prazo de 120 dias para a STI entrar em conformidade com a norma para que as contas de usuários fiquem de acordo com o padrão.

8 ANEXO
Modelo de Termo de Responsabilidade

Poder Judiciário
Justiça do Trabalho
Tribunal Regional do Trabalho da 7ª Região

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF nº _____, identidade nº _____, expedida pelo _____, em _____, e lotado no(a) _____ (Nome do órgão ou entidade), DECLARO, sob pena das sanções cabíveis nos termos da _____ (legislação vigente) que assumo a responsabilidade por:

I) tratar o(s) ativo(s) de informação como patrimônio do (Nome do órgão ou entidade);

II) utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do (Nome do órgão ou entidade);

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

IV) utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do (Nome do órgão ou entidade);

V) responder, perante o (Nome do órgão ou entidade), pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Fortaleza, CE, _____de _____de _____ .

_____
Assinatura
Nome do usuário e seu setor organizacional

_____
Assinatura
Nome da autoridade responsável pela autorização do acesso