TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO
Gabinete da Presidência

RESOLUÇÃO GP N. 7, DE 21 DE NOVEMBRO DE 2014

Institui a Política de Segurança da Informação e Comunicação (POSIC-TRT3) no âmbito do Tribunal Regional do Trabalho da 3ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as disposições do Decreto n. 3.505, de 13 de junho de 2000, sobre Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO o art. 13 da Resolução n. 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça (CNJ), que incumbiu ao Comitê Gestor de cada tribunal elaborar e aplicar a respectiva Política de Segurança da Informação alinhada às diretrizes nacionais;

CONSIDERANDO as Diretrizes para a Gestão de Segurança da Informação no âmbito do Poder Judiciário, emanadas do CNJ;

CONSIDERANDO a Resolução n. 99, de 24 de novembro 2009, do CNJ, que, ao instituir o Planejamento Estratégico de Tecnologia da Informação e Comunicação no âmbito do Poder Judiciário, assentou a promoção da segurança da informação como objetivo estratégico, com determinação de associá-la a indicador de resultado, metas, projetos e ações;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

CONSIDERANDO o Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) desta 3ª Região estabelecer como indicador de resultado do mencionado objetivo o índice de aderência às políticas de segurança definidas;

CONSIDERANDO a Portaria GP/DG n. 74, de 17 de março de 2014, que, ao constituir o Comitê Gestor de Segurança da Informação (CGSI) para o biênio 2014-2015, incumbiu-o de propor a Política de Segurança da Informação e Comunicação do TRT da 3ª Região (POSIC-TRT3), bem como normas correlatas; e

CONSIDERANDO, dentre outros, os Projetos 5 - Implantação das melhores práticas de governança de TIC e 46 - Política de Segurança da Informação, respectivamente, do PETIC e do Planejamento Estratégico (Plano Plurianual 2010-2014) deste Tribunal,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSIC-TRT3).

Parágrafo único. Integram a POSIC-TRT3 normas e procedimentos complementares voltados para a proteção de informações, que serão aplicados aos magistrados, servidores, estagiários, empregados de empresas contratadas ou conveniadas, bem como usuários externos públicos ou privados.

Seção I
Dos Conceitos

Art. 2º Para os efeitos desta Resolução considera-se:

I - autenticidade: garantia de veracidade da fonte das informações;

II - confidencialidade: princípio de segurança da informação que garante acesso à informação apenas a usuários autorizados;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

III - disponibilidade: princípio de segurança da informação que garante acesso à informação por usuário autorizado quando necessário;

IV - informação: conjunto de dados, textos, imagens, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto;

V - integridade: princípio de segurança da informação que garante que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

VI - recurso de tecnologia da informação e comunicação: conjunto de componentes físicos ou lógicos que compõem soluções e aplicações de Tecnologia da informação; e

VII - segurança da informação: conjunto de medidas voltadas para a proteção de informações, com foco em preservação da confidencialidade, integridade, disponibilidade e autenticidade, além de garantia da continuidade dos serviços.

Seção II
Dos Princípios

Art. 3º Toda informação gerada, recebida, adquirida, armazenada, processada, transmitida ou descartada, em meio físico ou virtual, por este Tribunal, deve ser protegida por mecanismos adequados, de acordo com a respectiva confidencialidade, integridade, disponibilidade e autenticidade.

Parágrafo único. Os recursos de tecnologia da informação e comunicação disponibilizados devem ser utilizados para atividades profissionais pertinentes à execução de serviços e ao cumprimento da missão institucional.

Seção III
Das Diretrizes

Art. 4º O Comitê Gestor de Segurança da Informação (CGSI) regulamentará, por meio de atos normativos específicos, os seguintes temas:

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

I - tratamento da informação;

II - tratamento de incidentes de segurança da informação;

III - gestão de risco;

IV - gestão de continuidade;

V - auditoria, monitoramento e controle de recursos tecnológicos;

VI - acesso lógico;

VII - acesso físico;

VIII - internet; e

IX - correio eletrônico corporativo.

Parágrafo único. O Comitê Gestor poderá designar grupo de trabalho para elaborar proposta de regulamentação dos temas indicados no caput deste artigo, conforme diretrizes estabelecidas nas Subseções da Seção III desta Resolução.

Subseção I
Do Tratamento da Informação

Art. 5º Este Tribunal é responsável por informações geradas em seu âmbito, independente da forma de apresentação ou armazenamento, incumbindo-lhe custodiá-las em ambiente propício à adequada proteção e preservação.

Art. 6º A informação utilizada, armazenada, processada ou transmitida pelas unidades organizacionais deste Regional deverá ter o acesso controlado, de

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

acordo com a respectiva classificação de segurança.

Parágrafo único. O descarte de informações observará os prazos prescritos nos instrumentos de gestão documental, devendo ser realizado em conformidade com a segurança e a proteção requeridas pela respectiva classificação de segurança.

Subseção II
Do Tratamento de Incidentes de Segurança da Informação

Art. 7º Incidente de segurança da informação é qualquer evento relacionado à segurança de sistemas de computação ou de redes de computadores, confirmado ou sob suspeita, que:

I - viole a Política de Segurança da Informação e Comunicação deste Tribunal;

II - comprometa disposições normativas deste Regional ou diretrizes governamentais;

III - esteja em desconformidade com a legislação sobre a matéria; e

IV - represente ameaça à disponibilidade de serviços, bem como exponha ou facilite acesso não autorizado às informações sob a guarda deste Tribunal.

Parágrafo único. Os eventos indesejados ou inesperados, que tenham probabilidade de comprometer operações e ameaçar a segurança da informação do Tribunal, são considerados incidentes de segurança da informação e devem ser reportados à Central de Serviços de TIC.

Subseção III
Da Gestão de Risco

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

Art. 8º A unidade gestora de Segurança da Informação realizará, periodicamente, análises de risco para identificar vulnerabilidades e ameaças potenciais, com o objetivo de manter a qualidade da segurança da informação ao longo do tempo.

Parágrafo único. Os resultados de cada análise serão compilados em relatório gerencial, contendo descritivo dos riscos identificados, respectivas classificações e ações recomendadas, a ser apresentado ao CGSI.

Subseção IV
Da Gestão de Continuidade

Art. 9º Caberá à unidade gestora de Segurança da Informação a gestão do processo de continuidade do serviço de TI, com o objetivo de reduzir impactos decorrentes de interrupção de serviço causada por desastre ou falha de segurança, por intermédio de ações de prevenção, resposta e recuperação.

Subseção V
Da Auditoria, do Monitoramento e do Controle de Recursos Tecnológicos

Art. 10. Incumbe à Diretoria da Secretaria de Coordenação de Informática registrar e monitorar o uso de recursos tecnológicos, com o intuito de detectar e evidenciar incidentes de segurança.

§ 1º As auditorias sobre recursos tecnológicos deste Tribunal serão:

I - ordinárias, realizadas periodicamente, para avaliar a conformidade técnica de serviços, ferramentas e equipamentos; e

II - extraordinárias, realizadas por solicitação, para apurar eventos que exponham a segurança de ativos de informação e boas práticas de utilização do ambiente informatizado.

§ 2º A solicitação de auditoria em incidente não previsto nesta Resolução

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

será analisada e deliberada pelo CGSI.

Subseção VI
Do Controle de Acesso

Art. 11. Os serviços de acesso à rede de computadores deste Tribunal abrangem computadores, estrutura de rede, intranet, internet, correio eletrônico e sistemas relacionados.

Art. 12. O acesso aos recursos de tecnologia da informação e comunicação será individual, pessoal e intransferível, autorizado pelo diretor responsável pela área de lotação.

§ 1º O usuário é responsável pela guarda e sigilo da respectiva senha e responderá por acesso realizado por meio de sua credencial (login).

§ 2º O acesso lógico aos recursos de tecnologia da informação e comunicação poderá exigir autenticação segura, por meio de credencial de acesso ou de certificação digital.

Subseção VII
Da Internet

Art. 13. O uso do serviço de internet corporativo deve estar associado às atividades deste Tribunal.

Parágrafo único. Os acessos serão monitorados e registrados para análise de segurança contra ameaças, roubo de dados e disseminação de conteúdos maliciosos.

Art. 14. O Comitê Gestor de Segurança da Informação, poderá autorizar o bloqueio de acesso a sítios externos, em função de:

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

I - conteúdo incompatível com as atividades profissionais;

II - desrespeito à legislação nacional; ou

III - risco à segurança da informação na rede de computadores do Tribunal.

Parágrafo único. Os acessos à internet serão monitorados para análises de segurança contra ameaças, roubo de dados e disseminação de conteúdos maliciosos.

Subseção VIII
Do Correio Eletrônico Corporativo

Art. 15. O uso do correio eletrônico corporativo deve estar associado às atividades deste Tribunal.

Art. 16. O uso não apropriado do correio eletrônico corporativo do Tribunal é passível de apuração de responsabilidade do usuário.

Parágrafo único. Por uso não apropriado considera-se o envio de mensagens de correio eletrônico contendo:

I - materiais obscenos, ilegais ou antiéticos;

II - materiais preconceituosos ou discriminatórios;

III - materiais caluniosos ou difamatórios;

IV - propagandas com objetivos comerciais;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

V - listas de endereços eletrônicos dos usuários do correio eletrônico corporativo do Tribunal;

VI - vírus ou qualquer programa danoso;

VII - material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

VIII - material protegido por leis de propriedade intelectual;

IX - entretenimento;

X - assuntos ofensivos;

XI - músicas, vídeos ou animações que não sejam de interesse específico do trabalho; ou

XII - spam (mensagem maliciosa em massa).

Art. 17. O endereço de correio eletrônico da unidade será de responsabilidade do respectivo gestor, admitindo-se delegação para operá-lo.

Seção IV
Da Utilização de Programas e Aplicativos

Art. 18. A instalação e a remoção de programas de computador em equipamento de informática do Tribunal serão realizadas, exclusivamente, mediante intervenção da DSCI.

Art. 19. A instalação e a utilização de programas de computador estão condicionadas à:

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

I - homologação pela área de TIC;

II - existência e disponibilidade de licenças de uso; e

III - conformidade com as atividades da Instituição e com a área de atuação das unidades.

Parágrafo único. É vedada a instalação de programa de computador cuja licença ou direito de uso não pertença à Instituição.

Seção V
Da Fundamentação Legal

Art. 20. A Política de Segurança da Informação e Comunicação desta 3ª Região tem por fundamentos:

I - Resolução n. 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça (CNJ), que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário;

II - Norma Complementar n. 03/IN01/DSIC/GSIPR, que estabelece diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

III - Lei n. 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

IV - ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;

V - ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

VI - ABNT NBR ISO/IEC 27005:2011 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação;

VII - Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), arts. 154-A, 154-B, 266, § 1º, 313-A, 313-B e 325, § 1º; e

VIII - Lei n. 8.112, de 11 de dezembro de 1990.

Seção VI
Das Penalidades

Art. 21. O descumprimento das disposições desta POSIC-TRT3 ou de normas específicas sobre segurança da informação sujeitam o infrator às penalidades previstas na legislação e nos regulamentos internos do Tribunal.

Parágrafo único. A inobservância desta Política por magistrado ou servidor poderá configurar infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Seção VII
Das Disposições Finais

Art. 22. A supervisão e o acompanhamento do cumprimento da POSIC-TRT3 incumbem à unidade gestora de segurança da informação.

Parágrafo único. No âmbito das respectivas competências, as unidades organizacionais deste Tribunal adotarão providências para a implementação da POSIC-TRT3.

Art. 23. O Comitê Gestor de Segurança da Informação e Comunicação determinará a revisão e a atualização periódicas das disposições da POSIC-TRT3.

Art. 24. Casos omissos e dúvidas sobre a aplicação da POSIC-TRT3

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.

serão submetidos ao Comitê Gestor de Segurança da Informação.

Art. 25. Esta Resolução entra em vigor na data de sua publicação.

MARIA LAURA FRANCO LIMA DE FARIA
Desembargadora Presidente

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 7, de 21 de novembro de 2014. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1629, 22 dez 2014. Caderno Administrativo, p. 12-17.