TRIBUNAL SUPERIOR DO TRABALHO
PRESIDÊNCIA

ATO Nº 764/GDGSET.GP, DE 27 DE NOVEMBRO DE 2012

Estabelece as diretrizes de segurança da informação no âmbito do Tribunal Superior do Trabalho.

O **PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO**, no uso de suas atribuições legais e regimentais,

Considerando o Ato TST.GP. nº 493/2009, que cria o Comitê Gestor de Segurança da Informação e define suas competências no âmbito do Tribunal Superior do Trabalho;

Considerando o Ato TST.GDGSET.GP. nº 86/2010, que define os papéis e as responsabilidades de Área Gestora, Gestor, Gerente e Operador de Sistemas Informatizados e de Bases de Dados no âmbito do Tribunal Superior do Trabalho;

Considerando que a NBR ISO/IEC 27002:2005, norma que estabelece boas práticas em segurança da informação, recomenda revisões periódicas da política de segurança da informação das instituições;

Considerando as recomendações da Secretaria de Fiscalização de Tecnologia da Informação referentes à segurança da informação publicadas nos acórdãos do Tribunal de Contas da União;

Considerando as melhores práticas para a proteção e controle da informação referenciadas nas disciplinas do COBIT, ITIL, NBR ISO/IEC 17799 e a família de normas NBR ISO/IEC 27000, seguidas pelas principais organizações e órgãos governamentais;

Considerando a necessidade de ampliar as diretrizes e os padrões de segurança para garantir um ambiente tecnológico controlado e seguro, de forma a oferecer as informações necessárias aos processos de trabalho deste Tribunal com integridade, confidencialidade e disponibilidade;

Considerando a necessidade de regular a concessão de acessos aos sistemas informatizados e à rede de computadores; o uso da Internet e seus recursos; a utilização do serviço de correio eletrônico corporativo; bem como o controle, monitoramento e auditoria de segurança da informação no âmbito do Tribunal;

Considerando os danos potenciais decorrentes da instalação de programas não homologados e inadequados, bem como o risco de disseminação de vírus de

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

computador a partir das estações de trabalho e de dispositivos móveis;

Considerando o contido no Processo Administrativo nº 500.459/2012-7;

RESOLVE:

Art. 1º. Este Ato define a Política de Segurança da Informação do Tribunal Superior do Trabalho, cabendo aos usuários a observância de suas disposições e às unidades administrativas, no âmbito de suas competências, a implementação e o acompanhamento de ações para a segurança da informação.

Art. 2º .Para efeitos deste aplicam-se as seguintes definições:

I – Confidencialidade: princípio de segurança da informação que garante o acesso à informação somente a usuários autorizados;

II – Integridade: princípio de segurança da informação que salvaguarda a exatidão e a completeza da informação e dos métodos de processamento;

III – Disponibilidade: princípio de segurança da informação que garante aos usuários autorizados acesso à informação e aos ativos correspondentes;

IV – Ativos de informação: patrimônio composto por pessoas, por elementos de infraestrutura tecnológica (hardware e software), bem como pelos dados e informações gerados e manipulados nos processos de trabalho do Tribunal;

V – Controle de acesso: conjunto de recursos que efetivam as autorizações e as restrições de acesso aos ativos de informação;

VI – Ambiente computacional ou informatizado: conjunto de recursos que utiliza ou disponibiliza serviços de tecnologia da informação e sistemas de informação do Tribunal;

VII – Análise de risco e vulnerabilidades: avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de sua ocorrência;

VIII – Usuários: conjunto composto por ministros, servidores, prestadores de serviço e estagiários no exercício de suas funções públicas, para fins de segurança da informação, que tenham acesso aos recursos de Tecnologia da Informação sob responsabilidade da SETIN, divididos da seguinte forma:

a. Usuário interno: ministro, servidor ativo ou unidade do Tribunal;

b. Usuário inativo: ministro aposentado, servidor aposentado ou pensionista;

c. Usuário colaborador: prestador de serviço terceirizado, estagiário ou outro colaborador do Tribunal;

d. Usuário externo: pessoa física ou jurídica;

IX – Sítio: é um conjunto de páginas web, isto é, de hipertextos acessíveis, geralmente, pelo protocolo HTTP ou HTTPS na Internet. Também conhecido por site, sítio na Internet, website, etc;

X – SPAM: termo usado para referir-se aos e-mails não solicitados e indesejados, que são enviados para um grande número de pessoas;

XI – Programa de computador: conjunto de instruções em linguagem natural ou codificada executado por computador; dispositivos; instrumentos ou equipamentos periféricos, baseados em técnica digital ou analógica, para fazê-los funcionar de modo e para fins determinados;

XII – Licença de uso: cessão de direito de utilização do programa de computador, outorgada pelo detentor dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado, mediante pagamento único ou periódico;

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

XIII – Programa de terceiro: programa que não foi elaborado por equipe de informática da SETIN;

XIV – Programa de livre distribuição: programa que oferece período de avaliação gratuito, após o qual é requerido pagamento pela licença de uso, ou que pode ser utilizado gratuitamente por tempo indeterminado.

XV – Vírus: programas criados para causar algum dano ao computador infectado, seja apagando dados, capturando informações ou alterando o funcionamento normal da máquina;

XVI – Conteúdo evasivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a saída de informações ou dados;

XVII – Conteúdo intrusivo: arquivo ou programa com artifícios capazes de burlar os mecanismos de segurança da informação estabelecidos no TST, permitindo a entrada de informações ou dados.

CAPÍTULO I
DO CONTROLE DE ACESSO À REDE DE COMPUTADORES

Art. 3º. Os serviços de acesso à rede de computadores do Tribunal abrangem: estrutura de diretórios de rede, Intranet, Internet e correio eletrônico.

§ 1º O acesso padrão à rede de computadores do Tribunal é assim regulado:

I – Para usuário interno: será facultado o acesso a toda rede de computadores do Tribunal;

II – Para usuário inativo: será permitido o acesso à Intranet;

III – Para usuários colaboradores e externos: será facultado o acesso à rede de computadores do Tribunal e o envio e recebimento de mensagens eletrônicas internas, sendo vedada a utilização de Internet e o envio ou o recebimento de mensagens externas de correio eletrônico.

§ 2º Em casos de comprovada necessidade de serviço, o responsável pela unidade poderá solicitar à SETIN, motivadamente, acesso à Internet ou o envio e recebimento de mensagens externas de correio eletrônico para usuários colaboradores e externos.

Art. 4°. A solicitação de concessão de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço.

§ 1° Na solicitação de acesso à rede de computadores do Tribunal para usuários internos, constará nome completo e código do usuário interessado, bem como os serviços solicitados, conforme descritos no art. 3º.

§ 2° No caso de usuários colaboradores ou externos, a solicitação conterá ainda o tempo de validade do acesso à rede de computadores do Tribunal, sendo o limite a duração do estágio ou do contrato.

§ 3° A SETIN poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso concedido ao usuário.

Art. 5º. O acesso à rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Capítulo X deste Ato.

Art. 6°. O acesso à rede de computadores do Tribunal e seus serviços dar-se-á pela combinação nome de usuário e senha, que é pessoal e intransferível.

§ 1° A senha deverá ter um tamanho mínimo de 6 (seis) caracteres alfanuméricos, devendo ser evitada aquela de fácil dedução.

§ 2° A senha de acesso à rede de computadores do Tribunal será alterada com a periodicidade de 45 (quarenta e cinco) dias.

§ 3° O sistema impedirá o usuário de reutilizar as suas 5 (cinco) últimas senhas.

Art. 7°. A solicitação de revogação de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço, quando houver o desligamento do usuário de sua unidade.

CAPÍTULO II
DO CONTROLE DE ACESSO AOS SISTEMAS INFORMATIZADOS E AOS BANCO DE DADOS

Art. 8º. A solicitação de concessão de acesso aos sistemas informatizados do Tribunal será encaminhada pelo responsável da unidade ao gestor do respectivo sistema.

§ 1° Na solicitação de acesso aos sistemas informatizados do Tribunal, deverá constar nome completo e código do usuário interessado, bem como o tipo de acesso a ser concedido.

§ 2° No caso de usuários colaboradores ou externos, a solicitação deverá conter ainda o tempo de validade do acesso aos sistemas informatizados do Tribunal, sendo o limite a duração do estágio ou do contrato.

Art. 9º. O acesso aos sistemas informatizados e aos bancos de dados será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 10. A solicitação de revogação de acesso aos sistemas informatizados do Tribunal será realizada pelo responsável da unidade ao gestor do sistema, quando houver o desligamento do usuário de sua unidade.

Art. 11. Os servidores lotados na Coordenadoria de Desenvolvimento de Sistemas da SETIN poderão ter acesso aos sistemas em produção e aos bancos de dados para realizar manutenções, mediante autorização expressa do gestor do sistema.

Art. 12. O gestor do sistema poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso do usuário ao sistema informatizado do Tribunal.

CAPÍTULO III
DO CONTROLE DE ACESSO AO GABINETE VIRTUAL

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Art. 13. A solicitação de concessão de acesso ao Gabinete Virtual do Tribunal será realizada pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço.

Parágrafo único. No Gabinete Virtual, o usuário contará o mesmo perfil de acesso que detem na rede de computadores e nos sistemas informatizados do Tribunal.

Art. 14. O acesso realizado pelo Gabinete Virtual será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 15. A solicitação de revogação de acesso ao Gabinete Virtual do Tribunal será realizada pelo responsável da unidade à SETIN, utilizando o Sistema de Solicitação de Serviço, quando houver o desligamento do usuário de sua unidade.

CAPÍTULO IV
DO CONTROLE DE ACESSO À INTERNET E À INTRANET

Art. 16. A concessão de acesso à Internet e à Intranet no âmbito do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 17. O acesso à Internet ou à Intranet, partindo de computadores situados no âmbito do Tribunal, será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 18. O uso não apropriado do acesso à Internet e à Intranet será passível de apuração de responsabilidade.

Parágrafo único. Entende-se por uso não apropriado o acesso a sítios ou quaisquer outros serviços:

I – de conteúdo considerado ofensivo, ilegal ou impróprio;

II – do tipo chat, bate-papo e troca de mensagens em tempo real que não tenham sido formalmente autorizados;

III – que apresentem vulnerabilidade de segurança ou possam comprometer a integridade e a disponibilidade da rede de computadores do Tribunal;

IV – que possuem conteúdos evasivos e/ou intrusivos.

Art. 19. A comprovação, por auditoria, do uso não apropriado implicará o bloqueio imediato da Internet para o usuário e a comunicação ao responsável da unidade de lotação do usuário.

Art. 20. Caberá à SETIN, a qualquer momento, o bloqueio de sítios cujo conteúdo seja considerado não apropriado.

Art. 21. É vedada a transferência entre a rede de computadores do Tribunal e a Internet dos seguintes tipos de arquivos:

I – fotos de conteúdos pornográficos;

II – músicas e filmes de qualquer formato;

III – programas ou arquivos executáveis;

IV – programas de conteúdo prejudicial à segurança do ambiente computacional desta Corte.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Parágrafo único. No caso do inciso II, a transferência poderá ser permitida pela autoridade competente. **(Redação dada pelo art. 1º do ATO GDGSET.GP Nº 540, de 28/9/2015)**

Art. 22. O acesso à Intranet poderá ser efetuado a partir de computadores que estejam fora das dependências do TST, mediante a combinação nome de usuário e senha da rede de computadores do Tribunal.

Art. 23. A SETIN será responsável pela manutenção da disponibilidade de banda na Internet e pelo seu monitoramento. Caso necessário, poderá estabelecer limites e quotas para a transferência de dados dos usuários.

CAPÍTULO V
DO CONTROLE DE ACESSO À REDE SEM FIO – WIRELESS

Art. 24. Os usuários internos deste Tribunal terão acesso à rede sem fio.

Art. 25. A solicitação de concessão de acesso à rede sem fio do Tribunal para usuários colaboradores e externos será feita pelo responsável da unidade, utilizando o Sistema de Solicitação de Serviço.

§ 1° O responsável da unidade assinará o Termo de Responsabilidade, disponibilizado na Intranet.

§ 2° O acesso dos usuários colaboradores e externos será revogado em 180 dias, caso o Termo de Responsabilidade não indique data e justificativa para sua manutenção.

Art. 26. O acesso à rede sem fio será realizado mediante a combinação nome de usuário e senha da rede de computadores do Tribunal.

Art. 27. O acesso efetuado pela rede sem fio do Tribunal deverá atender ao disposto nos capítulos de I a IV deste Ato e será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 28. A solicitação de revogação de acesso à rede sem fio do Tribunal será realizada pelo usuário à SETIN, utilizando o Sistema de Solicitação de Serviço.

Art. 29. A rede sem fio dará acesso à Internet, sendo vedada a comunicação direta com a rede interna do Tribunal.

CAPÍTULO VI
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 30. Os serviços de correio eletrônico corporativo do Tribunal serão destinados às atividades do Tribunal, sendo vedado o seu uso para assuntos particulares.

Art. 31. A concessão de acesso ao correio eletrônico corporativo do Tribunal seguirá o previsto no Capítulo I deste Ato.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Art. 32. A mensagem enviada ou recebida pelo correio eletrônico corporativo do Tribunal, seja seu destino interno ou externo, deverá primar pelo uso apropriado da ferramenta.

Art. 33. 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;

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 – entretenimentos e "correntes";

X – assuntos ofensivos;

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

XII – SPAM.

Art. 34. Ao usuário é permitida a participação em listas de discussão com assuntos relacionados ao interesse do trabalho.

Art. 35. O envio de mensagem eletrônica para listas de endereços eletrônicos do Tribunal deverá ser realizado utilizando o endereço de correio eletrônico corporativo da unidade.

Art. 36. Os anexos das mensagens de correio eletrônico não poderão exceder o tamanho estabelecido em norma interna da SETIN, disponível na Intranet do Tribunal.

Parágrafo único. Será vedado ao usuário o envio de anexo que configure o uso não apropriado do correio eletrônico corporativo, conforme Art. 36, parágrafo único.

Art. 37. O envio e o recebimento de mensagens do correio eletrônico corporativo do Tribunal serão registrados pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

Art. 38. A regra de denominação do endereço de correio eletrônico corporativo pessoal será, preferencialmente, o prenome e o sobrenome do servidor, em letras minúsculas, sem acentos, cedilhas ou caracteres especiais, separados pelo sinal de ponto, acrescido do sufixo "@tst.jus.br".

Parágrafo único. As exceções serão tratadas segundo norma interna da SETIN, disponível na Intranet do Tribunal.

Art. 39. A regra de denominação do endereço de correio eletrônico corporativo das unidades será, preferencialmente, a sigla oficial da unidade no Tribunal, em

letras minúsculas, sem acentos, cedilhas, traços, conectivos, pontos ou caracteres especiais, acrescido do sufixo "@tst.jus.br".

Parágrafo único. O endereço de correio eletrônico corporativo será de uso do responsável pela unidade, admitindo-se a designação de servidores para operá-lo.

Art. 40. As regras previstas nos arts. 38 e 39 deste Ato aplicam-se, no que couber, aos e-mails corporativos pessoais e das unidades criados sob a responsabilidade do Conselho Superior da Justiça do Trabalho – CSJT, com o sufixo "@csjt.jus.br", e da Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho – ENAMAT, com o sufixo "@enamat.gov.br".

Art. 41. **(Revogado pelo ATO GDGSET.GP.Nº 75, de 11/2/2015)**.

Art. 42. O limite de tamanho das caixas postais corporativas pessoais e das unidades do Tribunal será fixado em norma interna da SETIN, disponível na Intranet do Tribunal.

Art. 43. Será responsabilidade do usuário do correio eletrônico corporativo do Tribunal:

I – utilizar o correio eletrônico para objetivos e funções inerentes às suas atribuições funcionais;

II – eliminar periodicamente as mensagens contidas nas caixas postais;

III – não permitir acesso de terceiros ao correio eletrônico por meio de sua senha;

IV – notificar a SETIN, por meio do endereço seguranca@tst.jus.br, o recebimento de mensagens inapropriadas, conforme o disposto no Art. 33 deste Ato.

CAPÍTULO VII
DA UTILIZAÇÃO DA ESTRUTURA DE DIRETÓRIOS NA REDE DE COMPUTADORES

Art. 44. A concessão de acesso à estrutura de diretórios da rede de computadores do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 45. O usuário da rede de computadores do Tribunal terá acesso a diretório pessoal e restrito – denominado "P:" – e a diretório da unidade onde estiver lotado – denominado "K:" ou "G:" – com direitos de leitura, escrita e exclusão.

§ 1° Os responsáveis pelas unidades poderão solicitar a criação de novas estruturas de diretórios na rede de computadores do Tribunal e definirão as permissões de acesso dos usuários sob sua responsabilidade.

§ 2° O limite de tamanho dos diretórios será fixado pela SETIN em norma interna, disponível na Intranet do Tribunal.

Art. 46. A rede possuirá um diretório temporário – denominado "H:" – com acesso permitido a todos os usuários, destinado à transferência de documentos.

Parágrafo único. O conteúdo deste diretório não terá cópia de segurança e será excluído diariamente.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Art. 47. A SETIN será responsável pelo controle e monitoramento das capacidades dos diretórios da rede de computadores do Tribunal e dos tipos de arquivos que poderão ser gravados nessas áreas.

Art. 48. Será vedada a cópia, em diretório da rede de computadores do Tribunal, dos seguintes tipos de arquivos:

I – imagens, músicas e filmes de qualquer formato;

II – programas não homologados ou não licenciados;

III – programas de conteúdo prejudicial à segurança do ambiente computacional;

IV – outros arquivos digitais cuja utilização não seja de interesse do Tribunal.

Parágrafo único. A SETIN poderá excluir dos diretórios da rede os arquivos que se enquadrem nas alíneas de I a IV deste artigo, sem prévio aviso e sem realizar cópia de segurança dos arquivos excluídos.

Art. 49. Será responsabilidade do usuário da rede de computadores do TST:

I – utilizar os diretórios da rede somente para arquivar documentos referentes às suas atribuições funcionais;

II – primar pela eficiência na utilização dos recursos tecnológicos disponíveis, eliminando periodicamente os arquivos que não sejam necessários ou não façam parte do acervo de sua unidade;

III – não permitir acesso de terceiros à rede por meio de sua senha;

IV – notificar a SETIN, pelo endereço seguranca@tst.jus.br, quando tiver ciência da existência de arquivos na rede vedados, conforme o disposto no art. 37 deste Ato.

Art. 50. O acesso efetuado pela rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

CAPÍTULO VIII
DA UTILIZAÇÃO DE PROGRAMAS E APLICATIVOS

Art. 51. Este capítulo trata das diretrizes de homologação, instalação e utilização de programas e aplicativos de computador no âmbito do Tribunal.

Art. 52. A instalação e a utilização de programas de computador no Tribunal estão sujeitas aos seguintes requisitos:

I – existência de licenças de uso em quantidade suficiente;

II – homologação pelos técnicos da SETIN;

III – conformidade com a atividade da instituição e com a área de atuação das unidades;

IV – compatibilidade com os demais programas utilizados;

V – adequação aos recursos computacionais disponíveis; e

VI – obediência a planejamentos, cronogramas e prioridades existentes.

Art. 53. O equipamento de informática distribuído no Tribunal terá a instalação, pelos técnicos da SETIN, dos programas e aplicativos básicos homologados que atendam aos requisitos do artigo anterior.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Art. 54. A instalação de programas e aplicativos em equipamento de informática do Tribunal deverá ser realizada, exclusivamente, por técnicos da SETIN.

Art. 55. Será vedada a instalação de programa de terceiros, sem licença de uso regularmente contratada.

Art. 56. Caberá à SETIN manter o registro das licenças de uso de programas de terceiros utilizados pelo Tribunal.

Art. 57. A SETIN poderá autorizar a cessão de cópia de programa de computador adquirido ou contratado pelo Tribunal, em ambiente externo, nos termos da licença de uso.

Art. 58. A SETIN poderá realizar, para teste e avaliação, a instalação de programa ou aplicativo, com autorização do produtor, distribuidor ou revendedor, pelo prazo estipulado na autorização.

Art. 59. O usuário será responsabilizado pela instalação ou execução não autorizada de programa não homologado pela SETIN, considerando a possibilidade de dano às instalações de informática do Tribunal.

Art. 60. Será vedada a instalação e utilização de programas e aplicativos de computador que descaracterizem os propósitos da instituição e que possam prejudicar a segurança dos ativos de informação ou danificar o ambiente computacional do Tribunal.

Art. 61. A solicitação de instalação de programas e aplicativos deverá ser encaminhada à SETIN pelo Sistema de Solicitação de Serviços, acompanhada de justificativa.

Art. 62. A listagem dos programas e aplicativos homologados para a utilização no Tribunal deverá ser publicada na Intranet.

Art. 63. A SETIN deverá inventariar, sistematicamente, os programas e aplicativos instalados no Tribunal remotamente, sem prévia autorização do usuário.

Art. 64. A SETIN poderá remover, sem prévio aviso ao usuário e sem a realização de cópia de segurança, os programas e aplicativos que não cumprirem os requisitos do art. 52 deste Ato.

Art. 65. A atualização dos programas e aplicativos instalados no âmbito do Tribunal poderá ser realizada pela equipe técnica da SETIN remotamente, sem prévia autorização do usuário.

CAPÍTULO IX
DA UTILIZAÇÃO DE EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 66. A instalação de programas e aplicativos nos equipamentos portáteis do Tribunal observará os requisitos relacionados no art. 52 deste Ato.

Art. 67. Os microcomputadores portáteis pertencentes ao parque computacional do Tribunal deverão possuir a mesma proteção das estações de trabalho.

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

Art. 68. Será vedada a conexão de equipamento ou dispositivo móvel na Rede de Computadores do TST, sem a prévia verificação e autorização da equipe técnica da SETIN.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 69. Os dispositivos móveis de armazenamento deverão ser verificados pelo programa de detecção e proteção contra vírus antes de serem conectados a equipamento pertencente ao Tribunal.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que efetuar a conexão.

Art. 70. A solicitação de verificação de equipamento ou dispositivo móvel para autorização de conexão na rede de computadores do Tribunal deverá ser encaminhada à SETIN pelo Sistema de Solicitação de Serviços, acompanhada de justificativa.

Art. 71. O acesso efetuado pelos dispositivos móveis no ambiente tecnológico do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme Capítulo X deste Ato.

CAPÍTULO X
DO CONTROLE, MONITORAMENTO E AUDITORIA DE RECURSOS TECNOLÓGICOS

Art. 72. A utilização de recursos tecnológicos bem como o acesso aos ativos de informação no Tribunal serão registrados e monitorados pela SETIN, com o intuito de detectar e evidenciar incidentes de segurança.

Parágrafo único. Não será realizado o monitoramento de serviço de telefonia móvel ou fixa.

Art. 73. A SETIN será responsável por realizar auditorias ordinárias e extraordinárias nos ativos de informação do Tribunal.

§ 1° Auditorias ordinárias serão realizadas periodicamente, com o objetivo de avaliação da conformidade técnica dos serviços, ferramentas e equipamentos em funcionamento no Tribunal.

§ 2° Auditorias extraordinárias serão requeridas por solicitação superior para apurar eventos que colocam em risco a segurança dos ativos de informação e as boas práticas de utilização do ambiente informatizado do Tribunal.

Art. 74. Estarão sujeitos à auditoria extraordinária os seguintes eventos de segurança:

I – Na estação de trabalho: alteração de arquivos e da configuração da estação de trabalho;

II – Nos dispositivos móveis: alteração de arquivos e da configuração do dispositivo, acessos ou manipulação de dados indevidos;

III – Nos sistemas informatizados e nos bancos de dados do Tribunal:

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.

acessos ou manipulação de dados indevidos;

IV – No correio eletrônico corporativo: envio e recebimento de mensagens eletrônicas indevidas;

V – No acesso à Intranet, à Internet ou outro meio de acesso externo à rede de computadores do Tribunal: acessos e manipulação de dados indevidos;

VI – Na rede de computadores do Tribunal: alteração de arquivos e da configuração dos servidores.

Art. 75. A solicitação de auditoria em incidente não previsto neste Ato será analisada e deliberada pelo Comitê Gestor de Segurança da Informação.

CAPÍTULO XI
DA ANÁLISE DOS RISCOS E DAS VULNERABILIDADES DO AMBIENTE COMPUTACIONAL

Art. 76. À SETIN caberá, periodicamente, a avaliação das ameaças, impactos e vulnerabilidades dos ativos de informação e da probabilidade de suas ocorrências.

Art. 77. A SETIN manterá, instalado e atualizado, programa de detecção e proteção contra vírus e demais agentes nocivos à segurança dos ativos de informação no ambiente computacional do Tribunal.

Art. 78. Serão mantidos pela SETIN os planos de continuidade de negócios que visem a assegurar a integridade, a confidencialidade e a disponibilidade dos ativos de informação necessários para o cumprimento da missão institucional do Tribunal.

CAPÍTULO XII
DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 79. O usuário que efetuar qualquer acesso aos recursos computacionais do Tribunal que desrespeite este Ato será responsabilizado.

Art. 80. A SETIN poderá, constatado o não cumprimento deste Ato, a qualquer momento, suspender o acesso concedido ao usuário.

Art. 81. Caberá ao Comitê Gestor de Segurança da Informação, constituído pelo Ato TST.GP nº 493/2009, a revisão anual desta Política de Segurança da Informação.

Art 82. A inobservância das disposições deste Ato implicará responsabilidade administrativa na forma da lei.

Art. 83. O presente Ato entra em vigor a partir da data de sua publicação e revoga o ATO.GDGCA.GP.Nº 323/2006.

(*) Republicado em cumprimento ao disposto no Art. 2º do ATO GDGSET.GP Nº 540, de 28 de setembro de 2015.

Ministro ANTONIO JOSÉ DE BARROS LEVENHAGEN

Fonte: Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 39, 2 out. 2015, p. 7-17. Republicação.