ATO Nº 372/GDGSET.GP, DE 27 DE JUNHO DE 2023

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 a Lei de Acesso à Informação, Lei nº 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 da República;

considerando a Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

considerando a Portaria CNJ nº 162/2021, que aprova os protocolos e manuais criados pela Resolução CNJ nº 396/2021, que por sua vez instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

considerando o Ato TST.GP. nº 303/2021, que disciplina a composição e as atribuições do Comitê Gestor de Segurança da Informação do Tribunal Superior do Trabalho – CGSI;

considerando o Ato Conjunto TST.CSJT nº 27/2013, que define os papéis e as responsabilidades da unidade gestora, do gestor de sistema, da unidade de negócio e do usuário de sistemas informatizados e de bases de dados no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho;

considerando o Ato Conjunto TST.CSJT.GP nº 40/2018, que dispõe, no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho, sobre o acesso à informação e a aplicação da Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pelos órgãos públicos com o fim de garantir o acesso a informações;

considerando a Instrução Normativa GSI Nº 5/2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

considerando o conjunto de normas ABNT NBR ISO/IEC 27000, que especificam os requisitos para estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação;

considerando as melhores práticas para proteção e controle da informação referenciadas nas disciplinas do COBIT e nos processos da biblioteca ITIL em suas versões mais recentes;

considerando a necessidade de ampliar as diretrizes e os padrões de segurança, a fim de 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 regulamentar o acesso à rede de computadores, aos sistemas informatizados, aos bancos de dados, à internet, à intranet, à rede sem fio, às redes sociais e do tipo remoto;

considerando a necessidade de regulamentar o uso do serviço de correio eletrônico corporativo, da estrutura de diretórios na rede de computadores, de programas e aplicativos, de equipamentos de tecnologia da informação e de serviços em nuvem;

considerando a necessidade de regulamentar boas práticas, gestão de riscos e de vulnerabilidades do ambiente tecnológico, bem como o controle, monitoramento e a auditoria de recursos tecnológicos no âmbito do Tribunal;

considerando os danos potenciais decorrentes de acessos a sítios e aplicativos indevidos ou inadequados na internet e da instalação de programas não homologados e inadequados, bem como o risco de contaminação por programas maliciosos nas estações de trabalho e nos dispositivos móveis,

RESOLVE:

Art. 1º Definir 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 ato aplicam-se as seguintes definições:

I – Ambiente tecnológico: conjunto de recursos que utiliza ou disponibiliza serviços de tecnologia da informação e sistemas de informação do Tribunal;

II – Ativos de informação: base de dados e arquivos, contratos e

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas, aplicativos, sistemas, ferramentas de desenvolvimento e utilitários, equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

III – Central de Serviços de TIC: equipe dedicada a determinadas atividades de suporte técnico dos serviços de TIC, à qual cabe promover o contato inicial entre os usuários e a Secretaria de Tecnologia da Informação e Comunicação – SETIN;

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

V – 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;

VI – 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;

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

VIII – Correio eletrônico corporativo ou correio eletrônico: são consideradas corporativas as caixas de correio eletrônico dos usuários internos e colaboradores constantes da solução de e-mail gerenciada pelo TST;

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

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

XI – 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;

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

XIII – Programa de terceiros: programa que não foi desenvolvido pela equipe de informática da SETIN;

XIV – Programa malicioso: programa criado para causar algum dano ao computador infectado, seja apagando dados, capturando informações ou alterando o funcionamento normal da máquina;

XV – Serviço de diretório: sistema de software que armazena, organiza e fornece acesso a informações e permissões de acesso;

XVI – Autenticação multifator: método de autenticação que requer verificação de identidade adicional para o acesso a contas ou aplicativos, como a

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

leitura de uma impressão digital ou a adição de um código recebido por telefone.

CAPÍTULO I
DO CONTROLE DE ACESSO À REDE DE COMPUTADORES

Art. 3º Os serviços disponibilizados para acesso na rede de computadores do Tribunal abrangem: estrutura de diretórios de rede, intranet, internet, correio eletrônico corporativo e rede sem fio.

Parágrafo único. O acesso padrão à rede de computadores do Tribunal é assim regulado:

I – Para usuário interno: é permitido o acesso aos serviços disponibilizados na rede de computadores do Tribunal;

II – Para usuário previdenciário: é permitido somente o acesso aos serviços compatíveis com sua situação funcional;

III – Para usuário colaborador: é permitido o acesso aos serviços compatíveis com sua necessidade de trabalho;

IV – Para usuário externo: é permitido, mediante comprovada necessidade de serviço, o acesso aos serviços de rede de computadores, internet e rede sem fio em compatibilidade com requisitos definidos em normativo da SETIN.

Art. 4º A solicitação de concessão de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, por meio da Central de Serviços de TIC.

§ 1º Na solicitação de acesso para usuários internos, deverá constar nome completo e código do usuário interessado, bem como os serviços solicitados, conforme descritos no art. 3º.

§ 2º Na solicitação de acesso para usuários colaboradores ou externos, deverá constar o Termo de Responsabilidade com período de validade do acesso preenchido, sendo este o limite máximo de duração do estágio, do contrato ou da permanência.

§ 3º A SETIN deverá observar a obrigatoriedade de inclusão de todas as informações constantes do Termo de Responsabilidade no serviço de diretório para permitir rastreabilidade e monitoramento de informações nas contas de usuários.

Art. 5º A Coordenadoria de Segurança Cibernética – CSEC poderá, constatado o não cumprimento deste Ato, a qualquer momento, solicitar a suspensão do acesso concedido ao usuário.

Art. 6º É vedada a utilização de perfil de administrador local ou de administrador de domínio para pessoal que não seja técnico da SETIN ou da

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

Secretaria de Tecnologia da Informação e Comunicação – SETIC do Conselho Superior da Justiça do Trabalho – CSJT.

Art. 7º O acesso à rede de computadores do Tribunal e seus serviços dar-se-á por meio de credenciais de acesso válidas, tais como usuário e senha, certificados digitais ou autenticação multifator.

§ 1º As credenciais de acesso são pessoais e intransferíveis.

§ 2º É proibido aos usuários ceder suas credenciais de acesso a terceiros.

Art. 8º Para os casos em que o acesso dar-se-á por meio de usuário e senha, os seguintes padrões devem ser observados:

§ 1º A senha deverá ter um tamanho mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos 3 (três) dos seguintes tipos de caracteres: número, letra maiúscula, letra minúscula ou caractere especial, devendo ser evitada senha de fácil dedução.

§ 2º A senha será alterada a cada 6 (seis) meses.

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

Art. 9º A solicitação de revogação de acesso à rede de computadores do Tribunal será feita pelo responsável da unidade à SETIN, por meio da Central de Serviços de TIC, quando houver o desligamento do usuário de sua unidade.

Parágrafo único. A SETIN poderá, por questões de segurança ou administração de licenças em softwares contratados, criar regras no serviço de diretório para desativação das contas de usuários que não foram utilizadas na rede do Tribunal nos últimos 12 meses.

Art. 10. O acesso à rede de computadores do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme o Capítulo XIV deste Ato.

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

Art. 11. O acesso aos sistemas informatizados e aos bancos de dados do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 12. A solicitação de concessão de acesso aos sistemas

informatizados e aos bancos de dados do Tribunal será encaminhada à SETIN, por meio da Central de Serviços de TIC, pelo responsável da unidade ao gestor do respectivo sistema.

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

§ 2º No caso de usuários colaboradores ou externos, a solicitação deverá conter o Termo de Responsabilidade com período de validade do acesso preenchido, sendo este o limite máximo de duração do estágio, do contrato ou da permanência.

Art. 13. O acesso aos sistemas informatizados e aos bancos de dados do Tribunal será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme o Capítulo XIV deste Ato.

Art. 14. A revogação de acesso aos sistemas informatizados e aos bancos de dados do Tribunal será solicitada pelo gestor quando houver o desligamento do usuário de sua unidade.

§ 1º O rompimento do vínculo funcional do servidor deverá ser comunicado à Secretaria de Tecnologia da Informação e Comunicação – SETIN pelo gestor da unidade de lotação para que seja revogado o acesso aos sistemas informatizados e aos bancos de dados. (*Incluído pelo Ato n. 264/GDGSET.GP, de 6 de maio de 2024*)

§ 2º Na hipótese de o rompimento do vínculo funcional ser comunicado pelo ex-servidor, a revogação do acesso aos sistemas informatizados e aos bancos de dados dar-se-á a partir da data de ciência da Administração do Tribunal, de forma imediata, após o lançamento no Sistema de Recursos Humanos. (*Incluído pelo Ato n. 264/GDGSET.GP, de 6 de maio de 2024*)

§ 3º O encerramento do vínculo de estagiários, menores aprendizes e terceirizados deverá ser comunicado imediatamente à SETIN pela área responsável pelo acompanhamento desses vínculos e fiscalização dos respectivos contratos para a revogação de acesso ao ambiente tecnológico do TST. (*Incluído pelo Ato n. 264/GDGSET.GP, de 6 de maio de 2024*)

Art. 15. Os servidores responsáveis pelo desenvolvimento de sistemas do TST, do CSJT e da Escola Nacional de Formação e Aperfeiçoamento de Magistrados do Trabalho – ENAMAT, quando estes estiverem hospedados na infraestrutura tecnológica do Tribunal, poderão ter acesso aos sistemas em produção e aos bancos de dados para realizar manutenções, mediante autorização expressa do gestor do sistema.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

Art. 16. O gestor do sistema poderá, justificadamente, solicitar a suspensão ou o cancelamento do acesso do usuário ao sistema informatizado do Tribunal.

Art. 17. A infraestrutura que suporta os sistemas corporativos desenvolvidos por outras entidades e hospedados no ambiente tecnológico do Tribunal será mantida pelas equipes técnicas da SETIN, devendo ser aplicadas as atualizações e correções de segurança necessárias para manter o ambiente tecnológico do TST seguro e atualizado.

Art. 18. Para os sistemas desenvolvidos por outras entidades que são adotados pelo Tribunal, cujas funcionalidades não seguem os padrões estabelecidos neste Ato, o gestor ou responsável no Tribunal pelo sistema deverá formalizar pedido para adequação das funcionalidades não conformes a fim de registrar a necessidade de manutenção dos padrões de segurança do ambiente tecnológico do Tribunal.

CAPÍTULO III
DO CONTROLE DE ACESSO À INTERNET E À INTRANET

Art. 19. A concessão de acesso à internet e à intranet no âmbito do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 20. 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 – que apresentem vulnerabilidade de segurança ou possam comprometer a integridade e a disponibilidade da rede de computadores do Tribunal;

III – que possuem conteúdos evasivos e/ou intrusivos;

IV – de terceiros que tenham a finalidade de reduzir o número de caracteres de endereços de sítios;

V – de mensagens instantâneas não corporativas no âmbito do Tribunal.

Art. 21. A comprovação, por auditoria realizada pela SETIN, 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. 22. Caberá à CSEC, a qualquer momento, a solicitação de bloqueio de sítios ou serviços cujo conteúdo seja considerado não apropriado.

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

Art. 23. A transferência de arquivos a partir da rede corporativa por meio de download ou upload será autorizada somente para arquivos necessários ao desempenho das atividades laborais e que não coloquem em risco a segurança do ambiente tecnológico desta Corte.

Parágrafo único. A transferência poderá ser autorizada mediante justificativa encaminhada à Central de Serviços de TIC por magistrado ou gestor detentor de cargo em comissão, contendo expressamente a relação entre a atividade desempenhada e a demanda.

Art. 24. O acesso à intranet poderá ser efetuado a partir de computadores que estejam fora das dependências do Tribunal mediante o fornecimento de informações que validem os dados de servidores ativos, inativos ou cedidos.

Art. 25. A CITEC é a unidade responsável pelo controle de banda na internet e pelo seu monitoramento.

Parágrafo único. Caso necessário, serão estabelecidos limites e quotas para a transferência de dados dos usuários, objetivando garantir a disponibilidade dos serviços ofertados pelo TST à sociedade.

Art. 26. 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 o Capítulo XIV deste Ato.

CAPÍTULO IV
DO CONTROLE DE ACESSO À REDE SEM FIO

Art. 27. A concessão de acesso à rede sem fio no âmbito do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 28. A rede sem fio dará acesso à internet, sendo vedada a comunicação direta com a rede interna do Tribunal.

Art. 29. Os usuários internos deste Tribunal terão acesso à rede sem fio.

Art. 30. O acesso à rede sem fio será realizado mediante a combinação de nome de usuário e senha da rede de computadores do Tribunal ou via código de autorização, de forma pessoal e intransferível.

Parágrafo único. Não poderão ser compartilhados o código de autorização e a combinação de nome de usuário e senha da rede de

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

computadores do Tribunal.

Art. 31. Somente os pontos de acesso pertencentes ao Tribunal deverão fazer parte da infraestrutura de rede sem fio.

Art. 32. O acesso efetuado pela rede sem fio do Tribunal deverá atender ao disposto neste Ato e será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme o Capítulo XIV deste Ato.

CAPÍTULO V
DO CONTROLE DE ACESSO A REDES SOCIAIS

Art. 33. O acesso a redes sociais está sujeito à necessidade para o trabalho mediante justificativa motivada.

§ 1º A solicitação de acesso a redes sociais deverá ser encaminhada à SETIN, por meio da Central de Serviços de TIC, por Ministros, Chefes de Gabinetes de Ministros ou Gestores detentores de cargo em comissão de nível CJ4.

§ 2º A justificativa, integrante do Termo de Responsabilidade, deverá conter expressamente a relação entre a atividade desempenhada e a demanda, que deverá ser analisada pela unidade de Segurança Cibernética em relação ao nível de exposição às ameaças computacionais.

§ 3º No caso da Secretaria de Comunicação Social – SECOM e da Coordenadoria de Desenvolvimento de Pessoas – CDEP, a solicitação poderá ser feita por seus responsáveis.

CAPÍTULO VI
DO CONTROLE DE ACESSO REMOTO

Art. 34. A CITEC deverá disponibilizar ferramental para o acesso remoto que proporcione:

I – Segurança do meio de comunicação;

II – Autenticação dos usuários;

III – Limite de acesso restrito aos recursos computacionais segundo as necessidades de cada usuário.

Art. 35. Os usuários que utilizem o acesso remoto deverão observar os seguintes requisitos:

I – Manter o computador com as últimas atualizações e correções de segurança do sistema operacional instaladas;

II – Utilizar somente sistema operacional e programas licenciados;

III – Manter programa antivírus atualizado;

IV – Habilitar o firewall do sistema operacional;

V – Não salvar as senhas de acesso nos navegadores ou noutros programas;

VI – Alterar imediatamente suas senhas de rede e sistemas em caso de perda, roubo, descarte ou manutenção do equipamento utilizado para acesso remoto;

VII – Configurar a rede sem fio de origem do acesso com pelo menos o protocolo WPA2, alterando a senha padrão do roteador;

VIII – Armazenar os documentos corporativos exclusivamente nos locais adequados providos no ambiente de acesso remoto;

IX – Não armazenar informações sensíveis do TST em dispositivos pessoais;

X – Não expor dados e informações sensíveis do TST a terceiros;

XI – Observar o disposto nos Capítulos XII e XIII deste Ato.

Parágrafo único. O licenciamento do sistema operacional e demais programas instalados na estação de trabalho de origem do acesso remoto é de inteira responsabilidade do usuário.

Art. 36. O acesso remoto será monitorado e registrado pela SETIN, podendo a qualquer momento ser efetuada auditoria, conforme o Capítulo XIV deste Ato.

CAPÍTULO VII
DA UTILIZAÇÃO DO CORREIO ELETRÔNICO CORPORATIVO

Art. 37. A concessão de acesso ao correio eletrônico corporativo do Tribunal seguirá o previsto no Capítulo I deste Ato.

Art. 38. Os serviços de correio eletrônico corporativo do Tribunal serão destinados ao desempenho das atividades funcionais dos usuários, sendo vedado o seu uso para assuntos particulares.

§ 1º O endereço de correio eletrônico corporativo não deverá ser utilizado para cadastro em sítios ou serviços de interesse particular;

~~§ 2º Os serviços de correio eletrônico corporativo não serão disponibilizados para usuários previdenciários;~~

§ 2º Os serviços de correio eletrônico corporativo não serão disponibilizados para usuários previdenciários e para ex-servidores ocupantes de cargo efetivo ou cargo comissionado que tiveram rompido o vínculo funcional com o Tribunal. (*Redação dada pelo Ato n. 264/GDGSET.GP, de 6 de maio de 2024*)

§ 3º O acesso aos serviços de correio eletrônico corporativo permanecerá disponível pelo prazo de 30 (trinta) dias corridos a contar da publicação da aposentadoria;

§ 4º O acesso aos serviços de correio eletrônico corporativo dar-se-á por usuário e senha.

§ 5º O acesso aos serviços de correio eletrônico corporativo será revogado de forma imediata para os ex-servidores ocupantes de cargo efetivo ou cargo comissionado que tiveram rompido o vínculo funcional com o Tribunal. (*Incluído pelo Ato n. 264/GDGSET.GP, de 6 de maio de 2024*)

Art. 39. 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 outro programa malicioso;

VII – material de natureza político-partidária;

VIII – material protegido por leis de propriedade intelectual;

IX – entretenimentos;

X – assuntos ofensivos;

XI – arquivos de áudio, vídeo, imagem ou texto que não sejam de interesse específico do trabalho;

XII – envio de mensagens em massa não solicitadas.

Art. 40. O limite de tamanho das caixas postais corporativas do Tribunal será de responsabilidade da CITEC.

Art. 41. É vedado ao usuário o envio de anexo que configure o uso não apropriado do correio eletrônico corporativo, conforme o art. 39.

Art. 42. É 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.

Art. 43. 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 o Capítulo XIV deste Ato.

CAPÍTULO VIII
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 um ou mais diretórios de rede referentes à unidade de sua lotação, mapeados em sua estação de trabalho com os direitos de leitura e escrita.

§ 1º Diretórios de rede são para uso compartilhado, não sendo permitida a criação de diretório de rede para uso pessoal.

§ 2º Os responsáveis pelas unidades serão os gestores de seus respectivos diretórios de rede, devendo responder por seu uso e definir as permissões de acesso dos usuários sob sua responsabilidade, podendo ainda encaminhar solicitação de criação de novas estruturas de diretórios na rede de computadores do Tribunal.

Art. 46. A SETIN, em conjunto com o gestor da unidade usuária do diretório de rede, será responsável pelo controle e pelo monitoramento da capacidade do referido diretório da rede de computadores do Tribunal e dos tipos de arquivos que poderão ser armazenados em tais áreas.

Art. 47. A capacidade de armazenamento dos diretórios de rede das unidades será fixa, mas poderá ser incrementada quando solicitado pelo responsável da unidade, desde que revisado o diretório pelos usuários para identificar arquivos que não são mais necessários, tais como:

I - Arquivos pessoais de usuários que não estão mais lotados na unidade;

II - Material para estudo ou aulas que não estejam relacionadas com as atividades desempenhadas no Tribunal;

III - Arquivos pessoais não associados ao trabalho;

IV - Registros de eventos não relacionados à atividade da unidade.

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

I – Imagens, músicas e filmes não relacionados a atividades laborais;

II – Programas não homologados ou não licenciados;

III – Programas de conteúdo prejudicial à segurança do ambiente

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

tecnológico;

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

§ 1º A SETIN poderá excluir dos diretórios da rede os arquivos que se enquadrem nos incisos I a IV deste artigo, com prévio aviso, quando possível, e sem realizar cópia de segurança dos arquivos excluídos.

§ 2º Será autorizado o armazenamento de arquivos elencados no inciso I, desde que expressamente justificado.

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 e racionalidade na utilização dos recursos tecnológicos disponíveis, eliminando periodicamente os arquivos que não sejam necessários ou não façam parte do acervo de sua unidade.

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

CAPÍTULO IX
DA UTILIZAÇÃO DE PROGRAMAS E APLICATIVOS

Art. 51. 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 CSUP;

III – Conformidade com a atividade da instituição e com a área de atuação;

IV – Compatibilidade com os demais programas utilizados;

V – Adequação aos recursos computacionais disponíveis;

VI – Obediência a planejamentos, cronogramas e prioridades existentes;

VII – Análise pelos técnicos da CSEC.

Parágrafo único. Os programas instalados que porventura não atendam aos requisitos deste artigo poderão ser removidos pela CSUP, sem prévio aviso ao usuário e sem a realização de cópia de segurança.

Art. 52. A instalação de programas e aplicativos homologados, incluindo programas básicos, em equipamento de informática do Tribunal deverá ser executada, exclusivamente, por técnicos ou métodos autorizados pela SETIN.

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

Art. 53. É vedada a instalação de programa de terceiros sem licença de uso regularmente contratada.

Art. 54. Caberá à CSUP manter o registro das licenças de uso de programas de terceiros utilizados pelo Tribunal.

Art. 55. A SETIN poderá realizar, para teste e avaliação, a instalação de programa ou aplicativo, com autorização do produtor, distribuidor ou revendedor, quando couber, pelo prazo estipulado na autorização.

Art. 56. É vedada a instalação e a utilização de programas e aplicativos de computador não homologados ou que descaracterizem os propósitos do Tribunal ou que possam oferecer riscos à segurança dos ativos de informação ou danificar o ambiente tecnológico do Tribunal.

Parágrafo único. As extensões de navegadores são consideradas programas de computador.

Art. 57. A solicitação de instalação de programas e aplicativos homologados deverá ser encaminhada à SETIN pela Central de Serviços de TIC.

Art. 58. A CSUP manterá publicada na intranet a listagem dos programas e dos aplicativos homologados para a utilização no Tribunal.

Art. 59. A CSUP deverá inventariar, sistematicamente e de forma remota, os programas e aplicativos instalados no ambiente tecnológico do Tribunal.

Art. 60. A atualização dos programas e aplicativos instalados no âmbito do Tribunal poderá ser realizada pela equipe técnica da CSUP remotamente.

Art. 61. O usuário será responsabilizado pela instalação ou pela execução não autorizada de programa não homologado pela SETIN, considerando-se a possibilidade de dano às instalações de informática do Tribunal.

CAPÍTULO X
DA UTILIZAÇÃO DE EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 62. Os dispositivos portáteis pertencentes ao parque computacional do Tribunal deverão possuir a mesma proteção das estações de trabalho.

Art. 63. É vedada a conexão direta de equipamento ou dispositivo

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

portátil particular na rede cabeada de computadores do TST.

Parágrafo único. A não observância do disposto neste artigo implicará a responsabilização do usuário que causar incidente no ambiente tecnológico do TST.

Art. 64. Os dispositivos portáteis de armazenamento, ao serem conectados à rede cabeada ou a equipamento pertencente ao Tribunal, deverão ser verificados pelo programa de detecção e proteção contra vírus e outros programas maliciosos.

Art. 65. 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 o Capítulo XIV deste Ato.

CAPÍTULO XI
DA UTILIZAÇÃO DE SERVIÇOS EM NUVEM

Art. 66. A utilização de serviços em nuvem de uso corporativo deverá:

I – preceder de análise visando assegurar as garantias fundamentais no tratamento das informações pessoais, observando-se os termos da Lei nº 13.709/2018;

II – ser restrita a informação classificada como de caráter público.

Parágrafo único. Informação classificada em qualquer grau de sigilo não poderá ser armazenada em ambiente de nuvem.

Art. 67. O caráter público e os graus de sigilo da informação devem observar o Ato Conjunto TST.CSJT.GP nº 40/2018.

Art. 68. Cópias de segurança para os arquivos armazenados em nuvem são garantidas por 30 (trinta) dias.

CAPÍTULO XII
DA POLÍTICA DE MANUTENÇÃO, REMANEJAMENTO, DOAÇÃO OU DESCARTE DE EQUIPAMENTOS DE TIC

Art. 69. Em caso de manutenção de equipamentos de TIC, a unidade responsável da SETIN deverá:

I – realizar backup e eliminar as informações do equipamento quando a manutenção for realizada por equipe externa ou fora das dependências do Tribunal;

II – inspecionar o equipamento para garantir que não foi alterado

indevidamente e que não há mau funcionamento, após a manutenção por equipe externa ou fora das dependências do Tribunal.

Parágrafo único. Informações, programas ou equipamentos não devem ser retirados do local sem autorização prévia.

Art. 70. Em caso de remanejamento de equipamentos de TIC, a unidade responsável deverá formatar o equipamento antes de realizar o seu remanejamento para outra unidade.

Art. 71. Em caso de doação ou descarte de equipamentos de TIC, a unidade responsável da SETIN deverá realizar a formatação prévia do equipamento, utilizando solução que impeça a recuperação dos dados.

CAPÍTULO XIII
DAS BOAS PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

Art. 72. Durante a execução das suas atividades laborais, todos os usuários do TST, presencialmente ou em regime de trabalho remoto, devem:

I – Guardar em local seguro informações sensíveis ou críticas;

II – Desligar ou hibernar os computadores ao final do expediente;

III – Bloquear os computadores com senha sempre que se ausentar da estação de trabalho.

Parágrafo único. Deverão ser utilizados somente equipamentos do Tribunal na realização de trabalho presencial.

CAPÍTULO XIV
DO CONTROLE, MONITORAMENTO E AUDITORIA DE RECURSOS TECNOLÓGICOS

Art. 73. A utilização de recursos tecnológicos e o acesso aos ativos de informação no Tribunal serão registrados e monitorados pela SETIN, com o intuito de detectar e evidenciar incidentes de segurança ou uso indevido.

Art. 74. Os ativos de infraestrutura de tecnologia disponibilizados no parque computacional do Tribunal a outros órgãos deverão constar no monitoramento do ambiente tecnológico.

Art. 75. A SETIN é responsável por realizar auditorias nos ativos de Tecnologia da Informação do Tribunal.

Parágrafo único. Auditorias serão realizadas periodicamente, com o objetivo de avaliar a conformidade técnica de serviços, ferramentas e

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

equipamentos, apurar eventos que coloquem em risco a segurança dos ativos de informação e verificar as boas práticas de utilização do ambiente tecnológico do Tribunal.

Art. 76. Estarão sujeitos à auditoria os seguintes eventos de segurança:

I – Nas configurações de usuários: permissões de acessos;

II – Nas estações de trabalho e dispositivos móveis: alteração de arquivos, configuração, instalação de programas e acessos ou manipulação de dados indevidos;

III – Nos sistemas informatizados e nos bancos de dados do Tribunal: acessos ou manipulação de dados indevidos;

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

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

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

Art. 77. A solicitação de auditoria em incidente não previsto neste Ato será analisada e deliberada pelo Comitê Gestor de Segurança da Informação.

CAPÍTULO XV
DA GESTÃO DE RISCOS E DE VULNERABILIDADES DO AMBIENTE TECNOLÓGICO

Art. 78. A gestão de riscos dos ativos de informação de TIC e processos de trabalho relacionados caberá aos seus respectivos responsáveis, no âmbito da SETIN.

Art. 79. A gestão de vulnerabilidades dos ativos de informação de TIC será realizada no âmbito da SETIN.

Art. 80. A CSUP manterá, instalado e atualizado, programa de detecção e proteção contra programas maliciosos e demais agentes nocivos à segurança dos ativos de informação no ambiente tecnológico do Tribunal.

CAPÍTULO XVI
DA SENSIBILIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Art. 81. Todos os servidores, prestadores e colaboradores devem ser sensibilizados em relação à segurança da informação por meio de treinamento, educação e conscientização apropriados, considerando atualizações regulares das políticas, normas e procedimentos relevantes para a realização de suas funções.

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

§ 1º Recomenda-se que a sensibilização em segurança da informação contemple aspectos gerais, tais como:

I – O comprometimento da alta administração com a segurança da informação;

II – O conhecimento de obrigações e diretrizes de segurança da informação, bem como de necessidade de demonstração de conformidade, considerando políticas, normas, leis, regulamentações, contratos e acordos relacionados;

III – A responsabilidade pessoal por seus próprios atos e omissões, observando o compromisso para manutenção da segurança e proteção da informação pertencente ao Tribunal.

§ 2º A sensibilização em segurança da informação deverá ser realizada periodicamente.

§ 3º A sensibilização em segurança da informação deverá ser alinhada com políticas e procedimentos relevantes de segurança da informação, considerando necessidades específicas de proteção de informações e os controles que devem ser implementados.

§ 4º Deverão ser considerados múltiplos formatos para a sensibilização em segurança da informação, visando o amplo aproveitamento dos meios disponíveis para divulgação de conteúdos.

CAPÍTULO XVII
DAS DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 82. Os responsáveis pela elaboração de termo de referência ou de projeto básico de ações constantes do Plano de Contratações da SETIN deverão incluir em tais documentos:

I – requisitos de segurança da informação;

II – acordos de confidencialidade conforme o objeto a ser licitado;

III – ciência desta Política de Segurança da Informação.

Art. 83. Caberá à CSEC e ao Comitê Gestor de Segurança da Informação a revisão periódica desta Política de Segurança da Informação.

Art. 84. A CSEC poderá, constatado o não cumprimento deste Ato ou o iminente risco de segurança da informação, a qualquer momento, suspender o acesso ou utilização do recurso tecnológico concedido ao usuário.

Art. 85. A inobservância das disposições deste Ato implicará responsabilidade administrativa na forma da lei.

Art. 86. Os casos omissos, após análise da CSEC, serão resolvidos

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.

pelo Secretário da SETIN.

Art. 87. Este Ato entra em vigor na data de sua publicação e revoga o Ato GDGSET.GP n.º 183, de 27 de maio de 2019.

MINISTRO LELIO BENTES CORRÊA

Última alteração: Ato n. 264/GDGSET.GP, de 6 de maio de 2024.

Este texto não substitui o publicado no Boletim Interno [do] Tribunal Superior do Trabalho, Brasília, DF, n. 25, p. 3-16, 30 jun. 2023.