PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

OSMAR JOAO BARNEZE
29/05/2024 16:21

PORTARIA GP N.º 0581, DE 29 DE MAIO DE 2024.

ANEXO III

NSI03 – Política de Uso de Recursos de Tecnologia da Informação e Comunicação e Controle de Acesso

1. Objetivos

1.1. Estabelecer a Política de Uso de Recursos de Tecnologia da Informação e Comunicação e Controle de Acesso no âmbito do Tribunal Regional do Trabalho da 14ª Região.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2. Necessidade de definição de diretrizes voltadas à gestão dos recursos de tecnologia da informação.

2.3. Promover a segurança e continuidade das atividades do TRT da 14ª Região.

3. Referências normativas

3.1. Portaria GP 0436, de 13 de maio de 2021, do TRT da 14ª Região, que institui a Política de Segurança da Informação e Comunicação no âmbito do TRT da 14ª Região.

3.2. Norma Técnica ISO/IEC 27000:2018, que especifica conceitos e definições relacionados à segurança da informação.

3.3. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.4. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

3.5. Resolução CSJT nº 164, de 18 de março de 2016, que disciplina o uso e a concessão de certificados digitais institucionais no âmbito da Justiça do Trabalho de primeiro e segundo graus.

3.6. Lei 13.709 de 14 de agosto de 2018 (LGPD), que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

4. Conceitos e definições

4.1. Usuários: magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão;

4.2. Rede corporativa: conjunto de redes de dados locais e de longa distância (LAN/WAN), logicamente integradas, que oferecem serviços de comunicação interna de dados (intranet) e externa (internet) ao TRT da 14ª Região;

4.3. Certificado Digital A3: documento de identificação eletrônica, armazenado em mídia criptográfica (token), emitido por autoridade certificadora, que permite a identificação segura dos usuários no meio digital;

4.4. Recursos de TIC: impressoras, scanners, multifuncionais, computadores desktops computadores notebooks, servidores de rede, equipamentos de rede (switches, access points, roteadores, modems), equipamentos de infraestrutura de data center (storage, servidores Blade, appliance de segurança), sistemas informatizados, softwares, serviços de comunicação (internet e intranet) etc;

4.5. Ambiente Computacional: conjunto de hardware e software destinado ao processamento de dados.

4.6. SAU - Sistema de Atendimento ao Usuário: ferramenta de gestão dos serviços de atendimento prestados pela SETIC. Registra requisições ou incidentes oriundas dos usuários dos recursos de TIC.

4.7. Segurança da Informação: conjunto de regras que objetivam garantir a confidencialidade, integridade, disponibilidade e integridade da informação gerada.

5. Das contas de usuários

5.1. A Secretaria de Tecnologia da Informação e Comunicação (SETIC) realizará a habilitação inicial dos usuários para acesso à rede corporativa. A senha de acesso é de uso pessoal e intransferível, cabendo aos usuários mantê-la em sigilo, sendo vedada a sua cessão ou empréstimo sob qualquer pretexto.

5.2. A solicitação de habilitação inicial à rede corporativa deverá ser realizada mediante abertura de chamado técnico no Sistema de Atendimento ao Usuário (SAU) da SETIC e pode ser feito pela unidade de Recursos Humanos, quando do ingresso de novo magistrado/servidor, ou responsável pela unidade organizacional onde o usuário está lotado.

5.3. A senha de acesso inicial deverá ser alterada pelo usuário, conforme política de senha definida pela SETIC, no momento em que for realizado seu primeiro acesso ou sempre que solicitado pelo sistema.

5.4. Incumbe ao gestor da unidade ou à chefia imediata a conferência regular dos acessos concedidos aos servidores e estagiários vinculados a sua unidade, e sempre que possível, realizar os ajustes ativando ou desativando as permissões aos sistemas utilizados e, caso necessário, solicitar à SETIC mediante abertura de chamado técnico:

5.4.1. concessão dos acessos necessários ao desenvolvimento das atividades dos servidores e estagiários vinculados a sua unidade;

5.4.2. a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou estagiário da unidade, sempre que necessária sua adequação às atividades desenvolvidas;

5.4.3. a remoção dos acessos concedidos ao servidor ou estagiário, imediatamente após o afastamento ou desligamento da unidade;

5.5. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do servidor/estagiário que não faça mais parte de sua unidade.

5.6. A Secretaria de Gestão de Pessoas (SGEP), no âmbito de suas competências, comunicará à SETIC, mediante abertura de chamado técnico no SAU, os casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção e cessão a outro órgão, retorno à origem ou término do estágio de estudantes, ou ainda sempre que um usuário for desligado da instituição, para remoção de todos os acessos concedidos.

5.7. Os atos decorrentes da utilização dos sistemas informatizados, por meio de conta de acesso com identificação e senha, são de responsabilidade do usuário a qual a conta está formalmente vinculada.

5.8. Visando evitar acessos indevidos aos sistemas e serviços institucionais de TIC, os usuários devem:

5.8.1. Após o término das atividades realizadas na estação de trabalho, efetuar o encerramento da seção (*logoff*) ou o bloqueio da tela por senha;

5.8.2. Sempre que ausentar-se de sua estação de trabalho, realizar o bloqueio da tela por senha.

5.9. A SETIC implantará políticas para criação, renovação, bloqueio e expiração de senhas, com o intuito de aumentar o nível de segurança da rede corporativa.

5.10. Os usuários poderão ser responsabilizados, de forma irrefutável, pelo uso inadequado dos sistemas informatizados a partir de acessos realizados com suas credenciais.

5.11. O privilégio de usuário administrador para os computadores somente será concedido aos servidores da SETIC que necessitarem de acesso privilegiado para o estrito desempenho das suas atividades funcionais.

5.12. Os direitos de acesso à rede corporativa, à *internet* e aos sistemas informatizados, serão concedidos aos magistrados, servidores do quadro efetivo, servidores cedidos ou requisitados de outros órgãos, ocupantes de cargo em comissão e estagiários que estejam, necessariamente, desempenhando suas atividades laborais no TRT da 14ª Região de acordo com a necessidade de cada unidade judiciária ou administrativa e de acordo com a atribuição referente ao cargo,

mediante deferimento de perfis e níveis de acessos aprovados pelo Comitê de Segurança da Informação.

5.13. Os direitos de acesso a cada recurso serão configurados pela SETIC, devendo ser observadas as necessidades do serviço e poderão ser retirados ou restringidos por solicitação de magistrado, responsável pela unidade lotacional ou ainda, de forma imediata, pela SETIC, sempre que for comprovadamente identificado o uso inadequado dos recursos de TIC em situações que possam colocar em risco a segurança da rede corporativa.

5.14. O processo de Gestão de Usuários de sistemas informatizados deverá ser instituído com o objetivo principal de implementar boas práticas de segurança da informação na gestão de identidades e credenciais eletrônicas, bem como para o controle de acessos e privilégios aos sistemas, serviços de TIC e equipamentos de tecnologia da informação. O processo deverá contemplar os seguintes subprocessos: I - Gerenciamento de identidades; II - Gerenciamento de acessos; e III - Gerenciamento de privilégios.

5.15. Com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas institucionais, o processo de Gestão de Usuários de sistemas informatizados deverá, quando tecnicamente viável, adotar um padrão para utilização de credenciais de login único e interface de interação dos sistemas.

6. Do certificado digital

6.1. Aos usuários que justificarem a necessidade, será fornecido, pela Secretaria de Gestão de Pessoas, um certificado digital A3 com validade de 3 (três) anos.

6.2. O certificado digital é de uso pessoal, intransferível e hábil a produzir efeitos legais em todos os atos nos quais vier a ser utilizado, nos termos da legislação em vigor;

6.3. A utilização do certificado digital para qualquer operação implicará não repúdio e impedirá o titular de negar a autoria da operação ou de alegar que ela tenha sido praticada por terceiro;

6.4. O processo de emissão do certificado digital é composto pelas etapas de solicitação, validação presencial e gravação do certificado digital em mídia apropriada;

6.5. A renovação do certificado digital deverá ser realizada dentro do prazo de validade do certificado digital, em período não superior a 30 dias da data de expiração do certificado.

6.6. Os usuários deverão atentar-se para o prazo de expiração dos seus certificados, realizando processo de solicitação de novo certificado ou renovação dentro do prazo mencionado no parágrafo anterior.

6.7. O titular do certificado digital deverá custear a emissão de novo certificado ou ressarcir o erário em quaisquer das hipóteses abaixo:

6.7.1. Não renovação do certificado digital dentro do seu prazo de validade;

6.7.2. Renovação do certificado digital em desconformidade com o item 6, pelo valor proporcional ao tempo restante de validade do certificado;

6.7.3. Perda, extravio ou dano da mídia que resulte na inoperância do certificado digital, pelo valor proporcional ao tempo restante de validade do certificado;

6.7.4. Inutilização do certificado digital em razão de esquecimento da senha de utilização.

6.8. Para os demais casos, será observada a Resolução CSJT N. 164, de 18 de março de 2016, e suas eventuais alterações.

7. Do uso de criptografia e assinatura eletrônica

7.1. A criptografia de dados sensíveis será utilizada durante sua transmissão e armazenamento.

7.2. Os algoritmos de criptografia considerados seguros e utilizados pelo Tribunal serão os recomendados pelos órgãos reguladores e as melhores práticas da indústria, tais como AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), entre outros, de acordo com a necessidade e o contexto de cada aplicação.

7.3. Os dados armazenados em equipamentos portáteis, servidores e bancos de dados, sempre que possível, deverão ser criptografados para proteger contra acessos não autorizados.

7.4. O uso de assinatura eletrônica será utilizado para garantir a integridade e autenticidade de documentos gerados e armazenados nos sistemas utilizados pelo Tribunal.

8. Do acesso à *internet*

8.1. O acesso à *internet* dar-se-á, exclusivamente, por intermédio dos meios autorizados e configurados pela SETIC.

8.2. Excetuando-se os casos previstos neste ato e nas demais políticas internas de segurança da informação do TRT14, o acesso à *internet* provido pela rede corporativa deverá se restringir às páginas com conteúdo estritamente relacionado com as atividades laborais.

8.3. Possuem direito de acesso à *internet*, através da rede corporativa, os magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão que estejam lotados nas unidades do TRT da 14ª Região.

8.3.1. Prestadores de serviços terceirizados e estagiários poderão ter acesso à *internet* durante o período de prestação dos serviços ou estágio, observando as disposições aqui enumeradas, desde que formalmente solicitado e justificado pelo responsável da unidade onde está sendo prestado o serviço terceirizado ou estágio.

8.4. Aos magistrados e servidores que comprovadamente necessitem de acesso a *internet* móvel, serão fornecidos dispositivos de acesso a

internet móvel (modem 4G), com limite de pacote de dados definido conforme condições contratuais.

8.4.1. Os acessos realizados a partir dos dispositivos de *internet* móvel estão restritos às atividades laborais e enquadrados nas regras desta portaria e demais regras relativas aos Recursos de TIC estabelecidas.

8.5. Constituem uso indevido dos serviços de acesso à *internet* as seguintes ações:

8.5.1. Acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como: violência, pornografia, racismo, jogos etc;

8.5.2. Utilizar programas de troca de mensagens em tempo real (bate-papo), exceto os definidos como ferramenta de trabalho e homologados pela SETIC;

8.5.3. Acessar páginas de áudio e vídeo em tempo real ou sob demanda, exceto nos casos de comprovada necessidade, mediante solicitação e liberação da SETIC;

8.5.4. Excluem-se da proibição do item 7.5.3 os serviços de videoconferência homologados pela SETIC que forneçam recursos de comunicação entre magistrados, servidores e órgãos, notadamente aqueles que dão suporte ao regime de trabalho remoto/teletrabalho.

8.5.5. Obter na *internet* arquivos (*download*) que não estejam relacionados com suas atividades funcionais, a saber: imagens, áudio, vídeo, jogos e programas de qualquer tipo;

8.5.6. Acessar *sites* não confiáveis que possam apresentar vulnerabilidades de segurança ou que possam comprometer de alguma forma a segurança e integridade da rede corporativa e da segurança da informação.

8.6. É vedado aos usuários:

8.6.1. Utilizar-se de quaisquer meios que visem contornar os mecanismos de proteção e auditoria de acesso da rede corporativa do Tribunal ou que objetivem descaracterizar o acesso indevido às páginas ou serviços proibidos no artigo anterior;

8.6.2. Instalar em qualquer computador *softwares* que não tenham sido homologados pela SETIC, bem como a edição ou a execução de quaisquer arquivos alheios às atividades laborais;

8.6.3. Copiar programas de computador, licenças de *software* e sistemas implantados nas estações de trabalho, quer seja para uso externo, quer seja para uso em outra estação de trabalho do órgão;

8.6.4. Instalar quaisquer periféricos, componentes ou placas de *hardware* que não tenham sido adquiridos pelo Tribunal, exceto nos casos de comprovada necessidade e com acompanhamento de técnico qualificado da SETIC;

8.6.5. Conectar dispositivos não institucionais, portáteis ou não, na rede corporativa;

8.6.6. Conectar qualquer dispositivo, seja ativo ou passivo, independente de seu propósito, na rede corporativa, exceto aqueles homologados pela SETIC;

8.6.7. Utilizar qualquer tipo de tecnologia *wireless* que venha interferir no correto funcionamento da rede *wireless* do Tribunal, incluindo *access-points*, *bluetooth*, ancoragem *wi-fi*, etc;

8.6.8. Conectar qualquer dispositivo institucional em redes cabeadas ou sem fio não homologadas/institucionais, ou através de modems 3G/4G, exceto nos casos previamente autorizados pela SETIC;

8.6.9. Fazer acesso a sistemas de correio eletrônico que não sejam homologados pela SETIC;

8.6.10. Fornecer relação de endereços eletrônicos dos usuários do Tribunal para terceiros;

8.6.11. Armazenar, nas unidades de rede ou nas soluções baseadas em nuvem, arquivos não relacionados com as atividades institucionais, tais como: músicas, vídeos, fotos etc.

8.7. O acesso aos *sites* e serviços que estejam enquadrados como uso indevido, mas que sejam necessários ao desempenho das atribuições funcionais do usuário será liberado mediante solicitação com justificativa formal direcionada à SETIC.

8.8. A SETIC registrará os endereços das páginas acessadas pelos usuários e, sendo comprovada a utilização indevida do serviço de acesso à *internet*, o referido acesso será bloqueado ou restringido, com comunicação enviada ao superior hierárquico e, a depender dos riscos desta utilização, estes acessos serão apresentados ao Comitê de Segurança da Informação para tomada de providências.

8.9. Os parâmetros de configuração dos computadores serão definidos pela SETIC, que levará em conta os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional e da rede corporativa e não devem ser alterados pelos usuários a menos que seja orientado a fazê-lo pelos profissionais de suporte da SETIC.

8.10. Os *softwares* utilizados no ambiente computacional somente poderão ser instalados nas estações de trabalho por servidores da SETIC ou técnicos devidamente autorizados pela SETIC.

9. Do correio eletrônico e serviços de mensagens instantâneas

9.1. Aos magistrados e servidores do quadro efetivo em atividade, servidores cedidos ou requisitados de outros órgãos e ocupantes de cargo em comissão lotados no TRT da 14ª Região, será fornecida conta para acesso ao sistema de Correio Eletrônico (*e-mail*) e Comunicador Interno Institucional (*Chat*), que deverão ser utilizados de forma restrita para os objetivos e funções próprias e inerentes às suas atribuições e atividades funcionais.

9.2. A disponibilização de conta de e-mail e comunicador instantâneo a estagiários e colaboradores terceirizados é restrita e somente será realizada se atendidas, cumulativamente, as seguintes condições:

9.2.1. Existência de solicitação formal e fundamentada do chefe da unidade na qual estes colaboradores estiverem lotados;

9.2.2. Disponibilidade de licenças do serviço (contas ociosas) para atribuição imediata;

9.2.3. Deliberação e aprovação de cada solicitação pelo Comitê de Segurança da Informação.

9.3. O e-mail institucional é um instrumento de comunicação do TRT da 14ª Região que deve ser utilizado exclusivamente nas atividades laborais. É vedada a utilização do endereço corporativo na criação de contas particulares em plataformas de redes sociais ou qualquer tipo de conta na internet relacionada a webcommerce, streaming e serviços similares que não estejam ligados diretamente às atividades laborais.

9.4. As ferramentas de Correio Eletrônico e Comunicador Interno (*Google Chat*) são as principais ferramentas de comunicação e devem, de forma obrigatória, ser acessadas diariamente por todos os usuários.

9.5. Em caráter excepcional, o serviço de mensagens instantâneas *WhatsApp Web* poderá ser liberado às unidades que justificarem ser necessário, conveniente e adequado utilizá-lo com o propósito exclusivo de assuntos de interesse institucional do TRT14.

9.5.1. A liberação do acesso ao WhatsApp Web deverá ser solicitada à SETIC por meio de chamado técnico realizado via SAU, indicando qual o nome do usuário que terá acesso ao citado serviço.

9.5.2. Para a concessão de acesso ao WhatsApp Web, o solicitante deverá preencher o termo de consentimento e responsabilidade fornecido pelo suporte ao usuário no momento da solicitação.

9.5.2.1. Caso o WhatsApp Web seja solicitado pelo estagiário(a), o termo de consentimento deverá ser preenchido e assinado pelo gestor da unidade responsável.

9.5.3. A utilização do serviço tratado no item 8.5 é restrita a acessos realizados por contas associadas a números de telefones corporativos do TRT14 (celular ou fixo), pelo aplicativo *WhatsApp Business*.

9.5.4. O uso do serviço *WhatsApp Web* está restrito unicamente a assuntos de interesse institucional do TRT14, não sendo permitido, em hipótese alguma, sua utilização para finalidade diversa.

9.5.5. Dentro da rede corporativa, é vedado o recebimento de qualquer tipo de arquivo através do serviço WhatsApp Web, salvo nos casos em que controles adicionais tenham sido criados e implementados pela divisão de segurança da informação.

9.6. Os usuários devem manter os serviços de chat e e-mail ativos (*online)* sempre que o uso dos computadores estiver sendo realizado, mantendo-os ativos durante toda a jornada de trabalho.

9.7. As contas de correio eletrônico dos usuários serão desativadas e excluídas após 30 dias do desligamento do quadro funcional do Tribunal.

9.7.1. O eventual *backup* das mensagens e arquivos armazenados nas contas deverá ser solicitado à SETIC dentro do prazo supradescrito.

9.7.2. A exclusão da conta implicará na impossibilidade permanente de recuperação das mensagens e arquivos vinculados a ela.

9.7.3. O magistrado ou servidor efetivo desligado do quadro funcional deverá informar à Secretaria de Gestão de Pessoas um endereço de correio eletrônico pessoal, o qual será usado para os casos de comunicação de assuntos do seu interesse.

9.7.4. Para os fins deste artigo, considera-se desligamento do quadro funcional qualquer situação que desvincule o magistrado ou servidor da prestação de suas atividades funcionais ligadas diretamente ao TRT da 14ª Região, tais como: vacância, exoneração, aposentadoria, remoção, cedência, distribuição para outro órgão, falecimento etc.

9.8. O usuário deverá manter a capacidade de armazenamento de sua caixa postal dentro dos limites fornecidos pela SETIC, prezando pela limpeza periódica, eliminando mensagens desnecessárias.

9.9. Caracteriza-se uso inapropriado do serviço de correio eletrônico e serviços de mensagens instantâneas, enviar mensagens contendo:

9.9.1. Texto obsceno, ilegal, antiético, preconceituoso, discriminatório ou que atente flagrantemente a moral ou os bons costumes;

9.9.2. Conteúdo calunioso ou difamatório;

9.9.3. Listas de endereços eletrônicos dos usuários do Correio Eletrônico do Tribunal;

9.9.4. Vírus ou qualquer programa danoso;

9.9.5. Material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos, bem como material protegido por leis de propriedade intelectual;

9.9.6. Entretenimentos e correntes;

9.9.7. Assuntos ofensivos;

9.9.8. Imagens, áudio ou vídeo que não estejam relacionados ao desempenho das atividades funcionais;

9.9.9. Arquivos executáveis de qualquer tipo;

9.9.10. Mensagens comerciais não solicitadas, também conhecidas como *spam*;

9.9.11. Outros conteúdos notadamente fora do contexto do trabalho desenvolvido.

9.10. A ETIR - Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação da SETIC, deverá ser comunicada sempre que o usuário receber mensagens com os conteúdos descritos acima ou de remetentes desconhecidos e duvidosos que possam oferecer riscos à segurança da rede corporativa.

9.10.1. A comunicação à ETIR deve ser realizada por meio de mensagem de e-mail para o endereço etir@trt14.jus.br.

10. Do serviço de armazenamento de arquivos eletrônicos

10.1. A SETIC oferecerá serviços de armazenamento de arquivos eletrônicos a todos os magistrados e servidores em atividade e, excepcionalmente, a estagiários e outros usuários que, comprovadamente, necessitem do serviço para realização de trabalhos de interesse do TRT14.

10.2. O serviço de armazenamento de arquivos eletrônicos de que trata o artigo anterior será oferecido em duas modalidades:

10.2.1. Serviço de armazenamento de arquivos em rede: consiste em espaço de armazenamento de arquivos eletrônicos totalmente gerido pela SETIC que apresenta as seguintes características técnicas e operacionais:

10.2.1.1. Está hospedado na infraestrutura de datacenter do TRT14;

10.2.1.2. Tem capacidade limitada de acordo com a capacidade de infraestrutura disponível, atos e políticas da SETIC e com a natureza das atividades desenvolvidas pelos usuários;

10.2.1.3. Possui mecanismos de prevenção contra uso abusivo, tais como rejeição de arquivos de determinados tipos, rejeição de arquivos únicos com tamanho exagerado e outros controles, como descritos em políticas de armazenamento e segurança da SETIC;

10.2.1.4. Está coberto pela Política de *Backup* e Recuperação de arquivos da SETIC TRT14, com exceção das unidades de armazenamento de transferência temporária (por exemplo, unidade T, ou transfer).

10.2.2. Serviço de armazenamento em nuvem: consiste em espaço de armazenamento de arquivos eletrônicos parcialmente gerido pela SETIC que apresenta as seguintes características técnicas e operacionais:

10.2.2.1. Está hospedado em infraestrutura terceirizada (contratada) de computação em nuvem;

10.2.2.2. Tem capacidade limitada de acordo com os atos e políticas da SETIC e as limitações inerentes às contratações que regem os respectivos serviços;

10.2.2.3. Pode não fornecer meios de recuperação de arquivos totalmente apagados;

10.2.2.4. Pode possuir funcionalidades de compartilhamento de arquivos com outros usuários, inclusive externos ao TRT14, sendo responsabilidade de cada usuário os efeitos decorrentes do uso deste recurso;

10.2.2.5. Os arquivos armazenados nos drives compartilhados possuem como proprietário o Tribunal. Desta forma, após o desligamento do usuário, o encerramento de sua conta não ocasiona a perda das informações ali armazenadas;

10.2.2.6. Desde que expresso pelo proprietário, caso houver necessidade de migração dos arquivos armazenados no “Meu Drive”, este deverá solicitar a mudança de

proprietário dos arquivos de relevância para a instituição ou transferi-los para um drive compartilhado correspondente à sua unidade.

10.3. Visando proteger as informações institucionais, os usuários devem manter, sempre que possível, cópia dos arquivos de trabalho locais (hospedados apenas na estação de trabalho) em um dos serviços de armazenamento de arquivos eletrônicos especificados nos itens 9.2.1 e 9.2.2.

10.3.1. Em relação à geração e armazenamento de dados, os usuários devem observar a legislação vigente relacionada ao tratamento de dados pessoais e sensíveis, sendo proibido armazenar dados em desacordo com estas políticas nos serviços de armazenamento de rede definidos neste item e, principalmente, em unidades de armazenamento locais, como por exemplo, discos rígidos de estações de trabalho ou unidades de armazenamento externas.

10.3.2. Arquivos com dados pessoais ou sensíveis só podem ser mantidos armazenados localmente (nas estações de trabalho) pelo tempo necessário à realização do trabalho que motivou sua manipulação.

11. Do acesso aos Recursos de TIC

11.1. O acesso ao Centro de Dados do Tribunal e demais equipamentos de TIC - servidores de rede, computadores, *notebooks*, *scanners*, impressoras, multifuncionais, *racks*, *switches*, roteadores e outros - está restrito aos servidores da SETIC ou aos técnicos terceirizados devidamente autorizados pela SETIC.

11.2. Visando manter o adequado monitoramento dos serviços, o correto funcionamento da infraestrutura de rede, a longevidade dos equipamentos e atender aos requisitos de garantia, todos os equipamentos de rede (*switches*, roteadores, modens etc) devem permanecer energizados por *no-break*, ligados e conectados, exceto em casos previamente autorizados pela SETIC.

11.3. Eventual pedido de movimentação de equipamentos de TIC deverá ser feito pelos Gestores das unidades judiciárias ou administrativas, informando os motivos da solicitação à SETIC, a quem compete analisar a viabilidade técnica do pedido.

11.4. As movimentações internas e externas de equipamentos de TIC deverão ser registradas no Sistema de Movimentação de Bens, conforme regulamentação própria, sendo executadas pela SETIC ou pelo setor patrimonial do Tribunal.

11.4.1. Excepcionalmente, por necessidade de serviço, os magistrados e os diretores das unidades judiciárias e administrativas poderão autorizar a remessa à SETIC ou a retirada de estações de trabalho, servidores de rede, impressoras e outros equipamentos por funcionários devidamente identificados, registrando-se a ocorrência.

11.4.2. No caso de equipamentos retirados para manutenção, por empresa contratada para tal finalidade, deverá ser utilizado documento de autorização fornecido pela Secretaria de Tecnologia da Informação.

11.5. O acesso a dispositivos de armazenamento externos como *pen drives*, *HDs externos* e similares é vedado e possui bloqueio automático aplicado em todos os computadores corporativos. A eventual liberação de acesso desse tipo de dispositivo poderá ser realizada após a necessidade ter sido devidamente formalizada com justificativa relacionada diretamente às atividades laborais e, mediante avaliação da área de Segurança da Informação da SETIC, que sempre levará em conta os riscos associados.

12. Da Gestão e Controle de Ativos de Informação

12.1. O processo de Gestão e Controle de Ativos de Informação deverá ser instituído com o objetivo principal de implementar um conjunto coordenado de atividades voltadas para assegurar a preservação e o uso adequado dos ativos de informação institucionais, por meio do acompanhamento do seu ciclo de vida, desde a sua compra até o seu descarte.

12.2. O processo de que trata o caput deverá contemplar, no mínimo, as seguintes etapas: cadastro, atualização e exclusão de ativos.

12.3. Caberá aos gestores dos ativos de informação a execução do processo de Gestão e Controle de Ativos de Informação, sob a supervisão da Divisão de Segurança da Informação da Secretaria de Tecnologia da Informação e Comunicação.

12.4. O tratamento de ativos não autorizados será realizado através da implementação do protocolo 802.1x, ou, na sua ausência, pelo bloqueio ou liberação de seu acesso através do uso dos recursos disponíveis, nos termos deste ato.

13. Das disposições finais

13.1. Cada usuário é responsável pela Segurança da Informação do Órgão e deve conhecer, entender e cumprir as diretrizes, normas, procedimentos e instruções integrantes da Política de Segurança da Informação, zelando pela correta aplicação das medidas de proteção.

13.2. O usuário que apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, arquivo ou programa de computador, fizer uso indevido ou não autorizado dos equipamentos de TIC, bem como agir em desacordo com os termos deste ato fica sujeito à aplicação das penalidades administrativas, civis e penais cabíveis.

13.2.1. O disposto no item 11.2 aplica-se aos prestadores de serviços, aos estagiários, aos servidores e empregados de órgãos conveniados, no que couber.

13.2.2. Os diretores das unidades judiciárias e administrativas, verificando a existência de indícios de materialidade de qualquer fato descrito no item 11.2, comunicarão a ocorrência, de

imediato, ao superior hierárquico para adoção das providências cabíveis.

13.3. A SETIC deverá gerir a infraestrutura necessária para prover com segurança os serviços disponíveis na rede corporativa, assim como o acesso às redes externas, desenvolvendo as ações necessárias para o cumprimento deste ato.

13.4. Os casos omissos e as dúvidas surgidas na aplicação deste ato serão dirimidos pelo Comitê de Segurança da Informação, pelo Comitê de Gestão de TIC (CGesTIC) e pelo Comitê de Governança de TIC (CGTIC).