MINISTÉRIO PÚBLICO DA UNIÃO
ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO
DIRETORIA GERAL

PORTARIA Nº 0162, DE 30 DE NOVEMBRO DE 2021.

Regulamenta a Norma de Uso Aceitável de Recursos de Tecnologia da Informação na Escola Superior do Ministério Público da União.

O **DIRETOR-GERAL DA ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO**, no uso das atribuições que lhe foram conferidas pelos incisos I, II e XIV do art. 7º do Estatuto da ESMPU, aprovado pela Portaria PGR/MPU nº 95, de 20 de maio de 2020;

CONSIDERANDO o disposto na Portaria n° 92, de 13 de julho de 2021, que institui a Política de Segurança Institucional na Escola Superior do Ministério Público da União, e dá outras providências; RESOLVE:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1° Esta portaria estabelece a Norma de Uso Aceitável de Recursos de Tecnologia da Informação no âmbito da Escola Superior do Ministério Público da União (ESMPU) e entende que:

I – os recursos de tecnologia da informação englobam os equipamentos, serviços e sistemas de informação e infraestrutura de rede e de dados em uso institucional pela ESMPU, por exemplo:

a) estações de trabalho, microcomputadores de mesa (desktops) ou portáteis (notebooks);

b) dispositivos móveis institucionais (*smartphones, tablets, tokens*);

c) serviço de correio eletrônico;

d) canais de comunicação com a internet;

e) rede de dados cabeada, seus equipamentos e serviços;

f) rede de dados sem fio, seus equipamentos e serviços;

g) banco de dados institucionais;

h) sistemas de informação institucionais;

i) armazenamento de arquivos na rede interna;

j) serviços de tecnologia da informação em nuvem;

l) mecanismos de identificação digital, seus equipamentos e serviços;

m) equipamentos de impressão, digitalização e reprografia;

n) suprimentos e bens de consumo relacionados à tecnologia da informação.

II – os recursos de tecnologia da informação são fornecidos para que os usuários possam desempenhar suas atividades institucionais;

III – o usuário é responsável pelo correto uso dos recursos de tecnologia da informação a ele destinados, comunicando qualquer desvio, defeito ou comportamento anormal à área de tecnologia da informação;

IV – o usuário deve zelar pela segurança da informação ao que tiver acesso, de acordo com suas funções institucionais e o nível de sigilo da informação;

V – os equipamentos e recursos de tecnologia da informação devem ser utilizados com zelo e cuidado, de forma a garantir sua preservação e funcionamento adequado;

VI – a violação de dispositivos deste normativo poderá resultar em suspensão temporária de privilégios de acesso, após apuração dos fatos mediante procedimento interno da área de tecnologia da informação e comunicação ao Comitê Gestor de Segurança Institucional (CGSI);

VII – eventuais violações que também configurarem infração disciplinar serão encaminhadas à Diretoria-Geral para as providências cabíveis na esfera disciplinar ou criminal.

Parágrafo único. Esta norma de segurança da informação complementa a Política de Segurança da Informação nos Meios de Tecnologia da Informação da Escola Superior do

Ministério Público da União (PSIMTI/ESMPU), definindo as diretrizes para o uso aceitável dos recursos de tecnologia da informação por seus usuários autorizados.

CAPÍTULO II

DO USO ACEITÁVEL DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Seção I

Do Acesso

Art. 2° O acesso aos recursos de TI adotará os seguintes controles:

I – para a utilização dos recursos de tecnologia da informação da ESMPU é necessário o cadastramento do usuário e posterior liberação de acesso;

II – ao ser credenciado, o usuário será associado a um perfil, que indicará o nível de privilégio e os direitos de acesso aos recursos de tecnologia da informação;

III – solicitações de acesso a funcionalidades de sistemas de informação ou fontes de dados disponibilizadas em ferramentas de inteligência de negócio deverão ser previamente aprovadas pelos gestores de sistemas ou de dados;

IV – a credencial de acesso é pessoal e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, respondendo por qualquer violação ou ato irregular/ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua conta de acesso;

V – sempre que houver mudança de lotação ou desligamento do usuário, a área de tecnologia da informação deverá ser informada para que as alterações de acesso aos recursos de tecnologia da informação sejam providenciadas;

VI – o desligamento do usuário implicará na suspensão de todos os acessos;

VII – contas de usuário poderão ser bloqueadas após um longo período de inatividade, a ser definido pela área de tecnologia da informação;

Seção II

Da Segurança de Senhas para Contas de Usuários

Art. 3° A segurança de senhas para contas de usuários estabelece que:

I – as senhas associadas às credenciais de acesso a ativos/serviços de informação ou recursos computacionais da ESMPU são de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo;

II – as senhas de acessos iniciais dos usuários, quando fornecidas pela área de tecnologia da informação, deverão ser trocadas pelos usuários imediatamente após o seu recebimento;

III – os critérios mínimos de segurança de senhas das contas de usuários serão definidos pela área de tecnologia da informação.

Seção III

Do Acesso Remoto

Art. 4° Para o acesso remoto aos recursos de tecnologia da informação a partir de ambiente externo às dependências da ESMPU:

I – os recursos de TI e perfis de usuários autorizados para acesso remoto serão definidos pela área de tecnologia da informação;

II – nesta modalidade de acesso, serão aplicadas as mesmas restrições ao usuário quando da utilização dos recursos de tecnologia da informação no ambiente interno da ESMPU;

III – o acesso remoto deverá ser solicitado à área de tecnologia e destinado ao uso exclusivo do usuário solicitante;

IV – a configuração de equipamento particular será de responsabilidade do usuário, cabendo à área de tecnologia da informação a orientação através de roteiros, manuais ou procedimentos específicos sobre as configurações e pré-requisitos de segurança que estes dispositivos deverão cumprir para obter este tipo de acesso;

V – em caso de desconformidade de equipamentos com os critérios de configuração e segurança adotados, os acessos poderão ser bloqueados pela área de tecnologia da informação.

Seção IV

Das Estações de Trabalho e Dispositivos Móveis Institucionais

Art. 5° Em vista da segurança das estações de trabalho e dispositivos móveis institucionais e entendendo que, as estações de trabalho representam os microcomputadores de mesa (*desktops*) ou portáteis (*notebooks*) adquiridos pelo órgão, bem como seus periféricos, e os dispositivos móveis institucionais englobam, por exemplo, celulares, *tablets* e *tokens*:

I – o usuário deverá zelar pelas condições adequadas de instalação, preservação e uso dos equipamentos, com atenção especial ao cabeamento do equipamento, que deverá ser mantido em boas condições e manuseado com o devido cuidado. Caso note qualquer anormalidade, deverá comunicar o fato à área de tecnologia da informação;

II – é vedada a instalação de qualquer software sem a prévia homologação da área de tecnologia da informação;

III – é vedada a cópia dos softwares e sistemas implantados nas estações de trabalho ou dispositivos móveis para uso em outros locais, salvo por autorização em contrário;

IV – os dados referentes às atividades institucionais deverão obrigatoriamente ser salvos nas unidades de armazenamento de rede, nuvem institucional, ou outro recurso disponibilizado pela área de tecnologia da informação;

V – a manutenção técnica das estações de trabalho é uma atribuição específica da área de tecnologia da informação que, a seu critério, poderá delegar formalmente a outro responsável;

VI – cabe à área de tecnologia da informação providenciar a desconexão dos equipamentos e a sua instalação no local de destino;

VII – as estações de trabalho e seus periféricos somente poderão ser removidos dos locais de instalação pela área de patrimônio;

VIII – em caso de manutenção, atualização, troca ou devolução de equipamento de trabalho, a cópia de segurança (backup) dos dados é de inteira responsabilidade do usuário. Não será efetuado backup de dados armazenados nas estações de trabalho, dispositivos móveis ou em outro local não disponibilizado pela área de tecnologia da informação;

IX – os procedimentos e as operações realizadas por intermédio das estações de trabalho e dispositivos móveis institucionais serão de responsabilidade dos usuários que estiverem autenticados;

X – na hipótese de necessidade comprovada de utilização de equipamento pessoal para o desempenho de atividades profissionais dentro da rede corporativa, este deverá passar por

inspeção da área de tecnologia da informação, a fim de garantir os adequados requisitos e controles de segurança.

Seção V

Do Serviço de Correio Eletrônico

Art. 6° Quanto ao serviço de correio eletrônico:

I – prestar-se-á exclusivamente ao envio e recebimento de mensagens com conteúdo relacionado às funções institucionais;

II – não será permitida a utilização de outros serviços similares que não o oficialmente fornecido pela ESMPU para exercício da atividade funcional, salvo em caso de indisponibilidade;

III – as unidades da ESMPU poderão solicitar, com a devida justificativa, a criação de caixas postais institucionais, temporárias ou de caráter definitivo, que serão configuradas de acordo com a viabilidade técnica e orçamentária:

a) as unidades deverão indicar um responsável pela caixa postal institucional, que terá o poder de conceder e revogar o acesso aos demais usuários cabíveis e deverá gerenciar esta conta para que não ocorra acessos não-autorizados;

b) em caso de mudança do responsável pela caixa postal institucional, a unidade deverá indicar formalmente um novo responsável.

IV – os endereços de correio eletrônico serão criados conforme os padrões definidos pela área de tecnologia da informação;

V – o tamanho das caixas postais e anexos, o período de retenção das mensagens e critérios de backup serão definidos pela área de tecnologia da informação e limitados de acordo com os recursos disponíveis;

VI – as caixas e mensagens de correio eletrônico poderão ser automaticamente expiradas e eliminadas conforme critérios técnicos definidos pela área de tecnologia da informação;

VII – é vedado o uso dos recursos do correio eletrônico para a veiculação de mensagens que não sejam de interesse institucional, como de caráter político-partidário, religioso, publicitário, pessoal, comercial e de “correntes” de qualquer natureza, bem como divulgar informações confidenciais ou privilegiadas, obtidas em razão do cargo e, também, que possam comprometer a honra ou a fama alheia.

Seção VI

Do Acesso a Internet

Art. 7° O acesso à internet é fornecido aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas funções institucionais e:

I – toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet corporativa está sujeita a monitoramento e auditoria, com o objetivo de mitigar incidentes de segurança e otimizar a utilização dos canais de acesso à internet;

II – durante o monitoramento ou auditoria do acesso à internet, a ESMPU se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;

III – os limites de largura de banda, tanto de *upload* quanto de *download*, poderão ser alterados pela área de tecnologia da informação para manter os níveis adequados de internet para as atividades essenciais da instituição;

IV – durante o acesso à Internet fornecido pela ESMPU não será permitido o *download*, o *upload*, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento e/ou a cópia de qualquer conteúdo relacionado, direta ou indiretamente, salvo nos casos relacionados às atividades funcionais, com:

a) qualquer espécie de exploração sexual;

b) qualquer forma de conteúdo adulto, erotismo, pornografia;

c) qualquer forma de ameaça, chantagem e assédio moral ou sexual;

d) qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

e) preconceito baseado em cor, sexo, orientação sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

f) incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam estas lícitas ou não;

g) a prática e/ou a incitação de crimes ou contravenções penais;

h) a prática de propaganda política nacional ou internacional;

i) a prática de quaisquer atividades comerciais desleais;

j) o desrespeito a imagem ou aos direitos de propriedade intelectual da ESMPU;

l) a disseminação de códigos maliciosos e ameaças virtuais;

m) tentativa de expor a infraestrutura computacional da ESMPU a ameaças virtuais;

n) divulgação não autorizada de qualquer informação da ESMPU classificada como confidencial ou de uso interno;

o) uso de sites, aplicativos ou serviços que busquem contornar controles de acesso à internet.

Seção VII

Da Rede de Dados Cabeada

Art. 8° É vedada a conexão de equipamentos particulares na rede corporativa cabeada sem autorização prévia e inspeção pela área de tecnologia da informação.

Seção VIII

Da Rede de Dados Sem Fio

Art. 9° Os acessos a rede sem fio serão concedidos:

I – para a rede corporativa sem fio através de equipamentos institucionais homologados, salvo em casos excepcionais com o devido aval da área de tecnologia da informação;

II – para a rede sem fio de usuários visitantes conforme critérios estabelecidos pela área de tecnologia da informação. Caberão a estes usuários a realização das configurações necessárias ao acesso de seus equipamentos particulares para esta modalidade de rede de dados sem fio.

Seção IX

Dos Bancos de Dados

Art. 10. Serão considerados bancos de dados homologados as tecnologias de bancos de dados em que a área de tecnologia da informação, em especial a área de banco de dados, possuir o devido treinamento e conhecimento técnico para o devido suporte, portanto:

I – novas soluções de tecnologia da informação, sejam desenvolvidas, adquiridas ou cedidas, utilizarão preferencialmente banco de dados homologado;

II – a lista de bancos de dados homologados será disponibilizada pela área de tecnologia da informação;

III – solicitações de acesso a bancos de dados institucionais por usuários externos à área de tecnologia da informação deverão ser aprovadas primeiramente por todos os gestores dos sistemas que gerem os dados envolvidos;

IV – os procedimentos desta seção aplicam-se também a procedimentos de cópia de bases de dados (no todo ou em parte) com a finalidade de disponibilização de dados a terceiros;

V – caberá aos gestores dos sistemas, com o auxílio da área de tecnologia da informação, informar quais dados devem ser ofuscados, mascarados, criptografados ou removidos na cópia, observando-se os limites técnicos e tecnológicos disponíveis;

VI – a criação e disponibilização de fontes de dados em ferramentas de inteligência de negócio, caracterizadas por extrações ou acessos em tempo real aos bancos de dados homologados da ESMPU, deverá ser validada pelos gestores dos dados envolvidos.

Seção X

Dos Sistemas de Informação Institucionais

Art. 11. Um sistema de informação é considerado institucional quando é homologado pela área de tecnologia da informação ou inserido no catálogo de sistemas corporativos:

I – pode ser desenvolvido internamente, ou ainda adquirido, contratado ou instalado;

II – os usuários e gestores dos sistemas de informação deverão zelar pelo uso desses sistemas, pelas credenciais de acesso e pelo sigilo e preenchimento consciente e confiável das informações.

Seção XI

Do Armazenamento de Arquivos na Rede Interna

Art. 12. É disponibilizado aos usuários internos espaço para armazenamento de arquivos em rede, através da infraestrutura de servidor de arquivos da ESMPU, sendo que:

I – é vedada a utilização para armazenamento de arquivos que não possuam vinculação com as atividades institucionais;

II – cada usuário será responsável pela salvaguarda dos arquivos ou informações consideradas sensíveis a ESMPU;

III – os conteúdos de pastas que não possuam vinculação com as atividades institucionais, ou que infrinjam leis, especialmente aquelas relacionadas a direitos autorais, poderão ser removidos pela área de tecnologia da informação assim que detectados;

IV – é vedada a criação, remoção ou transmissão de arquivos que venham a comprometer o desempenho e funcionamento da rede de dados corporativa;

V – a área de tecnologia da informação poderá realizar a remoção ou indicar outro meio de armazenamento nos casos em que o tamanho dos arquivos onere a estrutura de armazenamento da ESMPU ou que possam causar algum incidente de segurança da informação;

VI – o tamanho das áreas de armazenamento de arquivos, o período de retenção e critérios de backup serão definidos pela área de tecnologia da informação e limitados de acordo com os recursos disponíveis;

VII – poderá ser disponibilizado espaço para armazenamento de arquivos em nuvem através de solução corporativa, sujeita às mesmas restrições de uso.

Seção XII

Dos Serviços em Nuvem

Art. 13. Os recursos de tecnologia da informação poderão ser hospedados externamente às dependências da ESMPU em ambiente de nuvem, sujeitos às mesmas condições de uso e restrições presentes neste normativo.

Seção XIII

Da Identificação Digital

Art. 14. Serão fornecidos certificados digitais para seus colaboradores, de acordo com as atribuições funcionais , necessidade de serviço e:

I – cabe exclusivamente ao usuário a conservação de seu certificado digital, independentemente do equipamento que o suporte, bem como de qualquer tipo de senha ou meio de autenticação relacionado ao mesmo;

II – o usuário deverá informar sobre quaisquer eventos ou suspeitas relativas ao comprometimento de sua senha e/ou o uso indevido de seu certificado digital.

Seção XIV

Dos Equipamentos de Impressão, Digitalização e Reprografia

Art. 15. O uso de equipamentos de impressão e reprografia (fotocopiadoras) deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da ESMPU ou que estejam relacionados com o desempenho das funções institucionais e:

I – o usuário deverá providenciar a retirada de documentos da impressora ou fotocopiadora que tenha solicitado a impressão, transmissão ou cópia que contenham informações da ESMPU, classificadas como de uso interno ou confidencial, devendo os mesmos serem descartados de acordo com os procedimentos adotados pela ESMPU;

II – a impressão ou cópia de documento em suporte físico deverá ser limitada à quantidade exata necessária para a tarefa determinada;

III – a área de tecnologia da informação poderá ativar quotas de impressão no intuito de obter maior gerência sobre o crescimento de uso deste recurso;

IV – é vedado o reaproveitamento de páginas já impressas e contendo informações classificadas como confidenciais, devendo as mesmas serem descartadas de acordo com os procedimentos adotados pela ESMPU;

Seção XV

Da Segurança Física

Art. 16. As instalações do centro de processamento de dados (CPD) da ESMPU serão mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado, a danos e interferências de origem humana ou natural.

Parágrafo único. O acesso às salas técnicas ou a instalações que contenham equipamentos de uso exclusivo da área de tecnologia da informação somente poderá ser realizado mediante autorização e supervisão de servidor desta unidade, salvo no caso de emergências.

Seção XVI

Do Monitoramento e Auditoria

Art. 17. A área de tecnologia da informação poderá implementar medidas de monitoramento e auditoria que contemplem as seguintes ações:

I – monitorar, armazenar, analisar conteúdo, filtrar ou impedir o tráfego de rede, de internet e de mensagens de correio eletrônico, conforme critérios por ela definidos e, nos casos excepcionais, pela Diretoria-Geral, com o objetivo de garantir o cumprimento das normas de segurança da informação, mitigar incidentes de segurança e otimizar a utilização dos recursos de tecnologia da informação;

II – promover auditorias no tráfego de rede e internet ou de mensagens de correio eletrônico, de ofício, ou por solicitação da Diretoria-Geral, para garantir a manutenção da disponibilidade dos recursos de tecnologia da informação;

III – promover inspeções em recursos de tecnologia da informação da ESMPU com o objetivo de verificar a existência de vírus, softwares não licenciados, conteúdo que viole direitos autorais ou propriedade intelectual, e para apurar a conformidade com as normas de segurança da informação;

IV – suspender serviços de rede, desligar equipamentos ou bloquear acessos, apagar arquivos ou mensagens de correio eletrônico, quando tal procedimento se fizer necessário para se restabelecer a operação normal de serviços ou para proteger recursos de tecnologia da informação, devendo ser restabelecida a operação normal assim que cessar a ameaça identificada;

V – limitar os espaços em áreas de armazenamento destinadas a arquivos ou mensagens de correio eletrônico, de acordo com a disponibilidade de ativos de tecnologia da informação;

VI – bloquear temporariamente contas de rede, contas de correio eletrônico e outras contas de acesso quando for essencial para garantir ou para preservar a segurança da informação, devendo o acesso ser liberado imediatamente após cessado o evento que deu causa ao bloqueio.

CAPÍTULO III

DAS DISPOSIÇÕES FINAIS

Art. 18. Regulamentações específicas decorrentes deste normativo serão definidas e disponibilizadas pela área de tecnologia da informação na intranet da ESMPU.

Art. 19. Os casos omissos e as dúvidas surgidas na aplicação do presente normativo serão dirimidos pela Diretoria-Geral, com o apoio técnico da área de tecnologia da informação.

Art. 20. Esta norma será revisada com periodicidade bianual ou extraordinariamente, quando necessário.

ALCIDES MARTINS
Diretor-Geral da ESMPU

Documento assinado eletronicamente por **Alcides Martins**, **Diretor-Geral**, em 30/11/2021, às 12:40 (horário de Brasília), conforme a Portaria ESMPU nº 21, de 3 de março de 2017.

A autenticidade do documento pode ser conferida no site https://sei.escola.mpu.mp.br/sei/autenticidade informando o código verificador **0309922** e o código CRC **EB8BC81D**.