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

PORTARIA Nº 0161, DE 30 DE NOVEMBRO DE 2021.

Regulamenta a Política de Segurança da Informação nos Meios de Tecnologia da Informação (PSIMTI) 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 Política de Segurança da Informação nos Meios de Tecnologia da Informação no âmbito da Escola Superior do Ministério Público da União (ESMPU) e entende que:

I – a informação corporativa é um bem essencial para suas atividades e também para resguardar a qualidade e a garantia dos serviços prestados; e

II – sua manipulação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança de seus dados corporativos;

III – trata-se de uma norma complementar à PSI - Política de Segurança Institucional e parte integrante do seu sistema de gestão corporativo, alinhada com as boas práticas e normas de referência na temática: ABNT NBR ISO/IEC 27001 e 27002; Marco Civil da Internet – Lei n° 12.965/2014; Lei Geral de Proteção de Dados (LGPD) – Leis: n° 13.709/2018 e n°

13.853/2019; resoluções CNMP N° 156/2016 – Segurança Institucional do MPU e CNMP N° 171/2017 – Política Nacional de TI; normas complementares GSI/PR Nº 1/2008 e Portaria PGR/MPF Nº 417/2013 - Plano de Segurança Institucional do MPF;

Parágrafo único. As disposições desta política aplica-se a todos os usuários de informação, incluindo qualquer indivíduo ou organização que, em algum momento, possuiu vínculo ou obteve acesso às informações institucionais ou fez uso de recursos de tecnologia da informação disponibilizados pela Escola.

Seção I

Glossário

Art. 2° Em caráter explicativo, expõem-se alguns termos utilizados neste normativo:

I – ATIVO: Tudo aquilo que possui valor para a ESMPU;

II – ATIVO DE INFORMAÇÃO: Patrimônio intangível da ESMPU, constituído por informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a ESMPU por parceiros ou terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitada pela infraestrutura computacional da ESMPU ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico ou mídia eletrônica transitados dentro e fora de sua estrutura física.

III – CONFIDENCIALIDADE: Propriedade dos ativos da informação da ESMPU, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas;

IV – INTEGRIDADE: Propriedade dos ativos da informação da ESMPU, de serem exatos e completos.

V – DISPONIBILIDADE: Propriedade dos ativos da informação da ESMPU, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas;

VI – SEGURANÇA DA INFORMAÇÃO: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da ESMPU.

VII – AMEAÇA: Causa potencial de um incidente, que pode vir a prejudicar a ESMPU;

VIII – VULNERABILIDADE: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da ESMPU

IX – INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da ESMPU;

X – RISCO DE SEGURANÇA DA INFORMAÇÃO: Efeito da incerteza sobre os objetivos de segurança da informação da ESMPU;

XI – CONTROLE DE SEGURANÇA DA INFORMAÇÃO: Medida de segurança adotada pela ESMPU para o tratamento de um risco específico;

XII – METADADOS: Dados secundários utilizados para descrever a estrutura de um dado principal, exemplo: criador do arquivo, data de modificação do arquivo, versão do arquivo, etc;

XIII – GESTOR DA INFORMAÇÃO: Usuário da informação ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

XIV – USUÁRIO DA INFORMAÇÃO: Colaboradores de qualquer área ou terceiros alocados na prestação de serviços a ESMPU, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a manipular qualquer ativo de informação da ESMPU para o desempenho de suas atividades profissionais;

CAPÍTULO II

DA SEGURANÇA DA INFORMAÇÃO NOS MEIOS DA TECNOLOGIA DA INFORMAÇÃO

Seção I

Das Diretrizes

Art. 3° A PSIMTI observará as seguintes diretrizes:

I – elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação nos meios da tecnologia da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade sejam atingidos através da adoção de controles contra ameaças provenientes de fontes externas e internas;

II – garantir a educação e conscientização de todos os níveis da organização sobre as práticas de segurança da informação e disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas;

III – atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

IV – tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades apropriadas;

V – garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

VI – melhorar continuamente a gestão de segurança da informação através da definição e revisão sistemática dos objetivos de segurança em todos os níveis da organização;

Seção II

Dos Objetivos

Art. 4° A PSIMTI tem por objetivos:

I – garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação nos meios da tecnologia da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos na instituição;

II – adotar padrões de comportamento seguros, adequados às metas e necessidades da Escola, com o objetivo de garantir níveis adequados de proteção as informações da instituição ou sob sua responsabilidade;

III – orientar quanto à adoção de controles e processos para atendimento dos requisitos de segurança da informação;

IV – resguardar as informações da ESMPU, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

V – prevenir possíveis causas de incidentes e a responsabilização legal da instituição, de seus colaboradores, parceiros e público; e

VI – minimizar os impactos às atividades acadêmicas e administrativas como resultado de falhas de segurança assim como manter a continuidade dos negócios da ESMPU.

Seção III

Das Atribuições

Art. 5° Os principais agentes envolvidos nesta política são:

I – NÚCLEO DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO (NUSEG), responsável pela gerência da segurança da informação nos meios de tecnologia da informação, que consiste em:

a) conduzir a gestão e operação da segurança da informação nos meios de tecnologia da informação, tendo como base esta política e demais normativos ou procedimentos;

b) elaborar e propor as normas e procedimentos de segurança da informação necessários para se fazer cumprir a PSIMTI;

c) identificar e avaliar as principais ameaças à segurança da informação, bem como propor e implantar medidas para reduzir o risco;

d) responder aos incidentes de segurança da informação, com apoio da Secretaria de Tecnologia da Informação, garantindo tratamento adequado.

II – GESTOR DA INFORMAÇÃO. Suas atribuições consistem em:

a) gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela ESMPU;

b) identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela ESMPU;

c) zelar pela qualidade e integridade das informações sob sua responsabilidade;

d) atuar, juntamente com os Gestores de Sistemas, na gestão dos acessos à informação e sistemas de informação sob sua responsabilidade.

III – USUÁRIOS DA INFORMAÇÃO. Suas atribuições consistem em:

a) ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação nos Meios de Tecnologia da Informação, bem como as demais normas e procedimentos de segurança aplicáveis.

b) encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre esta política, suas normas e procedimentos à NUSEG ou, quando pertinente, à STI;

c) comunicar à NUSEG qualquer evento que viole esta política ou que coloque ou possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da ESMPU;

d) responder pela inobservância desta política, bem como as demais normas e procedimentos de segurança aplicáveis, conforme definido no capítulo II, seção III, sanções e punições.

Seção IV

Das Sanções e Punições

Art. 6° A PSIMTI prever que:

I – as violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança da informação, serão passíveis de penalidades administrativas cujas sanções e punições serão analisadas por autoridade competente, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas em lei;

II – no caso de terceiros contratados ou prestadores de serviço, o incidente deverá ser comunicado ao Comitê Gestor de Segurança Institucional (CGSI) e também ao gestor do contrato que tomará as medidas cabíveis;

III – para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a ESMPU, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos incisos I e II desta seção.

Seção V

Dos Casos Omissos

Art. 7° Os casos omissos e as dúvidas surgidas na aplicação deste normativo serão dirimidos pela Diretoria-Geral, com o apoio do CGSI e do NUSEG.

Parágrafo único. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança da informação, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da ESMPU adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da ESMPU.

CAPÍTULO III

DAS DISPOSIÇÕES FINAIS

Art. 8° A Política de Segurança da Informação nos Meios de Tecnologia da Informação é aprovada pela Alta Direção da ESMPU e delega à STI a publicação de normativos e procedimentos de segurança que venham a compô-la.

Art. 9° Esta norma será revisada com periodicidade bianual ou extraordinariamente, quando necessário.

Art. 10. Esta Portaria entra em vigor na data de sua publicação.

ALCIDES MARTINS
Diretor-Geral da ESMPU

Documento assinado eletronicamente por **Alcides Martins**, **Diretor-Geral**, em 30/11/2021, às 12:26 (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 **0309916** e o código CRC **701B0754**.