UNIVERSIDADE ESTADUAL DE PONTA GROSSA

Av. General Carlos Cavalcanti, 4748 - Bairro Uvaranas - CEP 84030-900 - Ponta Grossa - PR - https://uepg.br - (42) 3220-3000

PORTARIA R. - Nº 2023.43

O REITOR DA UNIVERSIDADE ESTADUAL DE PONTA GROSSA, no uso de suas atribuições legais e estatutárias,

R E S O L V E:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação da Universidade Estadual de Ponta Grossa – UEPG.

Art. 2º Esta Portaria entrará em vigor na data de sua publicação. Reitoria da Universidade Estadual de Ponta Grossa.

Ponta Grossa, 07 de fevereiro de 2023.

Miguel Sanches Neto,

Reitor.

Documento assinado eletronicamente por **Miguel Sanches Neto**, **Reitor**, em 08/02/2023, às 14:02, conforme Resolução UEPG CA 114/2018 e art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.uepg.br/autenticidade informando o código verificador **1304680** e o código CRC **238EF5C3**.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE ESTADUAL DE PONTA GROSSA

CAPÍTULO I
OBJETIVO

Art. 1º A Política de Segurança da Informação e Comunicação da Universidade Estadual de Ponta Grossa – UEPG tem como objetivo estabelecer princípios, diretrizes e deveres no âmbito da segurança da informação para toda a Instituição e deve garantir:

I - a operacionalidade e a usabilidade dos recursos providos;

II - a conformidade legal;

III - o uso seguro dos recursos providos.

Art. 2º São objetivos desta política:

I - tratar a informação como um patrimônio, protegendo-a de acordo com sua classificação e seu grau de exposição a riscos;

II - garantir as propriedades fundamentais: integridade, disponibilidade, confidencialidade e autenticidade das informações e o não repúdio das ações a elas relacionadas;

III - estabelecer e padronizar práticas de segurança da informação na UEPG;

IV - assegurar a adequação dos processos e práticas da UEPG aos requisitos legais relativos à segurança da informação.

Art. 3º As medidas de segurança da informação e comunicação devem ser planejadas, aplicadas, implementadas e, periodicamente, avaliadas de acordo com os objetivos institucionais e os riscos para as atividades da UEPG.

CAPÍTULO II
ESCOPO

Art. 4º Esta política aplica-se:

I - a todos os usuários da UEPG;

II - às informações armazenadas em meios físicos de propriedade ou sob a guarda da UEPG;

III - a todos os ambientes computacionais e informações neles armazenadas, de propriedade ou sob a guarda da UEPG;

IV - aos contratos, convênios, acordos, termos e demais meios jurídicos celebrados pela UEPG.

Art. 5º Cabe ao usuário de informações a observância das regras e fica vedado alegar desconhecimento desta política.

§ 1º Esta política deve ser comunicada e largamente divulgada, garantindo que todos a conheçam e a pratiquem.

§ 2º A inobservância das políticas e normas de segurança sujeita o usuário a sanções internas e às demais sanções previstas na legislação, que eventualmente incidam sobre o caso.

CAPÍTULO III
PRINCÍPIOS E DIRETRIZES

Art. 6º São princípios da segurança da informação na UEPG:

I - privacidade: proteção dos dados pessoais para a garantia do direito fundamental a inviolabilidade da privacidade e intimidade;

II - proteção: zelo pela proteção das informações, independente do meio em que são armazenadas ou do ambiente em que estejam sendo processadas ou transitando;

III - adaptação: adoção de medidas de seguranças flexíveis para atender as necessidades e suportar a evolução tecnológica;

IV - proporcionalidade: adequação dos custos das ações de segurança da informação ao valor dos ativos e informações, considerando os riscos a que estão expostos, seguindo critérios de proporcionalidade;

V - prevenção: trabalhar de forma proativa para obtenção dos objetivos de segurança da informação.

Art. 7º Os princípios da segurança da informação na UEPG devem garantir:

I - a funcionalidade, a segurança e a estabilidade da infraestrutura de tecnologia de informação da UEPG;

II - o cumprimento às obrigações legais e regulatórias aplicáveis;

III - preservar e proteger as informações sob a responsabilidade da UEPG, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação (TIC), dos diversos tipos de ameaças e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato;

IV - prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

Art. 8º São diretrizes da segurança da informação na UEPG:

I - responsabilidade e comprometimento: compreender que a segurança da informação é responsabilidade de todos os usuários;

II - treinamento e conscientização: estabelecer iniciativas e programas de treinamento que fomentem a cultura de segurança da informação na UEPG;

III - gestão de riscos: avaliar riscos de segurança da informação por meio de processos contínuos;

IV - controle de acesso: controlar acessos de qualquer natureza aos ambientes físicos ou computacionais a fim de definir ações permitidas e garantir rastreabilidade, identificação do usuário e ações executadas;

V - contratações e aquisições seguras: incluir nos contratos, acordos, convênios e demais instrumentos legais, quando aplicável, especificações de segurança da informação que definam, ao menos, regras de transferência das informações, limites de eventuais tratamentos de dados pessoais e obrigações de atendimento a normas da UEPG;

VI - privacidade e proteção de dados pessoais: garantir os direitos e a privacidade dos titulares de dados pessoais e o tratamento adequado destes dados;

VII - desenvolvimento seguro: seguir princípios de segurança da informação e proteção de dados desde o planejamento e concepção até a execução em qualquer projeto de software desenvolvido, projetado, contratado ou mantido pela UEPG;

VIII - ambiente computacional seguro: manter o ambiente de hardware e software atualizado, em particular no que diz respeito a atualizações de segurança;

IX - identificação segura: conceder aos usuários contas pessoas intransferíveis e que não devem ser compartilhadas com terceiros.

CAPÍTULO IV
TERMOS E DEFINIÇÕES

Art. 9º Para os fins desta política são adotados os seguintes conceitos:

I - autenticidade: Consiste na garantia da veracidade da fonte das informações;

II - confidencialidade: Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações;

III - disponibilidade: Consiste na garantia de que as informações estejam acessíveis, a qualquer momento requerido, durante o período acordado;

IV - integridade: Assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - não-repúdio: Previne uma origem ou destino de negar a transmissão de mensagens, isto é, quando dada mensagem é enviada, o destino pode provar que esta foi realmente enviada por determinada origem, e vice-versa;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - ativo da informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios e também os recursos humanos que a eles têm acesso;

VIII - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

IX - incidente de segurança da informação: Um evento único ou uma série de eventos de segurança da informação indesejados ou inesperados, que possam comprometer as operações da UEPG ou violar sua política de uso.

CAPÍTULO V
NORMAS E RESPONSABILIDADES

Art. 10. Para o cumprimento das diretrizes desta política serão editadas normas de segurança da informação, dentro do contexto de cada atividade.

Parágrafo único. De acordo com a atividade, poderão ser detalhados diversos níveis destas normas, incluindo procedimentos operacionais, conforme normativas vigentes.

Art. 11. Cabe a todos os usuários abrangidos por esta política:

I - proteger as informações contra uso, acesso, divulgação, modificação ou destruição não autorizados conforme esta política;

II - notificar ocorrências de descumprimento das normas ou demais assuntos relacionados à segurança da informação, d e acordo com instrução normativa específica;

III - proteger suas contas pessoais contra o uso indevido;

IV - zelar pelo cumprimento desta política, difundindo-a internamente e priorizando ações para sua aplicação;

V - reportar eventuais dificuldades ou descumprimentos desta política, a fim de planejar ações de remediação, de acordo com instrução normativa específica;

VI - responder por eventuais violações dessa política.

CAPÍTULO VI
VIOLAÇÕES

Art. 12. As violações desta política e das demais normas de segurança aplicáveis, mesmo que por omissão ou tentativa não consumada, serão passíveis de penalidades.

Parágrafo único. Violações que, comprovadamente, exponham a infraestrutura da UEPG a situações que o afete, com prejuízo à sua operacionalidade, usabilidade, imagem ou que afete outros componentes do sistema, estarão sujeitas a medidas de mitigação emergenciais para reestabelecer a normalidade do sistema.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 13. Esta política e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura da UEPG ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente, conforme legislação vigente, sendo atualizados quando necessário.

Art. 14. Esta política e demais normas e os procedimentos de segurança da informação a ela associados deverão ser amplamente divulgados.