Universidade de Brasília

Boletim de Atos Oficiais da UnB em 01/11/2024

RESOLUÇÃO DA CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO Nº 02/2024

Atualiza a Resolução da Câmara de Planejamento e Administração nº 004/2018 - Política de Segurança da Informação e Comunicação - PoSIC da Universidade de Brasília - UnB.

A **CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO (CPLAD)** da UnB, no uso de suas atribuições estatutárias e regimentais, considerando o que dispõe Leis e Decretos Federais vigentes que tratam da Política Nacional de Segurança da Informação - PNSI e da Gestão de Segurança da Informação e Comunicação - GSIC nos órgãos e entidades da Administração Pública Federal – APF.

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação e Comunicação – PoSIC da UnB.

CAPÍTULO I

DO OBJETIVO E ABRANGÊNCIA

Art. 2º Esta PoSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicações - SIC no âmbito da UnB, com o propósito de diminuir a exposição ao risco a níveis que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam os objetivos estratégicos e as atividades precípuas de ensino, pesquisa e extensão desta Universidade.

Art. 3º Esta PoSIC e suas eventuais instruções normativas aplicam-se às unidades administrativas e acadêmicas, conforme estabelecido na Estrutura Regimental da UnB, abrangendo os servidores técnicos, corpo docente e discente, prestadores de serviço, colaboradores terceirizados, estagiários, jovens aprendizes, consultores externos e a quem, de alguma forma, tenha acesso aos ativos da instituição.

Art. 4º Os princípios e diretrizes gerais desta PoSIC também se aplicam às entidades vinculadas à UnB e a quaisquer relacionamentos com outros órgãos e entidades públicos ou privados.

CAPÍTULO II

DAS DEFINIÇÕES E CONCEITOS

Art. 5º Para os efeitos dessa Política considera-se:

I. ativos: tudo que tenha valor para a organização, material ou não. Para maior objetividade e delimitação de escopo nesta política, convém dividir os ativos de TI em grupos: ativos físicos, ativos de softwares, ativos de serviço, ativos de informação, ativos humanos e ativos intangíveis;

II gestão de riscos: o conjunto de processos e métodos para buscar um equilíbrio entre os riscos e os custos das operações, identificando, avaliando e controlando ameaças relacionadas à tecnologia da informação, por meio de técnicas avançadas em análise de vulnerabilidades, entendimento das prioridades, construção de plano de contingência, instituição de rotina de backups e treinamento dos colaboradores;

III. gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações da atividade institucional caso essas ameaças se concretizem, de forma a fornecer uma estrutura para que se desenvolva uma resiliência organizacional capaz de recuperar perdas de ativos a um nível aceitável pré-estabelecido, por intermédio de ações de prevenção, resposta e recuperação, de forma a salvaguardar os interesses das áreas envolvidas, a reputação, a marca da organização e suas atividades de valor agregado;

IV. gestão de conformidades: consiste no conjunto de princípios, estruturas, atividades e processos coordenados para dirigir e controlar os procedimentos que fazem parte da avaliação de conformidade, que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização;

V. gestão de incidentes: processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;

VI. gestão de segurança da informação e comunicações - GSIC: processo abrangente de gestão que desenvolve ações e métodos que visam a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, táticos e operacionais, não se limitando ao âmbito da tecnologia da informação e comunicação.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 6º O conjunto de documentos que complementa a PoSIC da UnB deverá guiar-se pelos seguintes princípios de SIC:

I. segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a atender aos objetivos institucionais e reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

II. menor privilégio: pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

III. auditabilidade: todos os eventos necessários à garantia da integridade, da confiabilidade e da autenticidade dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;