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;

IV. mínima dependência de segredos: os controles de SIC devem ser efetivos para mitigação de riscos e ameaças;

V. controles automáticos: deverão ser aplicados, sempre que possível, controles de segurança automáticos, especialmente aqueles controles que dependem da vigilância humana e do comportamento humano;

VI. resiliência: os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;

VII. defesa em camadas: controles devem ser desenhados em camadas ou níveis, de tal forma que, se uma camada de controle falhar, exista um tipo diferente de controle em outra camada

ou nível para prevenir a exploração das vulnerabilidades de segurança;

VIII. exceção aprovada: exceções à esta PoSIC devem sempre ser documentadas e ter apreciação do Comitê de Governança Digital - CGD da UnB, ou colegiado similar;

IX. substituição da segurança em situações de emergência: controles de segurança devem ser desconsiderados somente de formas predeterminadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 7º Esta PoSIC deverá ser mantida em pleno alinhamento ao Projeto Político Pedagógico Institucional - PPPI que declara princípios filosóficos e técnico metodológicos gerais que norteiam as práticas acadêmicas da UnB, bem como o seu Plano de Desenvolvimento Institucional - PDI.

Art. 8º A PoSIC visa assegurar a privacidade, no que couber, bem como a proteção de todos os dados, a confidencialidade, disponibilidade, autenticidade e integridade das informações e dos conhecimentos produzidos pela UnB em suas mais variadas atividades e atribuições institucionais.

Art. 9º O modelo de Gestão de SIC - GSIC da UnB deverá ser integrado e suportado pelos subsídios gerados pela Gestão de Riscos, Gestão de Ativos, Gestão de Incidentes, Gestão de Continuidade de Negócio e Gestão de Conformidade, em consonância com o especificado nas diretrizes desta PoSIC.

Art. 10. A GSIC deve suportar a tomada de decisões, bem como realizar a gestão de conhecimento e de recursos por meio do aproveitamento eficiente e eficaz dos ativos, possibilitando alcançar os objetivos estratégicos da UnB, assim como otimizar seus investimentos.

Art. 11. As ações de SIC devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade da UnB.

Art. 12. Os custos associados à GSIC deverão ser compatíveis com os custos dos ativos que se deseja proteger.

Art. 13. As instruções normativas, normas técnicas, procedimentos, manuais e metodologias de SIC da UnB devem considerar, subsidiariamente, normas e padrões da APF como referência nos processos de gestão e governança de SIC e devem estipular mecanismos que garantam a orientação à conformidade dos controles de SIC associados, inclusive sua auditabilidade.

Art. 14. A UnB deve possuir arcabouços normativos atualizados relativos à SIC, com vistas a gerir, manter, avaliar e atualizar critérios de proteção da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, conforme normas e legislação específica em vigor.

Art. 15. O acesso físico aos ambientes de Tecnologia da Informação e Comunicação - TIC da UnB deverão possuir controles, mecanismos de segurança e infraestrutura adequados aos níveis de segurança exigidos para cada local.

Art. 16. As instalações e infraestruturas críticas/sensíveis somadas aos processos e atividades que sustentam os serviços críticos de TIC disponibilizados pela UnB devem ser protegidos, considerando os riscos identificados, os níveis de segurança definidos e os controles de segurança implementados de forma a garantir a disponibilidade, integridade, autenticidade e

confidencialidade das informações e comunicações, bem como contra o acesso indevido, danos e interferências.

Art. 17. Quando da celebração de contratos, estes deverão conter, obrigatoriamente, cláusulas específicas sobre o sigilo, confidencialidade e uso das informações como condição imprescindível para que possa ser concedido o acesso às informações.

Art. 18. Deve ser estabelecida a integração e sinergia entre as instâncias e estruturas de supervisão e apoio definidas nesta PoSIC e aquelas definidas em outras políticas da UnB, por meio de modelos de relacionamento que considerem e compartilhem, quando possível, as competências, responsabilidades, informações e as próprias estruturas.

Art. 19. O uso da internet pela rede da UnB deve ser empregado para fins institucionais direta ou indiretamente relacionadas a atividades de gestão, ensino, pesquisa e extensão. Os usuários terão seus acessos autorizados conforme as políticas e normas de TIC da UnB.

Art. 20. O correio eletrônico da UnB é de uso institucional, e deve ser empregado por seus usuários para fins institucionais direta ou indiretamente relacionadas a atividades de gestão, ensino, pesquisa e extensão em obediência a esta PoSIC, aos princípios, diretrizes e legislações pertinentes que regem a APF, bem como a instruções normativas da UnB.

Art. 21. É de responsabilidade de todos que têm acesso aos ativos da UnB manter os níveis de segurança da informação adequados, segundo preceitos desta PoSIC e suas instruções normativas, os quais também estarão sujeitos a esta PoSIC e acatarão as suas implicações.

Art. 22. Os nomes de domínios de sítios e de correio eletrônico da UnB são endereços virtuais que patenteiam a imagem e prestígio da instituição diante da comunidade interna e externa, a identificando exclusivamente.

Parágrafo único. Neste contexto, todos os conteúdos institucionais direta ou indiretamente relacionados a atividades de gestão, ensino, pesquisa e extensão, devem utilizar endereço virtual institucional da UnB.

Art. 23. O tratamento de dados pessoais deve assegurar a titularidade e a sua proteção de forma a garantir os direitos fundamentais da intimidade, liberdade e privacidade, nos termos da legislação vigente e das políticas internas.

SEÇÃO I

DA GESTÃO DE RISCOS

Art. 24. A estrutura de SIC da UnB deverá estabelecer metodologia que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos.

Art. 25. As unidades administrativas e acadêmicas da UnB, com apoio da estrutura de SIC, deverão implementar e executar as atividades de gestão de riscos de SIC associados aos ativos sob sua responsabilidade.

Art. 26. Os riscos de SIC deverão ser considerados na contratação de serviços terceirizados, sendo os gestores das unidades administrativas e acadêmicas e dos ativos relacionados, gestores e fiscais de contrato, bem como os fornecedores e custodiantes os responsáveis por manter os níveis apropriados de segurança da informação na preparação, execução e entrega dos serviços.

SEÇÃO II

DA GESTÃO DE ATIVOS

Art. 27. A estrutura de SIC deve instituir normas e procedimentos que garantam a adequada gestão dos ativos da UnB em conjunto com as unidades responsáveis pelos respectivos ativos.

Art. 28. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos da UnB em níveis compatíveis ao seu grau de relevância para a consecução das atividades e objetivos estratégicos.

Art. 29. Os ativos da UnB devem ser associados a controles de segurança implementados independentemente do meio em que se encontram, devendo ser protegidos contra divulgação, modificações, remoção ou destruição não autorizadas.

Art. 30. Os usuários que possuem acesso aos ativos da UnB devem ser periodicamente conscientizados, capacitados e sensibilizados em assuntos de segurança de SIC, com particular atenção aos ativos de informação quanto à sua classificação da informação e de tratamento da informação.

Art. 31. Os processos e atividades que sustentam os serviços críticos disponibilizados pela UnB devem ser protegidos de forma a garantir a disponibilidade, integridade, autenticidade e confidencialidade das informações e comunicações.

SEÇÃO III

DA GESTÃO DA CONTINUIDADE DO NEGÓCIO

Art. 32. A estrutura de SIC da UnB, em conjunto com as unidades responsáveis pelos ativos, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de potenciais eventos que causem a indisponibilidade sobre os serviços de TIC da UnB.

SEÇÃO IV

DA GESTÃO DE INCIDENTES

Art. 33. A estrutura de SIC da UnB deverá criar e manter uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR da UnB, com a responsabilidade de coordenar as atividades relacionadas a incidentes de segurança em rede de computadores.

§ 1º Os eventos e incidentes de SIC devem seguir o Plano de Gerenciamento de Incidentes específico, no qual se definirá as responsabilidades e procedimentos para assegurar respostas tempestivas, efetivas e ordenadas perante incidentes de SIC de forma a contribuir para garantir a continuidade das atividades com vistas a não intervenção no alcance dos objetivos estratégicos da UnB;

§ 2º A ETIR da UnB deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede de computadores orientados pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov;

§ 3º A constituição e regulamentação da ETIR da UnB será efetivada por meio de documento formal aprovado pela Secretaria de Tecnologia da Informação - STI.

SEÇÃO V

DA GESTÃO DE CONFORMIDADE

Art. 34. O cumprimento desta PoSIC deverá ser avaliado periodicamente, por meio de verificações de conformidade realizadas com o apoio da estrutura de SIC.

Art. 35. Os controles de SIC devem ser analisados criticamente e verificados em períodos regulares pela estrutura de SIC da UnB, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes.

Art. 36. A estrutura de SIC da UnB deve instituir processos de análise e tratamento de conformidade, visando garantir o atendimento das leis, regulamentos e normas que regem as atividades no âmbito da APF.

CAPÍTULO V

DA ESTRUTURA DE SIC E SUAS RESPONSABILIDADES

Art. 37. A SIC é disciplina fundamental da boa governança corporativa, sendo de responsabilidade da Alta Administração da UnB.

Art. 38. A estrutura de SIC da UnB será responsável pelas atividades de definição e implementação de diretrizes, políticas, instruções, normas e procedimentos relativos à SIC, com atribuições definidas nesta PoSIC.

Art. 39. A estrutura de SIC deverá institucionalizar um modelo de GSIC capaz de apoiar os diversos níveis de gestão da UnB e suas unidades acadêmicas e administrativas no objetivo de integrar os controles e processos de SIC aos processos organizacionais existentes.

Parágrafo único. A participação na referida estrutura e eventuais grupos de trabalho associados não enseja remuneração de qualquer espécie ou quaisquer criações de cargos além daqueles já existentes na estrutura regimental da UnB, sendo considerada serviço público relevante.

Art. 40. É de responsabilidade dos 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 UnB, zelar pelo cumprimento das diretrizes desta política no âmbito de suas áreas de atuação.

Art. 41. A estrutura de SIC da UnB é constituída por:

I. Alta Administração;

II. CGD da UnB, ou colegiado com competência semelhante;

III. STI da UnB;

IV. ETIR da UnB.

Art. 42. No âmbito da PoSIC da UnB, compete à Alta Administração:

I. Prover as diretrizes e o apoio necessários às ações de SIC e definição da estrutura adequada para GSIC.

Art. 43. No âmbito da PoSIC, compete ao CGD da UnB, instância deliberativa constituída como último nível para discussão de questões relativas à SIC, em consonância com suas demais atribuições:

I. estabelecer os princípios estratégicos e as diretrizes de SIC, e assegurar os recursos financeiros, materiais e humanos necessários ao seu cumprimento, alinhados à missão institucional da UnB e ao arcabouço legal ao qual todos os órgãos da APF estão subordinados;

II. coordenar as revisões/atualizações da PoSIC da UnB, direcionando estratégias para promover a cultura de SIC com o apoio das demais unidades administrativas/acadêmicas e órgãos pertinentes, as ações permanentes de divulgação, treinamento, educação e conscientização dos

usuários em relação aos conceitos e às recomendadas boas práticas de SIC, em toda a sua abrangência;

III. coordenar elaboração dos planejamentos estratégico e tático de SIC e submetê-los à aprovação colegiada, mas sobretudo, monitorar e avaliar a execução dos mesmos, bem como propor ajustes cabíveis;

IV. revisar e analisar criticamente a PoSIC e conformidade de suas instruções normativas, resoluções e metodologias visando a sua aderência às necessidades e objetivos institucionais e por fim deliberar sobre aprovação;

V. providenciar a divulgação da PoSIC da UnB e de seus complementos no formato de instruções normativas.

Art. 44. A STI é o órgão executivo de TIC da UnB, e nesta esfera compete a este:

I. estabelecer e disseminar normas técnicas e manuais de procedimentos em conformidade às diretrizes desta instrução, além de implementar todo o escopo de diretrizes da PoSIC, com intuito de consolidar a cultura de SIC na UnB por meio de ações permanentes de conscientização;

II. explorar tecnologias para identificação de viabilidade no ambiente computacional da UnB e promover as ações de SIC e participações em eventos do tema;

III. apoiar os atores com responsabilidades nos processos das unidades administrativas e acadêmicas da UnB, para que estes possam implementar os controles de segurança sobre o modelo GSIC da UnB;

IV. sustentar e acompanhar trabalhos de auditoria, investigações e as avaliações de danos decorrentes de quebra de segurança e/ou violações da PoSIC da UnB para submissão ao CGD e às instâncias superiores, e emissão ao Gabinete de Segurança Institucional da Presidência da República, quando for o caso;

V. administrar, executar, monitorar e consolidar atividades do modelo de GSIC, auxiliando no âmbito administrativo/técnico o CGD da UnB quando necessário, inclusive nas revisões/atualizações da PoSIC;

VI. contribuir para elaboração do planejamento estratégico e tático de SIC da UnB;

VII. implementar e monitorar a Gestão de Ativos observando os níveis adequados e requisitos de SIC.

Art. 45. Compete à ETIR da UnB:

I. coordenar as atividades de tratamento de incidentes de SIC;

II. promover a recuperação de sistemas de informações;

III. agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC, avaliando as condições de segurança de redes por meio de verificações de conformidade e identificação de vulnerabilidades e artefatos maliciosos;

IV. realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

V. analisar ataques e invasões na rede de dados e comunicações da UnB;

VI. executar as ações necessárias para tratar violações de segurança;

VII. obter informações quantitativas acerca dos incidentes ocorridos, que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes para alimentação de uma base de conhecimento;

VIII. manter contato com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR, a CTIR Gov, concernente a assuntos de SIC;

IX. Cooperar com outras Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos; e

X. Participar de eventos relativos à SIC.

CAPÍTULO VI

DAS PENALIDADES

Art. 46. O descumprimento ou violação, pelo usuário, das regras previstas na PoSIC da UnB poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 47. A PoSIC e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura da UnB ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente, conforme legislação vigente, sendo atualizados quando necessário.

Art. 48. A PoSIC da UnB, as instruções normativas e os procedimentos de SIC a ela associados deverão ser amplamente divulgados.

Art. 49. Esta PoSIC entra em vigor na data de sua aprovação por meio de Resolução da CPLAD, em sua 16ª reunião, realizada em 17 de Outubro de 2024.

Professora Denise Imbroisi

Decana de Planejamento, Orçamento e Avaliação Institucional

Documento assinado eletronicamente por **Denise Imbroisi**, **Decana de Planejamento, Orçamento e Avaliação Institucional**, em 01/11/2024, às 15:08, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **11969838** e o código CRC **F6A17E43**.

Referência: Processo nº 23106.095996/2024-26 SEI nº 11969838