(Anexo 1):

RESOLUÇÃO DA CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO Nº 003/2018

Institui a Política de Governança de Tecnologia da Informação e Comunicação da Universidade de Brasília - PGTIC/UnB.

A CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO (CPLAD) DA UNIVERSIDADE DE BRASÍLIA na constância do seu mandato, no uso de suas atribuições estatutárias e regimentais, considerando o disposto no art. 4º da Portaria nº 19, de 29 de maio de 2017, da Secretaria de Tecnologia da Informação e Comunicação, no Acórdão nº 882/2017 - TCU-Plenário e no Guia de Governança de TIC do SISP v.02 - GovTIC, resolve:

Art. 1º Instituir a Política de Governança de Tecnologia da Informação e Comunicação da Universidade de Brasília - PGTIC/UnB.

CAPÍTULO I

DA POLÍTICA DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE DE BRASÍLIA - UnB

SEÇÃO I
DO OBJETIVO E ABRANGÊNCIA

Art. 2º Esta Política de Governança de Tecnologia da Informação e Comunicação (PGTIC/UnB) se aplica a todas as unidades da estrutura regimental da UnB.

SEÇÃO II
DOS CONCEITOS

Art. 3º Para efeitos desta Política ficam estabelecidos os seguintes conceitos:

I. Tecnologia da Informação e Comunicação - TIC: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

II. Governança de TIC: sistema pelo qual o uso atual e futuro da TIC é dirigido e controlado. Significa avaliar e direcionar o uso da TIC para dar suporte à organização. Consiste em políticas, papéis, fluxos e regras que visam alinhar a TIC com os objetivos estratégicos de gestão, ensino, pesquisa e extensão da organização;

III. Alta Administração: são agentes públicos responsáveis pela governança de TIC na UnB, a saber:
   a) Reitor, Vice-reitor e Decanos.

IV. Partes Interessadas: qualquer indivíduo, grupo ou organização que possa afetar, ser afetado, ou ter a percepção de que será afetado por uma decisão ou atividade. Neste contexto e, tendo como base o cenário da Administração Pública Federal - APF, são considerados como partes interessadas no uso de TIC:
   1. Sociedade;
   2. Governo Federal;
   3. Alta Administração;
   4. Comunidade Acadêmica;

5. Representantes das áreas administrativas e acadêmicas;
6. Gestores de TIC; e
7. Usuários de serviços de TIC.

V. Gestão de TIC: é responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TIC em consonância com a direção definida pela função de governança, a fim de atingir os objetivos corporativos;

VI. Governança Digital: é a utilização, pelo setor público, de recursos de TIC, com o objetivo de melhorar a disponibilização de informação e a prestação de serviços públicos, incentivar a participação da sociedade no processo de tomada de decisão e aprimorar os níveis de responsabilidade, transparência e efetividade do governo;

VII. Solução de TIC: conjunto de bens e/ou serviços de TIC e automação que se integram para o alcance dos resultados pretendidos; e

VIII. Serviços de TIC: conjunto de atividades de prestação de serviços, relacionadas aos sistemas estruturantes e finalísticos dos órgãos e entidades, que integram uma Solução de TIC.

SEÇÃO III
DOS OBJETIVOS

Art. 4º A Política de Governança de Tecnologia da Informação e Comunicação da UnB tem como objetivos:

I. promover o uso eficaz, eficiente e aceitável da TIC no âmbito dos órgãos de gestão, ensino, pesquisa e extensão da Universidade de Brasília/UnB;

II. promover alinhamento entre as boas práticas de governança e gestão de TIC às estratégias, planos e processos de TIC da Universidade de Brasília/UnB;

III. fomentar a integração e a otimização dos recursos de TIC entre órgãos da Universidade de Brasília/UnB;

IV. definir formalmente, no âmbito da Universidade de Brasília/UnB:

a) os princípios e as diretrizes para a governança de TIC;

b) os papéis e responsabilidades dos envolvidos nas tomadas de decisões sobre TIC;

c) as estruturas envolvidas na governança de TIC; e

d) os mecanismos de transparência e prestação de contas dos investimentos de recursos públicos aplicados em iniciativas de TIC.

SEÇÃO IV
DOS PRINCÍPIOS

Art. 5º A governança e gestão de TIC, bem como o uso dos seus recursos, no âmbito dos órgãos de gestão, ensino, pesquisa e extensão da UnB, orientam-se pelos seguintes princípios:

I. alinhamento dos planos, projetos, serviços e atividades de TIC aos objetivos de gestão, ensino, pesquisa e extensão e às necessidades das partes interessadas;

II. busca pelo papel estratégico da TIC com intuito de contribuir, de maneira eficaz, com a sustentação dos serviços públicos providos pela organização;

III. monitoramento e avaliação contínua do desempenho das ações de TIC, bem como do alcance das metas definidas nos planos de TIC, a fim de otimizar o uso de recursos e realizar benefícios para a UnB;

IV. transparência na aplicação dos recursos públicos, no desempenho e nos resultados das iniciativas de TIC;

V. definição dos papéis e responsabilidades acerca das tomadas de decisão que envolvam os diversos aspectos de TIC, de forma a assegurar a adequada prestação de contas das ações de TIC, bem como a responsabilização pelos atos praticados; e

VI. políticas e práticas claramente definidas, implementadas e fiscalizadas de maneira a garantir a conformidade das ações de TIC à legislação, aos regulamentos e normativos obrigatórios.

Art. 6º A governança de TIC deverá ser implantada, também em consonância com os princípios específicos de TIC da UnB, e no que couber, segundo o Guia de Governança de TIC do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

SEÇÃO V
DAS DIRETRIZES

SUBSEÇÃO I
DAS DIRETRIZES GERAIS

Art. 7º As práticas de governança e gestão de TIC observam as seguintes diretrizes:

I. ações de TIC dirigidas e controladas, mediante a utilização de instrumentos de avaliação, direção e monitoramento, conforme recomendações propostas pelos modelos de governança e gestão de TIC atuais, com o objetivo de identificar oportunidades e iniciativas que otimizem o uso da TIC, de forma a agregar valor às Unidades da UnB;

II. gestão de TIC baseada nas melhores práticas, integrada e alinhada às estratégias e necessidades das áreas de gestão, ensino, pesquisa e extensão;

III. elaboração de planos de TIC que contemplem objetivos de médio e de longo prazo, bem como prioridades e iniciativas de curto prazo, de forma alinhada aos planos estratégicos institucionais;

IV. elaboração de indicadores e fixação de metas para avaliação do alcance dos objetivos estabelecidos, em função dos benefícios esperados para as atividades fim da UnB;

V. ampla participação das unidades organizacionais na elaboração dos planos de TIC;

VI. transparência na execução dos planos de TIC;

VII. gestão de pessoas por competência, permitindo uma melhor alocação de recursos, com incentivo ao desenvolvimento técnico e gerencial continuado, de acordo com as necessidades evidenciadas por planos e prioridades institucionais;

VIII. recursos orçamentários destinados à TIC com alocação prioritária no provimento e manutenção de soluções que atendam às demandas estratégicas da UnB, refletidas em seus instrumentos de planejamento;

IX. avaliação periódica da conformidade das ações, processos e estruturas de TIC, em relação à legislação em vigor, normas internas e melhores práticas recomendadas;

X. gestão de riscos de TIC baseada na identificação, avaliação e redução dos riscos relacionados à TIC, de acordo com os níveis de tolerância previamente definidos;

XI. elaboração e manutenção de plano de continuidade, com vistas a permitir que os serviços de TIC, que sustentam processos críticos de gestão, ensino, pesquisa e extensão, mantenham-se disponíveis a um nível aceitável pela organização.

SUBSEÇÃO II
DAS DIRETRIZES DE PROVIMENTO DE SOLUÇÕES DE TIC

Art. 8º O provimento de soluções de TIC observam as seguintes diretrizes:

I. contratações de TIC sempre precedidas de planejamento, em conformidade à legislação e normativos vigentes, alinhadas aos planos e estratégias institucionais, e aos princípios de eficácia, eficiência, efetividade e economicidade;

II. gestão de fornecedores utilizando mecanismos de seleção, gerenciamento do relacionamento, gerenciamento de contratos e monitoramento do desempenho dos fornecedores de bens e/ou serviços de TIC;

III. prospecções de soluções de TIC com foco na otimização dos processos de trabalho e na integração de soluções;

IV. adoção de arquitetura e padrões tecnológicos que satisfaçam as diretrizes aprovadas pelo Comitê de Tecnologia da Informação da UnB - CTI/UnB, e que se baseiem preferencialmente em padrões de mercado e em diretrizes de interoperabilidade do Governo Federal;

V. definição, mensuração e revisão periódica de acordos de níveis de serviço;

VI. planejamento e gestão com foco no cumprimento dos níveis de serviço acordados para as soluções de TIC; e

VII. adoção da modalidade de provimento que se revelar, justificadamente, mais adequada à realização das estratégias e ao alcance dos objetivos institucionais.

Art. 9º O provimento de soluções de TIC compreende as seguintes modalidades:

I. desenvolvimento: construção de soluções, com recursos próprios ou de terceiros, para atender a necessidades específicas dos órgãos da UnB;

II. aquisição: adoção de soluções construídas externamente à UnB, por meio de contratação, recebimento de outros órgãos e entidades, utilização de equipamentos/infraestrutura para compor/complementar ou estender soluções existentes;

III. manutenção: alteração de solução existente para correção de erros, melhoria de qualidade, incorporação de novas funcionalidades, mudança nas regras de negócio ou adaptação a novas tecnologias.

§ 1º A aquisição, dependendo da solução, pode envolver a instalação, configuração, disponibilização, ajustes, treinamento, testes de validação, homologação, repasse tecnológico, bem como qualquer insumo ou atividade necessária para a disponibilização da solução de TIC.

§ 2º A UnB poderá fazer uso de outras formas de desenvolvimento ou obtenção de soluções de TIC baseadas em softwares/sistemas - proprietários ou livres/abertos - de informação que não estejam contempladas nas modalidades retro mencionadas, como por exemplo: acordos de cooperação técnica, parcerias internas e externas, transferências de conhecimento e tecnologia, entre outras.

Art. 10. A abordagem de provimento de soluções de TIC classifica-se, segundo a responsabilidade das unidades envolvidas, em:

I. centralizada: quando o desenvolvimento, a aquisição ou a manutenção da solução é realizada pelo Centro de Informática - CPD; ou

II. descentralizada: quando o desenvolvimento, a aquisição ou a manutenção da solução é realizada por outra unidade provedora, sob orientação técnica do CPD, e seguindo a arquitetura e os padrões tecnológicos estabelecidos nos normativos vigentes da UnB.

SUBSEÇÃO III
DAS DIRETRIZES PARA OS PLANOS DE TIC

Art. 11. Os seguintes planos norteiam as ações, aquisições, programas, projetos e serviços de TIC no âmbito das Unidades Acadêmicas e Administrativas da Universidade de Brasília/UnB:

I. Planejamento estratégico institucional - PDI/UnB), no que couber, com as leis orçamentárias PPA, LDO e LOA; e

II. Plano Diretor de Tecnologia da Informação e Comunicação da Universidade de Brasília/UnB - PDTIC/UnB em harmonia com o PDI/UnB;

Parágrafo único. Os planos constantes nos incisos I e II devem estar alinhados às recomendações gerais de TIC da APF, incluindo governança digital, comunicações de dados, segurança da informação, infraestrutura compartilhada e outras referências, além das melhores práticas de governança de TIC.

SUBSEÇÃO IV
DAS DIRETRIZES PARA A GESTÃO DE RISCOS DE TIC

Art. 12. As atividades de gestão de riscos de TIC devem obedecer às seguintes diretrizes específicas:

I. fomentar a cultura de gestão de riscos como fator essencial para implantar as estratégias e planos de TIC, tomar decisões e realizar os objetivos relacionados à TIC;

II. considerar se os riscos de TIC têm impacto sobre outras organizações públicas e demais partes interessadas, com consulta e compartilhamento de informações entre os atores envolvidos;

III. os riscos de TIC devem ser identificados, analisados, avaliados, tratados e monitorados de forma contínua, mediante processos formalizados; e

IV. a alta administração deverá estabelecer diretrizes de gestão de riscos relacionados à TIC, considerando os aspectos legais, financeiros, sociais, operacionais, tecnológicos, negociais e de imagem da UnB.

CAPÍTULO II
DOS PAPÉIS E RESPONSABILIDADES

SEÇÃO VI
DAS ESTRUTURAS ORGANIZACIONAIS

Art. 13. A governança e a gestão de TIC, bem como a coordenação, implantação e gestão da PGTIC serão de responsabilidade das seguintes estruturas organizacionais da UnB:

I. Alta Administração;

II. Comitê de Tecnologia da Informação - CTI/UnB; e

III. Centro de Informática - CPD.

SEÇÃO VII
DAS RESPONSABILIDADES

Art. 14. A Alta Administração é responsável pela governança de TIC (avaliação, direção e monitoramento da Gestão de TIC) no âmbito da UnB;

Art. 15. Compete ao Comitê de Tecnologia da Informação - CTI/UnB a responsabilidade pelo estabelecimento e alcance dos objetivos e das metas de TIC, e pela orientação das iniciativas e dos investimentos em TIC, bem como:

I. recomendar a aprovação do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC/UnB;

II. recomendar a aprovação do Plano de Contratações de Soluções de Tecnologia da Informação e Comunicações - PCTIC/UnB;

III. propor políticas e normas que assegurem o alinhamento das ações de tecnologia da informação e comunicação, no âmbito da UnB;

IV. definir diretrizes e estratégias para o planejamento da oferta de serviços e informações produzidos pela UnB por meio digital;

V. definir mecanismos de racionalização de gastos e de aplicação de recursos em tecnologia da informação e comunicação;

VI. recomendar a aprovação das políticas e normas de segurança da informação e Comunicação;

VII. realizar monitoramento e a avaliação da gestão de TIC, observando o desempenho das operações de TIC e da implementação das estratégias e planos e o cumprimento das políticas de TIC da UnB;

VIII. propor as prioridades dos programas de investimento em TIC visando alinhar as ações das Unidades aos objetivos e atribuições da UnB;

IX. estabelecer ações visando a integração de sistemas e informações, democratizando o acesso às pessoas que deles necessitam;

X. coordenar e articular as ações visando a prospecção e adoção de novas tecnologias de TIC;

XI. analisar e recomendar aprovação, em consonância com o PDTIC, a priorização dos projetos e demandas de Tecnologia da Informação e Comunicação; e

XII. monitorar e avaliar a implementação das políticas de TIC no âmbito da UnB.

Art. 16. Compete ao Centro de Informática - CPD gerir a TIC na Universidade de Brasília em consonância com as diretrizes definidas pela Alta Administração, bem como:

I. promover e incentivar a TIC na UnB visando obter eficiência institucional em todos os níveis e alcance da eficácia no suporte às atividades de ensino, pesquisa, extensão e administração da Instituição;

II. submeter ao CTI/UnB propostas do PDTIC e do PCTIC;

III. planejar e executar as aquisições de soluções de TIC;

IV. prover apoio administrativo, técnico e logístico necessário ao funcionamento do CTI/UnB, propondo políticas e diretrizes relacionadas à tecnologia da informação e comunicação, incluídas a segurança de informações eletrônicas e de recursos de comunicações, segurança cibernética, segurança em infraestruturas críticas de TIC; e

V. articular com órgãos do Poder Executivo Federal e dos outros Poderes assuntos relacionados ao uso da tecnologia da informação e de comunicação.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 17. Outras políticas e normas complementares relativas à gestão, segurança da informação e cibernética, bem como do uso de recursos de TIC, emanadas no âmbito das Unidades da UnB, devem estar harmonizadas com as disposições desta Política.

Art. 18. Esta Resolução entra em vigor na data de sua publicação.

(Anexo 2):

RESOLUÇÃO DA CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO Nº 004/2018

Institui a Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB.

A CÂMARA DE PLANEJAMENTO E ADMINISTRAÇÃO (CPLAD) DA UNIVERSIDADE DE BRASÍLIA, no uso de suas atribuições estatutárias e regimentais, tendo em vista o que dispõe o Decreto Nº 3.505 de 13 de junho de 2000, o disposto no art. 5º, inciso VII Instrução Normativa 01/DSIC/GSI/PR de 13 de junho de 2008, de 10 de junho de 2009 e Instrução Normativa Conjunta MP/CGU Nº 01, de 10 de maio de 2016, Norma Complementar 14/IN01/DSIC/GSIPR de 19 de março de 2018, resolve:

Art. 1º Instituir a Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB.

CAPÍTULO I
DO OBJETIVO E ABRANGÊNCIA

Art. 2º A PoSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicações - SIC no âmbito da Universidade de Brasília- UnB, com o propósito de limitar 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 Para os efeitos dessa Política considera-se:

I. ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os processos decorrentes das atividades de gestão, ensino, pesquisa e extensão, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

II. gestão de ativos de informação: processo abrangente de gestão que inventaria e mapeia os ativos de informação institucionais, identificando, no mínimo e de forma inequívoca, seu conjunto completo de informações básicas (nome, descrição e localização), seus respectivos responsáveis (proprietários e custodiantes), seus requisitos legais e de negócio, sua classificação, sua documentação, seu ciclo de vida, seus riscos associados e seus controles de SIC implementados, bem como os outros ativos de informação relacionados;

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 de informação 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 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; e

V. plano diretor de SIC: documento que estipula, para um período mínimo de 1 (um) ano, objetivos específicos, bem como seus indicadores e metas, com a finalidade de orientar e fazer cumprir a atuação das áreas acerca das ações necessárias de GSIC.

Art. 4º Esta PoSIC e suas eventuais normas complementares aplicam-se às Unidades Administrativas e Acadêmicas da UnB, conforme estabelecido na Estrutura Regimental da Universidade de Brasília, abrangendo os servidores, corpo docente e discente, prestadores de serviço, colaboradores, estagiários, jovens aprendizes, consultores externos e a quem, de alguma forma, tenha acesso aos ativos de informação da instituição.

Art. 5º 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 DOS PRINCÍPIOS

Art. 6º O conjunto de documentos que compõem esta PoSIC deverá guiar-se pelos seguintes princípios de segurança da informação e comunicações:

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 PoSIC devem sempre ser documentadas e ter aprovação superior; e

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 III
DAS DIRETRIZES GERAIS

Art. 7º A Política de Segurança da Informação deverá ser mantida em pleno alinhamento ao Projeto Político Pedagógico - PPPI que declara princípios filosóficos e técnico metodológicos gerais que norteiam as práticas acadêmicas da Universidade de Brasília, bem como ao Plano de Desenvolvimento Institucional da UnB – PDI.

Art. 8º A Política Segurança da Informação da UnB 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 normas, procedimentos, manuais e metodologias de SIC da UnB devem considerar, subsidiariamente, normas e padrões da APF (Administração Pública Federal) 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 TIC da UnB deverão possuir controles e mecanismos de segurança adequados aos níveis de segurança exigidos para cada local.

Art. 16. As instalações/infraestruturas – críticas ou sensíveis –, os processos e atividades que sustentam os serviços críticos de tecnologia da informação e comunicação (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 administração pública federal, bem como aos normativos internos 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 Normas Complementares, os quais também estarão sujeitos a esta PoSIC e acatarão as suas implicações.

SEÇÃO I
DA GESTÃO DE RISCOS

Art. 22. 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. 23. As Unidades Administrativas e Acadêmicas da UnB, com apoio da Estrutura de SIC, deverão implementar e executar as atividades de gestão de riscos de segurança da informação e comunicações associados aos ativos de informação sob sua responsabilidade.

Art. 24. 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 entrega dos serviços.

SEÇÃO II
DA GESTÃO DE ATIVOS

Art. 25. A Estrutura de SIC deve instituir normas e procedimentos que garantam a adequada gestão dos ativos de informação da UnB em conjunto com as unidades responsáveis pelos respectivos ativos.

Art. 26. Ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos de informação da UnB em níveis compatíveis ao seu grau de relevância para a consecução das atividades e objetivos estratégicos.

Art. 27. Os ativos de informação 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. 28. As pessoas que possuem acesso aos ativos de informação da instituição devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos de segurança e de tratamento da informação.

Art. 29. 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. 30. A Estrutura de SIC da UnB, em conjunto com as áreas responsáveis pelos ativos de informação da Universidade, 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. 31. A Estrutura de SIC da UnB deverá criar e manter uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), instituída pelo Comitê de Tecnologia da Informação - CTI, 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 deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV.

§ 3º A constituição e regulamentação da ETIR será efetivada por meio de documento formal aprovado por instância competente da UnB.

SEÇÃO V
DA CONFORMIDADE

Art. 32. O cumprimento desta PoSIC deverá ser avaliado periodicamente, por meio de verificações de conformidade realizadas com o apoio das Estruturas de SIC da UnB e do Comitê de Tecnologia da Informação - CTI da UnB.

Art. 33. 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. 34. 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 Administração Pública Federal.

CAPÍTULO IV
DA ESTRUTURA DE SIC E SUAS RESPONSABILIDADES

Art. 35. A SIC é disciplina fundamental da boa governança corporativa, sendo de responsabilidade da Alta Administração.

Art. 36. A Estrutura de SIC da UnB será responsável em assessorar a Alta Administração e o CTI nas atividades de definição e implementação de diretrizes, políticas, normas e procedimentos relativos à SIC, com atribuições definidas nesta PoSIC.

Art. 37. A Estrutura de SIC deverá institucionalizar um modelo de gestão de SIC - GSIC para a UnB capaz de apoiar os diversos níveis hierárquicos 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. 38. A Estrutura de SIC da UnB é constituída por:

I. Alta Administração;
II. Comitê de Tecnologia da Informação - CTI;
III. Centro de Informática - CPD; e
IV. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR.

Art. 39. No âmbito da PoSIC, compete à Alta Administração:

I. Prover as diretrizes e o apoio necessários às ações de SIC e definição da estrutura adequada para a Governança, Gestão de Riscos de TIC, Gestão de Continuidade de Negócios e Gestão da Segurança da Informação e Comunicação.

Art. 40. Compete ao CTI, instância colegiada consultiva 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 aos objetivos institucionais da UnB e ao arcabouço legal-normativo ao qual a UnB está subordinado;
II. direcionar estratégias para promover a cultura de segurança da informação e comunicações, coordenando, com o apoio das demais unidades e órgãos pertinentes, as ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de SIC, em toda a sua abrangência;
III. coordenar a elaboração da Política de Segurança da Informação e Comunicação, do Plano Diretor de SIC e do Programa Orçamentário de SIC, e submetê-los à aprovação;
IV. monitorar e avaliar a execução do Plano Diretor de SIC e do Programa Orçamentário de SIC vigentes, bem como propor e promover os ajustes cabíveis;
V. discutir e recomendar a aprovação de metodologias e normas complementares alinhadas às diretrizes desta PoSIC;
VI. avaliar, revisar e analisar criticamente a PoSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais da UnB;
VII. deliberar sobre proposta de alteração desta PoSIC, após parecer técnico de grupo de trabalho específico, submetendo-a à aprovação; e
VIII. providenciar a divulgação da PoSIC.

Art. 41. O Centro de Informática da UnB é o órgão executivo de TIC responsável por:

I. promover e disseminar, no âmbito da UnB, a cultura de SIC; II
II. coordenar as ações de SIC no âmbito da UnB;
III. apoiar os atores com responsabilidades nos processos das Unidades da UnB, para que eles possam implementar os controles de segurança em gestão de riscos, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes;
IV. discutir e aprovar normas operacionais e complementares, e manuais de procedimentos alinhados às diretrizes desta PoSIC;
V. propor recursos necessários às ações de SIC;
VI. consolidar e encaminhar os resultados dos trabalhos de auditoria de SIC às instâncias superiores, para posterior remissão ao Gabinete de Segurança Institucional da Presidência da República, quando for o caso;
VII. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e/ou violações da PoSIC e submeter às instâncias superiores;
VIII. realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos e benefícios na segurança da informação e comunicações;
IX. participar e estimular a participação em eventos relativos à SIC;
X. Assessorar administrativamente e tecnicamente o CTI em atividades relacionadas aos seguintes temas relativos à SIC:
   a) gestão de riscos de SIC;
   b) gestão de continuidade do negócio;

c) tratamento e resposta a incidentes de SIC;
d) conformidade em SIC.

XI. elaborar relatório de monitoramento da gestão de risco, gestão de ativos, gestão de continuidade de negócios e gestão de incidentes na UnB;

XII. subsidiar o CTI com informações e evidências em apurações quando da suspeita de ocorrências de quebras de segurança e/ou violações de SIC;

XIII. contribuir para elaboração do Plano Diretor de SIC, do Programa Orçamentário de SIC e da PoSIC com suas revisões;

XIV. implementar as diretrizes da PoSIC e as decorrentes normas complementares, normas operacionais e manuais de procedimentos no âmbito da UnB;

XV. elaborar e executar, no âmbito da UnB, processos que garantam a Gestão de Continuidade de Negócio, conforme legislação pertinente;

XVI. contribuir para consecução das ações permanentes de divulgação, treinamento, educação e conscientização dos usuários em relação aos conceitos e às práticas de SIC definidas pelo CTI com vistas à promoção da cultura de segurança da informação e comunicações, com o apoio das demais unidades e órgãos pertinentes, em toda a sua abrangência; e

XVII. implementar e monitorar os níveis adequados de segurança dos ativos de informação conforme os requisitos de SIC.

Art. 42. Compete à ETIR da UnB:

I. coordenar as atividades de tratamento de incidentes de segurança da informação e comunicação;

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 (CTIR Gov: Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal), concernente a assuntos de segurança da informação e comunicações;

IX. Cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

X. Participar de eventos relativos à SIC.

CAPÍTULO V DAS PENALIDADES

Art. 43. O descumprimento ou violação, pelo usuário, das regras previstas na Política de Segurança da Informação e Comunicações (PoSIC) poderá resultar na aplicação das sanções previstas em regulamentações internas e legislação em vigor.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS

Art. 44. 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. 45. A PoSIC, as normas e os procedimentos de SIC a ela associados deverão ser amplamente divulgados.

Art. 46. Esta Política entra em vigor na data de sua publicação.