



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

RESOLUÇÃO CONSU Nº 15/2026

Institui, ad referendum da plenária do Conselho Universitário, a Política Institucional de Segurança da Informação e Proteção de Dados da Universidade Estadual do Sudoeste da Bahia – UESB, estabelece diretrizes para a implementação e operacionalização do Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG no âmbito da Universidade e dá outras providências.

O Presidente do Conselho Universitário – Consu, da Universidade Estadual do Sudoeste da Bahia – Uesb, no uso de suas atribuições legais, estatutárias e regimentais e considerando:

- a) a autonomia universitária assegurada pelo art. 207 da Constituição Federal;
- b) a necessidade de assegurar a proteção das informações produzidas, recebidas, armazenadas, processadas, transmitidas ou custodiadas pela Universidade;
- c) a Lei Federal nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação;
- d) a Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;
- e) o Decreto Estadual nº 13.473, de 28 de novembro de 2011, que homologa a Resolução CIGOV nº 02/2011 e institui a Política de Segurança da Informação no âmbito dos órgãos e entidades da Administração Pública do Poder Executivo do Estado da Bahia, observada, no que couber, pela UESB;

Universidade Estadual do Sudoeste da Bahia – Uesb

Recredenciada pelo Decreto Estadual

Nº 16.825, de 04.07.2016

- f) o Decreto Estadual nº 24.105, de 2025, que dispõe sobre a aplicação da LGPD e institui a Política Estadual de Proteção de Dados Pessoais – PEPD no âmbito dos órgãos e entidades do Poder Executivo do Estado da Bahia;
- g) a Lei Estadual nº 12.618, de 28 de dezembro de 2012, e o Decreto Estadual nº 24.375, de 2 de março de 2026, que regulamentam o acesso a informações no âmbito do Estado da Bahia;
- h) a necessidade de adoção de mecanismos institucionais destinados a assegurar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e proteção dos dados e informações institucionais;
- i) que os dados acadêmicos, administrativos, financeiros, científicos, tecnológicos, de inovação e de pesquisa constituem ativos estratégicos da Universidade;
- j) a necessidade de fortalecimento da governança de dados e da interoperabilidade dos sistemas institucionais;
- k) a Portaria CAPES nº 158, de 17 de agosto de 2023, que instituiu o Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG;
- l) a Instrução Normativa GAB/Capes nº 1, de 23 de abril de 2026, que dispõe sobre a operacionalização da interoperabilidade e do compartilhamento de dados no âmbito do GoPG;
- m) o avançado estágio do ciclo de avaliação da pós-graduação e a necessidade de adoção tempestiva das providências institucionais necessárias à adequada organização, qualificação, integração e disponibilização das informações relativas aos Programas de Pós-Graduação da Universidade;
- n) que a UESB ainda não concluiu o processo de adesão ao GoPG, tornando necessária a adoção célere das medidas institucionais, administrativas e tecnológicas indispensáveis à sua efetiva participação no Programa;
- o) a importância estratégica da implantação do GoPG para os Programas de Pós-Graduação – PPGs da UESB, especialmente no que se refere à qualificação e consistência das informações acadêmicas, à integração das fontes institucionais de dados, à interoperabilidade com os sistemas da



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

CAPES e ao aprimoramento dos processos relacionados à avaliação da pós-graduação;

- p) que a implantação do GoPG contribuirá para o fortalecimento da governança das informações da pós-graduação, ampliando sua confiabilidade, integridade, rastreabilidade e interoperabilidade;
- q) por fim, a necessidade de estabelecer, em caráter imediato, as condições institucionais necessárias à formalização da adesão da UESB ao GoPG e ao início de sua implementação, sem prejuízo da posterior apreciação da matéria pela plenária do Conselho Universitário – CONSU;

RESOLVE:

Art. 1º Aprovar, ad referendum da plenária do Conselho Universitário – CONSU, a Política Institucional de Segurança da Informação e Proteção de Dados da Universidade Estadual do Sudoeste da Bahia – UESB, na forma do Anexo I desta Resolução.

Art. 2º Aprovar, ad referendum da plenária do Conselho Universitário – CONSU, as diretrizes para implementação e operacionalização, no âmbito da UESB, do Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG, na forma do Anexo II desta Resolução.

Art. 3º Integram esta Resolução:

I – Anexo I – Política Institucional de Segurança da Informação e Proteção de Dados da UESB;

II – Anexo II – Diretrizes para Implementação e Operacionalização do Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG no âmbito da UESB.

Art. 4º As normas, os padrões, os procedimentos, os manuais e as especificações de natureza técnica necessários à execução dos Anexos I e II poderão ser estabelecidos e atualizados por atos administrativos complementares das unidades competentes neles indicadas, desde que não impliquem alteração das competências, dos direitos, dos deveres ou das obrigações estabelecidos nesta Resolução.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 5º Os casos omissos serão dirimidos pelas instâncias competentes previstas nos Anexos I e II desta Resolução, cabendo recurso ao Conselho Universitário – CONSU, observadas as competências institucionais dos demais órgãos e unidades da Universidade.

Art. 6º Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Vitória da Conquista, 21 de setembro de 2026.



Prof. Robério Rodrigues Silva
Presidente do Consu

**PUBLICADA NO
DOE
22 SET. 2026**

AD PLENAM VITAM



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

ANEXO I DA RESOLUÇÃO CONSU Nº 15/2026

POLÍTICA INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS DA UNIVERSIDADE ESTADUAL DO SUDOESTE DA BAHIA – UESB

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS E DA ESTRUTURA NORMATIVA

Art. 1º Esta Política estabelece princípios, diretrizes, estrutura de governança e responsabilidades gerais para a segurança da informação e a proteção dos ativos de informação e tecnológicos sob responsabilidade da Universidade Estadual do Sudoeste da Bahia – UESB.

Parágrafo único. Os requisitos específicos, controles técnicos, regras operacionais, padrões e procedimentos necessários à implementação desta Política serão disciplinados em instrumentos complementares, observada a estrutura de regulamentação e operacionalização prevista neste Anexo.

Art. 2º Esta Política aplica-se:

- I – aos órgãos e unidades acadêmicas e administrativas da Universidade;
- II – aos(às) servidores(as) docentes e técnico-administrativos(as);
- III – aos(às) discentes;
- IV – aos(às) pesquisadores(as), bolsistas, estagiários(as), colaboradores(as) e prestadores(as) de serviços;
- V – às pessoas físicas ou jurídicas que, em razão de vínculo institucional, contrato, convênio, acordo, projeto ou outro instrumento, tenham acesso a informações, sistemas, serviços ou recursos tecnológicos da UESB.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 3º A implementação desta Política observará estrutura complementar de regulamentação e operacionalização, compreendendo:

- I – esta Política, de natureza estratégica, destinada a estabelecer princípios, diretrizes, competências e compromissos institucionais;
- II – instruções normativas, normas específicas e outros atos complementares destinados a estabelecer regras, requisitos, atribuições operacionais, critérios, controles e exceções;
- III – procedimentos, padrões técnicos, manuais, planos e orientações operacionais destinados a definir a forma de execução das atividades e os parâmetros tecnológicos aplicáveis.

§ 1º Os instrumentos complementares deverão observar a legislação aplicável, esta Resolução e as competências nela estabelecidas, não podendo alterar competências, direitos, deveres ou obrigações reservados a ato normativo superior.

§ 2º Os instrumentos previstos no inciso II poderão disciplinar de forma integrada aspectos institucionais, administrativos e técnicos necessários à implementação desta Política.

§ 3º A atualização de requisitos, periodicidades, fluxos, ferramentas, tecnologias e demais aspectos sujeitos a evolução operacional deverá ocorrer, preferencialmente, nos instrumentos complementares.

Art. 4º Para os fins desta Política, consideram-se:

- I – ativo de informação: dado, informação, documento, registro, base de dados, conhecimento ou outro recurso informacional que possua valor para a Universidade ou esteja sob sua responsabilidade;
- II – ativo tecnológico: sistema, aplicação, software, serviço, equipamento, infraestrutura, ambiente computacional, código, repositório ou outro recurso tecnológico utilizado para produzir, processar, armazenar, transmitir, proteger ou disponibilizar informações e serviços institucionais.

Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Parágrafo único. As referências genéricas a ativos institucionais compreendem, conforme o contexto, ativos de informação e ativos tecnológicos.

CAPÍTULO II DOS PRINCÍPIOS

Art. 5º A segurança da informação na UESB observará, entre outros, os seguintes princípios:

- I – confidencialidade;
- II – integridade;
- III – disponibilidade;
- IV – autenticidade;
- V – rastreabilidade;
- VI – privacidade e proteção dos dados pessoais;
- VII – necessidade de conhecimento e privilégio mínimo;
- VIII – prevenção e gestão de riscos;
- IX – continuidade dos serviços institucionais;
- X – transparência, observadas as hipóteses legais de restrição de acesso;
- XI – responsabilização e prestação de contas;
- XII – finalidade, adequação e necessidade no tratamento de dados pessoais;
- XIII – interoperabilidade e padronização, quando aplicáveis;
- XIV – utilização ética e responsável das informações e dos recursos institucionais;
- XV – proporcionalidade entre os controles adotados, a criticidade dos ativos, os riscos identificados e os recursos institucionais disponíveis;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

XVI – definição clara de responsabilidades conforme as competências e o controle efetivamente exercido sobre processos, informações, ativos e camadas ou componentes tecnológicos;

XVII – segregação adequada entre necessidades institucionais, decisões administrativas e execução técnica dos controles;

XVIII – melhoria contínua, com priorização das ações segundo risco, impacto e relevância institucional.

CAPÍTULO III

DA GOVERNANÇA E DAS RESPONSABILIDADES

Art. 6º Compete à Reitoria, no âmbito desta Política:

I – assegurar a existência da estrutura institucional de governança de segurança da informação e proteção de dados;

II – estabelecer ou aprovar prioridades institucionais, consideradas as recomendações das instâncias competentes;

III – decidir, quando cabível, sobre riscos institucionais cuja aceitação exceda a competência das unidades responsáveis;

IV – promover, observadas as disponibilidades administrativa e orçamentária, a provisão dos recursos necessários à implementação das medidas consideradas prioritárias;

V – designar os responsáveis e instâncias previstos nesta Política quando depender de ato da Reitoria.

Art. 7º Fica instituído o Comitê de Segurança da Informação e Proteção de Dados – CSIPD da UESB, órgão colegiado permanente de natureza consultiva, de articulação e de acompanhamento institucional, vinculado à Reitoria.

§ 1º O Comitê será constituído por representantes:

I – da Reitoria;

II – da Pró-Reitoria de Graduação – PROGRAD;



Universidade Estadual do Sudoeste da Bahia – Uesb

Recredenciada pelo Decreto Estadual

Nº 16.825, de 04.07.2016

III – da Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação – PROPPi;

IV – da Pró-Reitoria de Extensão – PROEX;

V – da Pró-Reitoria de Administração – PROAD;

VI – do(a) representante da área de gestão de pessoas da UESB;

VII – da Direção da Unidade de Informática – UINFOR;

VIII – da Gerência da Unidade de Informática – UINFOR;

IX – da Coordenação Local da UINFOR no Campus de Jequié;

X – da Coordenação Local da UINFOR no Campus de Itapetinga;

XI – da área de redes da UINFOR, indicado pela Direção da UINFOR;

XII – da área de suporte da UINFOR, indicado pela Direção da UINFOR.

§ 2º A composição nominal será estabelecida por Portaria da Reitoria.

§ 3º O Comitê poderá convidar especialistas e representantes de outras unidades para reuniões ou grupos de trabalho, sem direito a voto.

Art. 8º Compete ao CSIPD:

I – acompanhar, em nível institucional, a implementação desta Política;

II – promover a articulação entre as unidades envolvidas em segurança da informação e proteção de dados;

III – acompanhar riscos de segurança da informação que, por sua abrangência ou impacto, ultrapassem a competência de uma única unidade;

IV – acompanhar as ações institucionais relacionadas à proteção de dados pessoais, respeitadas as competências do(a) Encarregado(a) e das demais unidades;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

V – promover a integração entre segurança da informação, proteção de dados, gestão documental e demais áreas relacionadas;

VI – propor ações institucionais de conscientização e capacitação;

VII – acompanhar, no âmbito de suas competências, a segurança e a proteção dos dados compartilhados no Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG, na forma do Anexo II;

VIII – encaminhar à Reitoria matérias institucionais que envolvam conflitos de competência, necessidade de decisão administrativa ou riscos relevantes que não possam ser tratados pelas unidades responsáveis.

§ 1º O CSIPD exerce funções de articulação, acompanhamento e assessoramento institucional, não lhe cabendo dirigir, autorizar, revisar ou substituir decisões de natureza predominantemente técnica relativas à arquitetura, configuração, conectividade, operação, segurança ou administração dos ambientes tecnológicos.

§ 2º Recomendações ou manifestações do Comitê que impliquem impacto operacional, necessidade de recursos, alteração de prioridade técnica ou modificação de ambiente tecnológico terão natureza consultiva e dependerão de análise da unidade técnica competente quanto à viabilidade e aos impactos, além de decisão da autoridade administrativa competente quando necessária.

§ 3º O CSIPD não exercerá função de auditoria sobre as unidades institucionais, sem prejuízo da atuação dos órgãos e agentes legalmente competentes de auditoria, controle e fiscalização.

Art. 9º Compete à unidade responsável pela Tecnologia da Informação, no âmbito dos ativos, sistemas, serviços e infraestruturas sob sua gestão:

I – prestar assessoramento técnico às instâncias de governança e às unidades institucionais;

II – definir e manter padrões técnicos e arquitetônicos compatíveis com esta Política e com as normas complementares;

Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

III – implementar, administrar e revisar os controles técnicos de segurança aplicáveis aos ambientes sob sua gestão;

IV – administrar tecnicamente os serviços de infraestrutura, redes, processamento, armazenamento, virtualização, segurança e demais recursos tecnológicos sob sua responsabilidade;

V – apoiar tecnicamente a avaliação de criticidade, riscos, continuidade e requisitos de proteção;

VI – identificar e comunicar riscos, vulnerabilidades, limitações técnicas e necessidades de recursos;

VII – executar ou apoiar ações técnicas de prevenção, contenção, investigação, recuperação e melhoria relacionadas a incidentes;

VIII – elaborar e manter, no âmbito de sua competência, normas técnicas, padrões e procedimentos necessários à operação segura dos ambientes institucionais.

§ 1º As decisões de natureza predominantemente técnica relativas à arquitetura, configuração, conectividade, proteção, administração e operação dos ambientes sob gestão da unidade responsável pela Tecnologia da Informação serão tomadas no âmbito da própria unidade, observados esta Política e os demais atos aplicáveis.

§ 2º As instâncias de governança e as demais unidades institucionais não substituirão a unidade técnica competente na definição dos meios tecnológicos, arquiteturas, configurações ou controles necessários à segurança dos ambientes sob sua gestão.

§ 3º Serão encaminhadas às instâncias administrativas competentes as matérias que envolvam aceitação de risco institucional relevante, conflito de competência, necessidade de recursos extraordinários, decisão jurídica, alteração de competência ou outra matéria que exceda a esfera técnica.

Art. 10. Compete às unidades acadêmicas e administrativas, relativamente aos processos e informações sob sua responsabilidade:



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

- I – informar a finalidade, a relevância, os impactos e as necessidades funcionais dos processos e informações que utilizem;
- II – indicar, no âmbito de suas competências, os perfis funcionais que necessitem de acesso às informações e sistemas;
- III – comunicar alterações de vínculo, atribuição ou necessidade que possam exigir revisão de acessos;
- IV – participar, quando necessário, da avaliação de criticidade e dos requisitos de continuidade;
- V – comunicar incidentes, riscos e mudanças relevantes de que tenham conhecimento;
- VI – cumprir e promover o cumprimento das normas de segurança aplicáveis às atividades sob sua responsabilidade.

Art. 11. Quando a administração de ativo, sistema, aplicação ou infraestrutura tecnológica for compartilhada, delegada ou atribuída a unidade, agente ou terceiro distinto da unidade responsável pela Tecnologia da Informação, os limites de administração e responsabilidade deverão ser formalmente definidos.

§ 1º A definição prevista no caput deverá abranger, conforme aplicável, infraestrutura física ou virtual, conectividade, sistema operacional, aplicações, código-fonte e componentes de software, banco de dados, credenciais, atualizações, cópia de segurança, registros, monitoramento e resposta a incidentes.

§ 2º A disponibilização de infraestrutura tecnológica, conectividade ou outros serviços pela Universidade não implica, por si só, responsabilidade integral da unidade provedora pela administração dos sistemas, aplicações, códigos, dados ou demais componentes mantidos no ambiente.

§ 3º O responsável pela administração técnica do ambiente deverá zelar, dentro das camadas ou componentes tecnológicos que lhe forem atribuídos, pela manutenção, atualização, configuração segura e tratamento das vulnerabilidades, observadas esta Política e as normas complementares aplicáveis.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 4º A responsabilidade pela administração técnica não se confunde com a responsabilidade institucional pela finalidade, utilização, qualidade ou requisitos funcionais das informações e processos.

Art. 12. Compete ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais exercer as atribuições previstas na Lei Geral de Proteção de Dados Pessoais – LGPD e na regulamentação aplicável, bem como orientar as unidades e instâncias de governança quanto à proteção de dados pessoais.

Parágrafo único. A atuação do(a) Encarregado(a) não substitui as responsabilidades das unidades responsáveis pelos processos, das unidades administrativas, dos agentes de tratamento ou dos responsáveis pela administração técnica dos ambientes.

Art. 13. A definição e a implementação de medidas de segurança observarão a criticidade dos ativos, os riscos identificados, as exigências legais e regulatórias, a viabilidade técnica e a disponibilidade de recursos humanos, tecnológicos, materiais e orçamentários.

§ 1º Quando a mitigação de risco depender de aquisição, contratação, ampliação de capacidade, disponibilização de pessoal, serviço especializado ou outro recurso não disponível, a limitação deverá ser registrada e comunicada às instâncias competentes, com indicação, quando possível, das medidas mitigadoras tecnicamente viáveis.

§ 2º Caberá à autoridade competente deliberar, conforme a relevância do risco, sobre priorização, provisão de recursos, tratamento adicional ou aceitação do risco residual.

§ 3º A aceitação de risco institucional relevante não compete exclusivamente à unidade técnica encarregada da implementação do controle.

§ 4º A não implementação integral de controle em razão de impossibilidade técnica, material, operacional ou de insuficiência de recursos, quando devidamente registrada e comunicada, não caracterizará, isoladamente, descumprimento da unidade executora, sem prejuízo da adoção das medidas mitigadoras tecnicamente viáveis e das obrigações legais ou regulatórias de cumprimento obrigatório.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

CAPÍTULO IV

DAS INFORMAÇÕES INSTITUCIONAIS, DA CATEGORIZAÇÃO E DA CRITICIDADE

Art. 14. As informações produzidas, recebidas, armazenadas, processadas ou custodiadas no exercício das atividades institucionais constituem ativos de informação submetidos à governança, proteção e gestão da Universidade, observados os direitos dos titulares, a propriedade intelectual, as restrições legais, os direitos de terceiros e os demais regimes jurídicos aplicáveis.

Art. 15. Os processos e conjuntos relevantes de informações institucionais deverão possuir unidade responsável por sua finalidade, utilização, qualidade e requisitos funcionais de acesso, observadas as competências institucionais aplicáveis.

§ 1º A administração técnica dos sistemas, bancos de dados, equipamentos ou infraestruturas que armazenem ou processem informações institucionais não transfere ao responsável pela administração técnica a responsabilidade pela finalidade administrativa ou acadêmica dessas informações.

§ 2º As unidades técnicas responsáveis pela administração dos ambientes definirão, no âmbito de suas competências, os mecanismos tecnológicos necessários à proteção, processamento, disponibilidade e segurança das informações.

Art. 16. As informações institucionais receberão tratamento compatível com sua natureza, sensibilidade, finalidade, criticidade e eventuais restrições legais de acesso.

§ 1º Para fins administrativos de segurança e tratamento, sem prejuízo das classificações previstas na legislação de acesso à informação, poderão ser adotadas categorias como pública, de uso interno e restrita.

§ 2º As categorias administrativas previstas neste artigo possuem finalidade de proteção e gestão da informação e não criam, substituem ou ampliam hipóteses legais de sigilo ou de classificação previstas na legislação.

Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 3º A categorização como de uso interno ou restrita não constitui, isoladamente, fundamento para negativa de acesso à informação, que observará as hipóteses e procedimentos previstos em lei.

§ 4º Dados pessoais e dados pessoais sensíveis serão tratados de acordo com a LGPD e demais normas aplicáveis, independentemente da categoria administrativa adotada.

Art. 17. A criticidade de processos, sistemas, serviços e ativos será avaliada separadamente da classificação de acesso à informação e considerará, entre outros fatores:

- I – impacto de indisponibilidade, perda, alteração ou comprometimento;
- II – abrangência dos usuários e processos afetados;
- III – dependências e interdependências tecnológicas;
- IV – obrigações legais, regulatórias ou contratuais;
- V – impactos acadêmicos, administrativos, financeiros, científicos, reputacionais ou de segurança;
- VI – capacidade e complexidade de recuperação.

§ 1º A avaliação de criticidade deverá combinar as informações de impacto fornecidas pelas unidades responsáveis pelos processos com a avaliação técnica das unidades competentes, quando houver dependência tecnológica.

§ 2º Os critérios, níveis, metodologia, responsabilidades e procedimentos de revisão serão definidos em norma específica.

Art. 18. Norma específica disciplinará a gestão e o tratamento das informações institucionais, incluindo, conforme aplicável, responsabilidades, categorização administrativa, criticidade, qualidade, armazenamento, compartilhamento, retenção, transferência, conservação, descarte e demais formas de tratamento.

Parágrafo único. A regulamentação relativa à retenção, conservação, arquivamento e descarte observará as competências da gestão



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

documental, as tabelas de temporalidade e a legislação arquivística aplicável.

CAPÍTULO V

DA GESTÃO DE ATIVOS DE INFORMAÇÃO E TECNOLÓGICOS

Art. 19. Os ativos de informação e tecnológicos deverão ser identificados, documentados e protegidos de forma compatível com sua relevância, criticidade e riscos.

§ 1º As unidades acadêmicas e administrativas deverão identificar, no âmbito de suas atribuições, os processos, informações e serviços relevantes sob sua responsabilidade.

§ 2º A unidade responsável pela Tecnologia da Informação manterá inventário dos ativos tecnológicos sob sua administração, em nível de detalhamento compatível com as necessidades de gestão e segurança.

§ 3º A identificação de ativos e responsáveis será realizada progressivamente e integrada aos processos institucionais de gestão de riscos.

Art. 20. A gestão de ativos deverá contemplar responsabilidades ao longo de seu ciclo de vida, incluindo ingresso, utilização, alteração, transferência, manutenção, desativação, descarte e eventual mudança de unidade responsável ou de responsável pela administração técnica.

Art. 21. A implantação ou conexão à infraestrutura institucional de servidor, equipamento ou ambiente tecnológico que não esteja sob administração direta da unidade responsável pela Tecnologia da Informação dependerá de prévia comunicação e de anuência técnica quanto às condições de conexão.

§ 1º A anuência prevista no caput terá por finalidade verificar a compatibilidade do ativo com os requisitos de segurança, arquitetura e conectividade institucional, não implicando transferência de sua administração para a unidade responsável pela Tecnologia da Informação.

Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 2º O ambiente deverá possuir unidade responsável e agente ou prestador responsável por sua administração técnica formalmente identificados.

§ 3º Deverão ser definidos, conforme aplicável, os limites de administração por camada ou componente tecnológico, abrangendo, entre outros, infraestrutura, sistema operacional, aplicações, código e componentes de software, banco de dados, credenciais, atualizações, cópia de segurança, registros, monitoramento e resposta a incidentes.

§ 4º A unidade responsável pela Tecnologia da Informação poderá prestar orientação e apoio técnico à implantação e adequação do ambiente aos requisitos institucionais.

§ 5º O apoio técnico, a disponibilização de conectividade, endereçamento, regras de acesso ou outros recursos institucionais não caracterizam transferência da administração do ambiente à unidade responsável pela Tecnologia da Informação.

§ 6º A conexão e a permanência do ativo na infraestrutura institucional estarão condicionadas ao atendimento dos requisitos de segurança aplicáveis.

§ 7º Quando identificado risco relevante à infraestrutura, aos sistemas, às informações ou aos demais usuários da Universidade, poderão ser aplicadas as medidas técnicas de contenção previstas no art. 39.

§ 8º O descumprimento das responsabilidades ou requisitos aplicáveis poderá ensejar as providências previstas nesta Política e em seus instrumentos complementares, sem prejuízo da apuração cabível nos termos da legislação.

Art. 22. Norma específica disciplinará a gestão de ativos de informação e tecnológicos, incluindo inventário, identificação de responsáveis, ciclo de vida, uso aceitável, transferência, desativação, descarte, ativos administrados por terceiros ou de forma descentralizada e tratamento de exceções.

Parágrafo único. A norma poderá estabelecer requisitos para registro, comunicação e anuência de conexão, atribuição e transferência de



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

administração técnica, controles mínimos de segurança, manutenção de sistemas e softwares, atualização, monitoramento, cópia de segurança, tratamento de vulnerabilidades, resposta a incidentes, regularização, isolamento e desativação de ambientes descentralizados, bem como regras de uso aceitável dos ativos e recursos tecnológicos.

CAPÍTULO VI

DA GESTÃO DE IDENTIDADES, CREDENCIAIS E CONTROLE DE ACESSO

Art. 23. O acesso às informações, sistemas, serviços e recursos tecnológicos institucionais será concedido segundo os princípios da necessidade, do menor privilégio e da vinculação às atribuições acadêmicas, administrativas, profissionais ou técnicas do usuário.

Art. 24. As credenciais individuais são pessoais e intransferíveis, sendo vedado seu compartilhamento.

§ 1º O usuário é responsável pela adequada utilização e proteção das credenciais que lhe forem atribuídas, sem prejuízo da responsabilidade institucional pela adoção dos mecanismos técnicos de autenticação e proteção aplicáveis.

§ 2º É vedada a utilização deliberada de credencial individual atribuída a outra pessoa ou a cessão da própria credencial individual a terceiro.

Art. 25. Contas administrativas, privilegiadas, técnicas, de serviço, de aplicação ou destinadas à integração entre sistemas deverão possuir responsável identificado e controles compatíveis com os riscos decorrentes de sua utilização.

Parágrafo único. O uso de privilégios administrativos deverá ser restrito às atividades que efetivamente os exijam e sujeito a mecanismos de rastreabilidade compatíveis com a criticidade do ambiente.

Art. 26. A gestão de acessos deverá contemplar, conforme aplicável:

- I – identificação individual;
- II – autenticação compatível com o risco;
- III – concessão de privilégios mínimos necessários;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

- IV – segregação de funções quando exigida pela criticidade ou pelo risco;
- V – revisão, adequação, suspensão e revogação de acessos;
- VI – proteção de acessos administrativos e privilegiados;
- VII – registro das operações relevantes.

Art. 27. A concessão, alteração, suspensão e revogação de acessos deverão estar vinculadas à necessidade institucional, às atribuições do usuário e às informações de vínculo mantidas pelas fontes institucionais competentes, sempre que tecnicamente aplicável.

Art. 28. Norma específica disciplinará a gestão de identidades, credenciais, autenticação, privilégios e controle de acesso, incluindo concessão, revisão, alteração, suspensão, revogação, autenticação multifator, contas privilegiadas, contas técnicas e de serviço, segredos de autenticação, exceções e responsabilidades operacionais.

CAPÍTULO VII

DO ARMAZENAMENTO, DAS CÓPIAS DE SEGURANÇA, DA RECUPERAÇÃO E DA CONTINUIDADE

Art. 29. As informações institucionais deverão ser armazenadas preferencialmente em ambientes administrados, contratados ou formalmente autorizados pela Universidade, observados os requisitos de segurança, proteção de dados e continuidade aplicáveis.

Art. 30. A Universidade manterá processo institucional de cópia de segurança e recuperação para os sistemas, serviços e conjuntos de dados incluídos no escopo do serviço de backup, com controles proporcionais à criticidade e aos riscos.

§ 1º Os requisitos de recuperação deverão considerar as necessidades do processo institucional e a avaliação técnica do serviço.

§ 2º As cópias de segurança deverão ser protegidas contra acesso, alteração, exclusão ou comprometimento indevidos e submetidas a mecanismos de verificação e restauração compatíveis com o risco.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 3º A responsabilidade técnica pelas rotinas de backup limitar-se-á aos ativos e serviços abrangidos pelo respectivo serviço institucional ou formalmente atribuídos ao responsável pela administração técnica.

Art. 31. A hospedagem ou o armazenamento de sistema, aplicação ou informação em infraestrutura institucional não implica, por si só, inclusão automática no serviço de cópia de segurança.

§ 1º A abrangência do serviço, os critérios de inclusão e exclusão e as responsabilidades pelas cópias de ativos administrados por unidades ou terceiros serão definidos em norma específica.

§ 2º Quando ativo ou serviço relevante não estiver abrangido pelo serviço institucional de cópia de segurança, deverá existir definição de responsabilidade quanto às medidas de proteção e recuperação aplicáveis, observados os arts. 11 e 21.

Art. 32. A Universidade estabelecerá medidas de continuidade e recuperação para os processos e serviços considerados essenciais ou críticos, segundo avaliação de risco e capacidade institucional.

§ 1º A definição dos requisitos de continuidade deverá considerar o impacto informado pelas unidades responsáveis pelos processos e a viabilidade técnica indicada pelas unidades competentes.

§ 2º A incompatibilidade entre o nível de continuidade requerido e a capacidade disponível será tratada no processo de gestão de riscos.

Art. 33. Normas específicas disciplinarão:

I – o serviço institucional de cópia de segurança e recuperação, incluindo escopo, responsabilidades, periodicidade, retenção, proteção, restauração, testes, monitoramento, exceções e critérios de inclusão;

II – a continuidade e a recuperação de serviços, incluindo critérios de criticidade, requisitos de recuperação, planos, responsabilidades, testes e tratamento de indisponibilidades.

CAPÍTULO VIII



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

DA SEGURANÇA DE SISTEMAS, REDES E INFRAESTRUTURA TECNOLÓGICA

Art. 34. Os ambientes tecnológicos institucionais deverão possuir controles de segurança proporcionais à criticidade dos ativos e aos riscos identificados, incluindo, quando aplicável:

- I – proteção de perímetro e segmentação de redes;
- II – mecanismos de detecção, prevenção e contenção de ameaças;
- III – proteção contra códigos maliciosos;
- IV – gestão de atualizações, configurações e vulnerabilidades;
- V – criptografia de dados em trânsito e, quando necessária, em armazenamento;
- VI – proteção de interfaces de programação de aplicações – APIs;
- VII – controle de acesso administrativo;
- VIII – gestão de certificados, chaves, segredos de autenticação e credenciais técnicas;
- IX – registros e monitoramento de eventos;
- X – avaliações técnicas de segurança compatíveis com o risco;
- XI – proteção de endpoints, dispositivos e meios de acesso remoto quando integrantes do ambiente institucional.
- XII – controle de meios de conectividade externa independentes da infraestrutura institucional;
- XIII – controle da instalação e utilização de equipamentos capazes de alterar, estender, intermediar ou redistribuir a conectividade de rede.

Art. 35. No âmbito dos ambientes, serviços e infraestruturas sob sua gestão, bem como quanto às condições técnicas de conexão de ativos à infraestrutura institucional, a unidade responsável pela Tecnologia da Informação poderá estabelecer padrões técnicos obrigatórios de arquitetura, configuração,



Universidade Estadual do Sudoeste da Bahia – Uesb

Recredenciada pelo Decreto Estadual

Nº 16.825, de 04.07.2016

conectividade, administração, atualização, proteção e monitoramento necessários à segurança e à interoperabilidade institucional.

§ 1º Os padrões técnicos deverão observar esta Política, as normas complementares e a gestão de riscos, podendo ser atualizados conforme evolução tecnológica e operacional.

§ 2º A contratação, implantação ou utilização, nas dependências da Universidade, de serviço de acesso à Internet, enlace de dados ou outro meio de conectividade externa independente da infraestrutura institucional dependerá de prévia anuência da unidade responsável pela Tecnologia da Informação.

§ 3º É vedada a implantação unilateral da conectividade prevista no § 2º. A unidade interessada deverá apresentar formalmente a necessidade, sua justificativa e, quando aplicável, os requisitos que não possam ser adequadamente atendidos pela infraestrutura institucional existente.

§ 4º A análise técnica poderá estabelecer condições de instalação, segmentação, isolamento, interconexão, monitoramento e acesso aos recursos institucionais necessárias à preservação da segurança, da rastreabilidade e da estabilidade da infraestrutura. A existência de necessidade específica devidamente justificada não implica autorização automática de interligação à rede institucional.

§ 5º A instalação ou conexão à infraestrutura institucional de roteadores, switches, pontos de acesso sem fio, repetidores, gateways, equipamentos destinados à tradução de endereços de rede – NAT, servidores de DHCP ou DNS, dispositivos de tunelamento ou outros equipamentos capazes de alterar, estender, intermediar ou redistribuir a conectividade dependerá de prévia anuência da unidade responsável pela Tecnologia da Informação, independentemente da propriedade do equipamento.

§ 6º É vedada a utilização não autorizada de equipamento ou serviço que crie ou redistribua acesso à rede institucional, estabeleça sub-redes ou redes sem fio não autorizadas, forneça serviços de infraestrutura capazes de interferir nos serviços institucionais, realize roteamento, NAT, tunelamento ou interligação de redes em desacordo com os padrões



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

aplicáveis, reduza indevidamente a identificação ou a rastreabilidade dos usuários e dispositivos ou possibilite contorno dos mecanismos institucionais de autenticação, segmentação ou proteção.

Art. 36. A Universidade manterá processo de gestão de vulnerabilidades e atualizações de segurança orientado por risco, criticidade, exposição e viabilidade de tratamento.

§ 1º O tratamento das vulnerabilidades será priorizado segundo severidade, exposição, criticidade, impacto, dependências, compatibilidade e risco operacional, observados os critérios definidos em norma específica.

§ 2º Vulnerabilidades que representem risco grave ou iminente poderão ensejar medidas emergenciais de contenção.

§ 3º Riscos decorrentes de vulnerabilidades cujo tratamento dependa de recursos ou decisões fora da competência da unidade executora serão tratados nos termos do art. 13.

Art. 37. A Universidade adotará mecanismos de criptografia, gestão de certificados, chaves e segredos de autenticação compatíveis com os riscos e com a natureza dos serviços, especialmente nos acessos administrativos, integrações e tratamento de informações que requeiram proteção adicional.

Art. 38. Os ambientes físicos que suportem serviços tecnológicos relevantes deverão possuir medidas de proteção compatíveis com sua criticidade, contemplando controle de acesso, condições ambientais, energia, proteção contra eventos físicos e registro das ocorrências relevantes, quando aplicável.

Parágrafo único. A proteção desses ambientes será executada de forma coordenada entre as unidades responsáveis pela infraestrutura física, patrimonial, elétrica, predial e tecnológica, conforme suas respectivas competências.

Art. 39. A unidade responsável pela administração do recurso afetado ou pela infraestrutura de segurança e conectividade correspondente poderá, no âmbito dos recursos sob sua gestão, adotar medidas emergenciais de contenção, inclusive restrição ou suspensão temporária de acessos, comunicações,



Universidade Estadual do Sudoeste da Bahia – Uesb

Recredenciada pelo Decreto Estadual

Nº 16.825, de 04.07.2016

dispositivos, sistemas ou serviços que apresentem risco concreto e relevante à segurança ou à continuidade institucional.

§ 1º As medidas deverão ser proporcionais ao risco e limitadas ao tempo necessário à contenção, análise ou adoção de medida substitutiva adequada.

§ 2º A ocorrência, a medida adotada e seus fundamentos deverão ser registrados e comunicados às unidades afetadas e às instâncias competentes, conforme o caso.

§ 3º As medidas poderão alcançar ativos administrados por outras unidades ou terceiros quando necessárias à proteção da infraestrutura institucional, limitando-se, nesses casos, às camadas, componentes tecnológicos e recursos sob administração da unidade que adotar a medida.

§ 4º Identificada conectividade externa ou equipamento de rede não autorizado cuja operação esteja em desacordo com os requisitos institucionais ou possa comprometer a segurança, a rastreabilidade ou a estabilidade da rede, a unidade responsável pela Tecnologia da Informação poderá suspender ou restringir tecnicamente sua conectividade.

§ 5º Na hipótese do § 4º, a unidade responsável pela Tecnologia da Informação poderá solicitar à unidade responsável pelo ambiente a desconexão, regularização, substituição ou remoção do equipamento ou serviço, sem prejuízo das demais providências cabíveis.

Art. 40. Normas específicas poderão disciplinar, isolada ou conjuntamente, segurança de redes, servidores, virtualização, endpoints, acesso remoto, vulnerabilidades e atualizações, criptografia, certificados, segredos de autenticação, conectividade externa, equipamentos de rede, segurança física de ambientes tecnológicos e demais controles previstos neste Capítulo.

CAPÍTULO IX

DO DESENVOLVIMENTO, DA AQUISIÇÃO, DAS INTEGRAÇÕES, DOS SERVIÇOS EM NUVEM E DE TERCEIROS



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 41. O desenvolvimento, a aquisição, a contratação, a implantação e a manutenção de sistemas e serviços tecnológicos deverão considerar requisitos de segurança da informação e proteção de dados proporcionais aos riscos e à criticidade do objeto.

Art. 42. A administração do ciclo de vida de sistemas deverá observar, quando tecnicamente aplicável e proporcional ao risco, controles de mudança, segregação adequada entre ambientes ou funções e proteção dos acessos privilegiados utilizados no desenvolvimento, manutenção e operação.

Art. 43. A integração de sistemas institucionais com sistemas externos deverá utilizar mecanismos seguros e padronizados, compatíveis com os requisitos de interoperabilidade, autenticação, autorização, rastreabilidade e proteção das informações envolvidas.

§ 1º O intercâmbio automatizado de informações utilizará, preferencialmente, protocolos padronizados e interfaces de programação de aplicações – APIs, observadas as normas técnicas aplicáveis.

§ 2º É vedado o acesso direto de sistemas externos às bases de dados institucionais, ressalvadas as hipóteses expressamente previstas em lei ou tecnicamente justificadas e formalmente autorizadas pela unidade ou autoridade competente pelo processo ou informação, mediante avaliação da unidade técnica competente e observados os requisitos de proteção de dados quando aplicáveis.

Art. 44. A utilização de serviços em nuvem, plataformas externas ou outros serviços tecnológicos não administrados diretamente pela Universidade deverá ser precedida de avaliação compatível com a natureza das informações, os riscos, as responsabilidades contratuais, a proteção de dados e os requisitos de continuidade aplicáveis.

Parágrafo único. A avaliação envolverá as unidades competentes de acordo com a natureza do serviço e dos riscos identificados, podendo compreender aspectos técnicos, contratuais, jurídicos, de proteção de dados, continuidade e gestão da informação.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 45. Contratos, convênios, acordos e demais instrumentos que envolvam acesso, desenvolvimento, administração, armazenamento, processamento ou compartilhamento de informações e recursos tecnológicos deverão contemplar, quando pertinente, requisitos de segurança da informação, confidencialidade, proteção de dados pessoais, comunicação de incidentes, continuidade, reversibilidade e responsabilidades das partes.

Parágrafo único. O acompanhamento das obrigações de segurança caberá aos responsáveis pelo instrumento e às unidades competentes, com apoio técnico especializado quando necessário.

Art. 46. Normas específicas disciplinarão, conforme a necessidade institucional, o desenvolvimento e a aquisição segura de sistemas, a gestão de mudanças, as integrações e APIs, os serviços em nuvem, o acesso de terceiros e os requisitos de segurança aplicáveis a contratações tecnológicas.

CAPÍTULO X

DOS REGISTROS, DO MONITORAMENTO, DA AUDITORIA E DA RASTREABILIDADE

Art. 47. Sistemas e serviços institucionais deverão manter registros de eventos compatíveis com sua criticidade, finalidade e capacidade técnica, suficientes para apoiar segurança, auditoria, investigação e prestação de contas, conforme aplicável.

§ 1º Os registros poderão abranger autenticações, acessos administrativos, alterações relevantes, operações de compartilhamento, eventos de segurança e outras ações definidas em norma específica.

§ 2º Os registros deverão ser protegidos contra acesso, alteração ou exclusão não autorizados.

Art. 48. O monitoramento de eventos de segurança será adotado conforme criticidade, risco, disponibilidade de fontes de registro e capacidade operacional.

§ 1º A exigência de monitoramento ativo, contínuo ou em regime especial dependerá de definição expressa de escopo, responsabilidade e capacidade necessária à sua execução.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 2º O monitoramento deverá possuir finalidade institucional definida e observar necessidade, proporcionalidade, proteção de dados pessoais e restrição de acesso aos registros produzidos.

Art. 49. Registros, documentos e informações relacionados a operações institucionais deverão ser disponibilizados aos agentes competentes de auditoria, controle e fiscalização quando legalmente requisitados, observadas as restrições de acesso, a proteção das informações envolvidas e a legislação aplicável.

Art. 50. Norma específica disciplinará geração, conteúdo, proteção, retenção, acesso, correlação, monitoramento, disponibilização e descarte de registros e trilhas de auditoria, segundo os riscos, requisitos legais e capacidade dos ambientes.

CAPÍTULO XI

DO COMPARTILHAMENTO DE INFORMAÇÕES E DA PROTEÇÃO DE DADOS PESSOAIS

Art. 51. O compartilhamento de informações institucionais com órgãos, entidades ou terceiros deverá:

- I – possuir finalidade institucional e fundamento jurídico adequado;
- II – limitar-se às informações necessárias ao atendimento da finalidade;
- III – observar as normas de segurança da informação e proteção de dados pessoais;
- IV – utilizar mecanismos de transmissão e acesso compatíveis com o risco;
- V – possibilitar rastreabilidade adequada das operações;
- VI – observar, quando aplicável, padrões técnicos e semânticos de interoperabilidade;
- VII – respeitar restrições legais relativas à propriedade intelectual, sigilo e demais limitações aplicáveis.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 52. A autorização institucional para compartilhamento caberá à unidade responsável pelo processo ou informação, observadas as manifestações jurídicas, de proteção de dados ou de outras áreas quando exigidas.

Parágrafo único. A unidade técnica responsável pela integração ou transmissão definirá e implementará os mecanismos tecnológicos de proteção, não lhe cabendo, por essa atuação, determinar isoladamente a finalidade ou a base jurídica do compartilhamento.

Art. 53. Quando o compartilhamento envolver dados pessoais, deverão ser observados adicionalmente a finalidade do tratamento, a base legal aplicável, as categorias de dados, os agentes envolvidos, os requisitos de retenção, as medidas de segurança, os registros pertinentes e os direitos dos titulares, na forma da legislação aplicável.

Art. 54. Norma específica poderá disciplinar os fluxos de autorização, responsabilidades, registros, meios técnicos, integrações, transferências, retenção e demais requisitos relacionados ao compartilhamento de informações e dados pessoais.

CAPÍTULO XII

DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 55. A UESB manterá processo institucional de identificação, registro, classificação, tratamento e acompanhamento de incidentes de segurança da informação, proporcional à natureza, abrangência, criticidade e impacto das ocorrências.

Art. 56. Qualquer pessoa abrangida por esta Política que tenha conhecimento de incidente ou suspeita de incidente envolvendo informações, sistemas ou recursos institucionais deverá comunicar a ocorrência pelos canais definidos pela Universidade tão logo dela tenha conhecimento.

Art. 57. O tratamento de incidentes observará classificação de severidade, priorização, capacidade operacional e responsabilidades definidas para os ativos afetados.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 1º As unidades e os responsáveis pela administração técnica dos ativos afetados executarão, dentro das camadas ou componentes tecnológicos e das competências que lhes tenham sido atribuídas, as ações de contenção, análise e recuperação cabíveis, podendo aplicar as medidas emergenciais previstas no art. 39.

§ 2º As unidades afetadas deverão fornecer informações e adotar as providências administrativas necessárias ao tratamento do incidente.

§ 3º Incidentes que excedam a capacidade interna poderão demandar acionamento de fornecedores, cooperação externa, contratação especializada ou outras providências institucionais.

Art. 58. Incidentes envolvendo dados pessoais deverão ser comunicados ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais e tratados segundo a LGPD, a regulamentação da Autoridade Nacional de Proteção de Dados – ANPD e os fluxos institucionais aplicáveis.

Parágrafo único. As comunicações a titulares, à ANPD ou a outras autoridades serão realizadas pela Universidade segundo as competências e procedimentos definidos, não se confundindo com as atividades técnicas de contenção e recuperação.

Art. 59. Norma específica disciplinará a gestão de incidentes, incluindo canais de comunicação, classificação, escalonamento, responsabilidades, contenção, preservação de evidências, análise, recuperação, comunicação institucional, registro, tratamento pós-incidente e acionamento de apoio externo.

CAPÍTULO XIII

DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 60. A segurança da informação será orientada por processo contínuo de gestão de riscos, de forma proporcional à relevância dos ativos e processos envolvidos.

Parágrafo único. O processo compreenderá, conforme aplicável, identificação de ativos, ameaças, vulnerabilidades, impactos,



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

probabilidade, controles existentes, tratamento, risco residual, monitoramento e revisão.

Art. 61. Os riscos poderão ser evitados, mitigados, compartilhados, transferidos ou aceitos, conforme critérios institucionais.

§ 1º As unidades técnicas poderão identificar, analisar e recomendar medidas de tratamento, mas a aceitação de risco que produza impacto institucional relevante caberá à autoridade que detenha competência sobre o processo e suas consequências.

§ 2º Riscos cuja aceitação ou tratamento exceda a competência da unidade responsável serão encaminhados à autoridade administrativa competente, podendo o CSIPD ser consultado quando a matéria envolver repercussão institucional, proteção de dados ou competências de múltiplas unidades.

§ 3º A aceitação de risco não afasta o cumprimento de obrigação legal, regulatória, judicial ou contratual de observância obrigatória, nem autoriza tratamento de informação ou dado pessoal em desconformidade com a legislação aplicável.

Art. 62. Quando o tratamento recomendado depender de recurso não disponível ou de decisão externa à competência da unidade executora, deverão ser registrados, em nível compatível com a relevância do risco, a condição identificada, o tratamento recomendado, a limitação existente, as medidas compensatórias possíveis e o encaminhamento realizado.

Art. 63. A priorização das ações de segurança observará, entre outros critérios:

- I – criticidade e impacto institucional;
- II – probabilidade e severidade dos riscos;
- III – exposição a ameaças;
- IV – obrigações legais, regulatórias ou contratuais;
- V – riscos aos direitos e liberdades dos titulares de dados pessoais;
- VI – dependência de processos e serviços essenciais;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

VII – viabilidade técnica e disponibilidade de recursos.

Parágrafo único. Prioridades decorrentes de programas, convênios, acordos ou obrigações externas específicas serão tratadas nos respectivos instrumentos, sem alterar a priorização geral desta Política.

Art. 64. Norma específica disciplinará a metodologia de gestão de riscos de segurança da informação, incluindo critérios de avaliação, níveis de risco, responsabilidades, registro, tratamento, aceitação, acompanhamento e revisão.

CAPÍTULO XIV

DAS RESPONSABILIDADES DOS USUÁRIOS E DA CULTURA DE SEGURANÇA

Art. 65. Toda pessoa que utilize informações ou recursos tecnológicos da UESB é responsável por utilizá-los de forma adequada e compatível com a finalidade autorizada.

Parágrafo único. Constituem deveres dos usuários, sem prejuízo de outros previstos em norma específica:

- I – preservar suas credenciais e meios de autenticação;
- II – utilizar informações e recursos exclusivamente para finalidades autorizadas;
- III – observar regras de categorização e tratamento da informação;
- IV – comunicar incidentes, suspeitas ou vulnerabilidades de que tenham conhecimento;
- V – evitar armazenamento ou compartilhamento de informações institucionais em serviços ou dispositivos não autorizados quando houver restrição aplicável;
- VI – observar as normas de proteção de dados pessoais;
- VII – cumprir orientações de segurança aplicáveis aos recursos utilizados.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 66. A UESB promoverá ações de conscientização, capacitação e formação em segurança da informação e proteção de dados, de acordo com prioridades e planejamento institucional.

Parágrafo único. As ações poderão envolver o CSIPD, o(a) Encarregado(a), a unidade responsável pela Tecnologia da Informação, as unidades de gestão de pessoas, comunicação institucional e demais setores competentes.

Art. 67. O uso aceitável dos ativos e recursos tecnológicos poderá ser regulamentado em norma específica, observados esta Política e os regimes legais e disciplinares aplicáveis.

Parágrafo único. O descumprimento desta Política ou de seus instrumentos complementares poderá ensejar apuração e adoção das providências cabíveis nos termos da legislação e das normas institucionais aplicáveis, observados os direitos e garantias pertinentes.

CAPÍTULO XV

DAS NORMAS COMPLEMENTARES E DA IMPLEMENTAÇÃO

Art. 68. As matérias disciplinadas nesta Política poderão ser regulamentadas e detalhadas por instruções normativas, normas técnicas, padrões, procedimentos, planos, manuais e demais instrumentos administrativos compatíveis com a natureza do assunto.

§ 1º Os instrumentos complementares poderão detalhar atribuições operacionais, requisitos técnicos, fluxos de trabalho, critérios, classificações, procedimentos, controles, periodicidades, prazos, exceções e demais condições necessárias à implementação desta Política, observadas as competências estabelecidas nesta Resolução.

§ 2º A regulamentação complementar poderá abranger conjuntamente aspectos institucionais, administrativos, organizacionais e técnicos quando necessários à adequada disciplina da matéria.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 3º Os instrumentos complementares poderão ser atualizados em razão da evolução dos riscos, das tecnologias, dos requisitos institucionais, da capacidade operacional e da legislação aplicável.

§ 4º Matérias correlatas poderão ser disciplinadas conjuntamente em um mesmo instrumento quando isso favorecer coerência e eficiência administrativa.

Art. 69. Instrumento complementar que discipline atividade operacional continuada deverá definir, em nível compatível com o tema, seu escopo, as atribuições operacionais, as condições de execução e os recursos ou capacidades necessários.

Parágrafo único. Requisitos que impliquem monitoramento contínuo, regime de plantão, prazo máximo de resposta, expansão substancial de escopo, aquisição de solução, contratação de serviço ou dedicação permanente de pessoal deverão ser precedidos de avaliação de viabilidade e capacidade institucional.

Art. 70. A implementação desta Política será progressiva e orientada por riscos, criticidade, maturidade institucional e disponibilidade de recursos técnicos, humanos e orçamentários.

§ 1º As prioridades de implementação observarão os critérios estabelecidos nesta Política e nas normas complementares aplicáveis.

§ 2º A existência de requisito ainda não implementado deverá ensejar avaliação e tratamento do respectivo risco, não se presumindo, isoladamente, omissão da unidade executora quando sua implementação depender de recurso, capacidade ou decisão fora de sua competência.

§ 3º Obrigações legais ou regulatórias de cumprimento obrigatório serão submetidas às instâncias competentes para adoção tempestiva das providências necessárias.

Art. 71. Esta Política e seus instrumentos complementares serão revistos quando houver alteração relevante no contexto institucional, regulatório, tecnológico ou de riscos que justifique sua atualização.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Parágrafo único. Os instrumentos de menor nível poderão prever ciclos próprios de revisão compatíveis com a velocidade de mudança do respectivo tema.

CAPÍTULO XVI DAS DEFINIÇÕES

Art. 72. Para os fins desta Política, considera-se:

I – autenticação: processo de verificação da identidade de usuário, sistema ou entidade;

II – ativo tecnológico de administração descentralizada: servidor, equipamento, sistema computacional ou outro recurso tecnológico conectado à infraestrutura institucional cuja administração técnica, total ou parcial, seja exercida por unidade, agente ou terceiro distinto da unidade central responsável pela Tecnologia da Informação;

III – camada ou componente tecnológico: parte funcional ou estrutural de ambiente tecnológico suscetível de administração ou responsabilidade específica, incluindo, conforme aplicável, infraestrutura física, conectividade e rede, virtualização, sistema operacional, plataformas e serviços intermediários, banco de dados, aplicação, código e componentes de software, mecanismos de autenticação, registros, cópias de segurança e demais componentes necessários à operação do ambiente;

IV – confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa, sistema, órgão ou entidade não autorizada;

V – criticidade: grau de impacto associado ao comprometimento, à indisponibilidade, à perda ou à alteração de ativo, serviço ou processo;

VI – criptografia: conjunto de técnicas destinado a proteger informação por meio de transformação controlada, de modo a restringir seu acesso ou alteração indevida;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

VII – disponibilidade: propriedade de que a informação ou serviço esteja acessível e utilizável, sob demanda, por quem esteja autorizado;

VIII – incidente de segurança da informação: evento ou conjunto de eventos que comprometa ou possa comprometer a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações ou serviços institucionais;

IX – integridade: propriedade de preservação da exatidão, completude e consistência da informação contra alteração ou destruição não autorizada ou acidental;

X – interoperabilidade: capacidade de sistemas distintos trocarem e utilizarem informações de forma consistente;

XI – responsável pela administração técnica: unidade, agente ou prestador formalmente incumbido da administração de determinada camada ou componente tecnológico, serviço ou ambiente, nos limites das atribuições que lhe tenham sido conferidas;

XII – risco residual: risco remanescente após a consideração dos controles existentes ou planejados;

XIII – rastreabilidade: propriedade que permite reconstruir ou identificar operações relevantes realizadas sobre informação, sistema ou serviço;

XIV – segredo de autenticação: informação confidencial utilizada por sistema, aplicação, serviço ou mecanismo tecnológico para autenticação, autorização, proteção criptográfica ou estabelecimento de confiança, incluindo, conforme aplicável, tokens, chaves de acesso, chaves privadas, senhas de contas técnicas, segredos compartilhados e outros valores equivalentes;

XV – tratamento de dados pessoais: toda operação realizada com dados pessoais, nos termos da LGPD;

XVI – titular: pessoa natural a quem se referem os dados pessoais objeto de tratamento, nos termos da LGPD;

XVII – unidade responsável pelo processo ou informação: unidade institucional responsável, conforme suas competências, pela finalidade,



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

utilização, qualidade, impacto e requisitos funcionais relacionados ao processo ou conjunto de informações.

CAPÍTULO XVII

DAS DISPOSIÇÕES FINAIS E DAS REFERÊNCIAS NORMATIVAS

Art. 73. Programas, convênios, acordos ou iniciativas que imponham requisitos específicos de segurança, proteção de dados ou interoperabilidade serão executados conforme seus instrumentos próprios e esta Política, cabendo às unidades responsáveis articular as providências técnicas, administrativas e orçamentárias necessárias.

Art. 74. Os casos omissos serão apreciados pela instância competente conforme a natureza da matéria.

I – questões predominantemente técnicas relativas aos ambientes, serviços e infraestruturas sob gestão da unidade responsável pela Tecnologia da Informação serão tratadas pela unidade técnica competente;

II – questões de governança, segurança institucional ou proteção de dados que ultrapassem a competência de uma única unidade poderão ser submetidas ao CSIPD;

III – questões administrativas, de recursos, conflito de competência ou decisão institucional serão encaminhadas à Reitoria ou à autoridade competente;

IV – eventual apreciação pelo CONSU observará as competências previstas na legislação, no Estatuto, no Regimento e nesta Resolução.

DAS REFERÊNCIAS NORMATIVAS

Art. 75. As ações de segurança da informação e proteção de dados no âmbito da UESB observarão, no que couber:

I – a Lei Federal nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação – LAI;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

II – a Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD;

III – a Lei Federal nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet;

IV – o Decreto Federal nº 8.771, de 11 de maio de 2016, que regulamenta a Lei Federal nº 12.965/2014, com suas alterações posteriores;

V – o Decreto Estadual nº 13.473, de 28 de novembro de 2011, que homologa a Resolução CIGOV nº 02/2011 e institui a Política de Segurança da Informação no âmbito dos órgãos e entidades da Administração Pública do Poder Executivo do Estado da Bahia;

VI – a Lei Estadual nº 12.618, de 28 de dezembro de 2012, que regula o acesso a informações no âmbito do Estado da Bahia;

VII – o Decreto Estadual nº 24.375, de 2 de março de 2026, que regulamenta a Lei Estadual nº 12.618/2012;

VIII – o Decreto Estadual nº 24.105, de 14 de novembro de 2025, que dispõe sobre a aplicação da LGPD e institui a Política Estadual de Proteção de Dados Pessoais – PEPD no âmbito dos órgãos e entidades do Poder Executivo Estadual;

IX – as regulamentações da Autoridade Nacional de Proteção de Dados – ANPD;

X – as normas e regulamentos específicos aplicáveis às atividades da Universidade, inclusive os relacionados ao Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG, na forma do Anexo II;

XI – a família ABNT NBR ISO/IEC 27000 e outros referenciais técnicos reconhecidos, como fontes de boas práticas, observada sua adequação à realidade institucional;

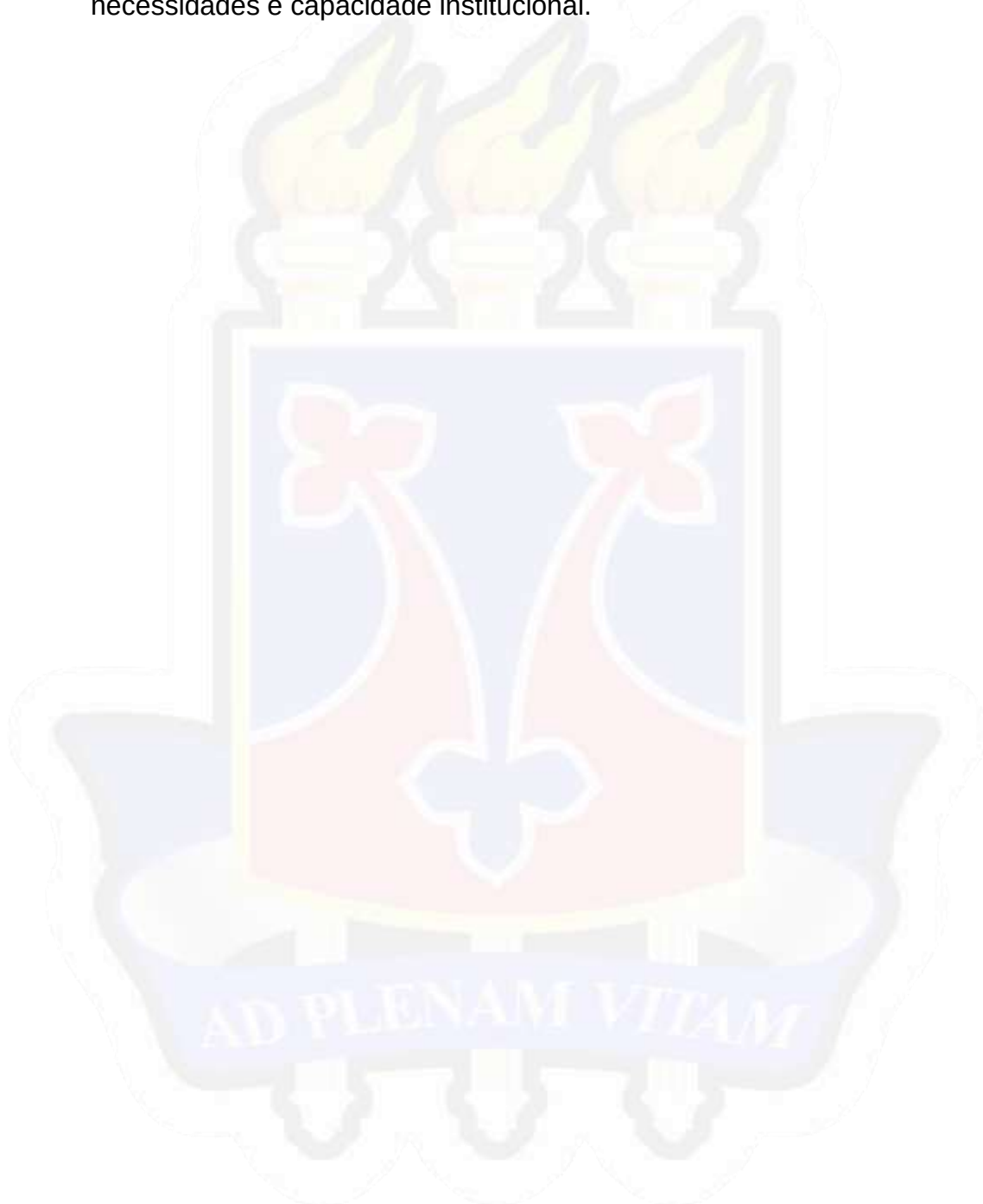
XII – demais normas legais e infralegais aplicáveis.

Parágrafo único. A adoção de referencial técnico de boas práticas não implica, por si só, obrigação de implementação integral, certificação ou



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

aquisição de solução específica, devendo sua aplicação observar riscos,
necessidades e capacidade institucional.





Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

ANEXO II DA RESOLUÇÃO CONSU Nº 15/2026

DIRETRIZES PARA IMPLEMENTAÇÃO E OPERACIONALIZAÇÃO DO PROGRAMA DE GOVERNANÇA COLABORATIVA DE INFORMAÇÕES DA PÓS-GRADUAÇÃO – GoPG NO ÂMBITO DA UESB

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 1º. A participação da UESB no Programa de Governança Colaborativa de Informações da Pós-Graduação – GoPG observará a Portaria CAPES nº 158, de 17 de agosto de 2023, a Instrução Normativa GAB/Capes nº 1, de 23 de abril de 2026, com suas alterações posteriores, este Anexo, o Anexo I desta Resolução e os padrões, modelos, guias, manuais, repositórios de metadados, comunicados e especificações técnicas e semânticas oficialmente publicados pela CAPES para execução do Programa.

§ 1º A implementação do GoPG no âmbito da UESB compreenderá, de forma integrada, os seguintes eixos:

- I – Gestão Organizacional;
- II – Gestão da Informação;
- III – Tecnologia da Informação;
- IV – Segurança e Proteção de Dados;
- V – Comunicação e Relacionamento.

§ 2º A atuação institucional no âmbito do GoPG observará a finalidade pública e legítima do Programa, a utilização responsável e ética dos dados, a interoperabilidade, a segurança da informação, a proteção dos dados pessoais, a transparência, a rastreabilidade, a prestação de contas e a divisão de responsabilidades prevista nesta Resolução.

CAPÍTULO II DAS COMPETÊNCIAS DA UESB

Art. 2º. Para os fins do GoPG, compete à UESB, observada a distribuição interna de competências estabelecida no Anexo I:

- I – designar formalmente os representantes institucionais responsáveis pela coordenação e pela execução técnica das ações do Programa;



Universidade Estadual do Sudoeste da Bahia – Uesb

Recredenciada pelo Decreto Estadual

Nº 16.825, de 04.07.2016

- II – designar formalmente o setor ou unidade responsável pelo tratamento, compartilhamento e gestão dos dados tratados no contexto do GoPG;
- III – disponibilizar os recursos humanos, tecnológicos e materiais necessários à execução das atividades sob sua responsabilidade;
- IV – manter os dados institucionais em formato estruturado e interoperável, em conformidade com os padrões técnicos, semânticos e modelos definidos pela CAPES;
- V – disponibilizar os dados institucionais segundo os modelos e conjuntos mínimos oficialmente definidos pela CAPES;
- VI – adotar controles e procedimentos internos destinados a assegurar a atualização, consistência, integridade, veracidade e qualidade das informações sob sua responsabilidade;
- VII – utilizar, preferencialmente, as fontes originárias das informações, observadas as fontes externas admitidas pela regulamentação do GoPG;
- VIII – manter controle e registro das operações de compartilhamento, assegurando rastreabilidade, transparência e prestação de contas;
- IX – limitar o tratamento e o compartilhamento ao mínimo necessário ao atendimento das finalidades do GoPG, observados os princípios da finalidade, necessidade, adequação e proporcionalidade;
- X – adotar medidas técnicas e administrativas adequadas à proteção dos dados pessoais tratados no âmbito do GoPG;
- XI – utilizar protocolos padronizados de coleta de dados e Interfaces de Programação de Aplicativos – APIs, de acordo com as especificações oficialmente estabelecidas pela CAPES;
- XII – zelar pela adequada utilização dos dados e informações disponibilizados no âmbito do Programa;
- XIII – assegurar, no âmbito de suas competências, o exercício dos direitos dos titulares de dados pessoais, nos termos da LGPD;
- XIV – promover transparência ativa das ações de interoperabilidade e compartilhamento de dados, observadas a legislação de acesso à informação, a LGPD e as normas da CAPES;
- XV – prevenir, identificar, comunicar e tratar incidentes de segurança relacionados às atividades sob sua responsabilidade;
- XVI – assegurar acesso aos documentos, registros e informações relacionados à execução do GoPG aos agentes competentes da Administração Pública, internos ou externos, quando solicitado no exercício de suas atribuições legais, para fins de auditoria, controle ou fiscalização;
- XVII – observar as restrições legais relativas à propriedade intelectual;



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

XVIII – cooperar de forma contínua com a CAPES para o regular desenvolvimento do GoPG, oferecendo, dentro de suas possibilidades e competências, os meios e facilidades necessários à execução das ações sob sua responsabilidade.

CAPÍTULO III

DAS FONTES DE DADOS

Art. 3º. Constituem fontes de dados utilizadas na interoperabilidade do GoPG, observada a regulamentação da CAPES:

- I – os sistemas acadêmicos institucionais, relativamente às informações de discentes, docentes, pós-doutores, disciplinas, matrículas, orientações e demais dados acadêmicos relacionados aos Programas de Pós-Graduação;
- II – os repositórios institucionais responsáveis pelo registro e disponibilização da produção intelectual, incluindo dissertações, teses, artigos, livros, capítulos, trabalhos em eventos e demais produtos vinculados aos Programas de Pós-Graduação;
- III – as fontes externas de dados relacionadas às informações da pós-graduação utilizadas, conforme definição da CAPES, para compor, complementar ou atualizar dados acadêmicos, científicos e institucionais na Plataforma Sucupira.

§ 1º Os conjuntos de dados e os serviços de interoperabilidade associados a cada fonte observarão os padrões técnicos, semânticos, modelos de dados, metadados e conjuntos mínimos oficialmente definidos pela CAPES.

§ 2º As correções e atualizações deverão ser realizadas, sempre que aplicável, na respectiva fonte originária da informação, preservadas as informações anteriormente consolidadas nos termos das normas da CAPES.

§ 3º Quando a fonte originária for externa à UESB, a Universidade adotará apenas as providências que estejam compreendidas em suas competências, observados os mecanismos de correção ou atualização próprios da respectiva fonte.

CAPÍTULO IV

DA COORDENAÇÃO INSTITUCIONAL

Art. 4º. Fica a Pró-Reitoria de Pesquisa e Pós-Graduação – PROPPi responsável pela coordenação institucional do GoPG no âmbito da UESB, em articulação com a unidade responsável pela Tecnologia da Informação e com o(a) Encarregado(a) pelo Tratamento de Dados Pessoais.

Parágrafo único. A coordenação institucional prevista neste artigo não afasta nem substitui as competências administrativas, funcionais ou técnicas das unidades envolvidas, especialmente as competências da unidade responsável pela Tecnologia da Informação estabelecidas no Anexo I.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 5º. A Reitoria designará formalmente, mediante Portaria:

- I – os representantes institucionais responsáveis pela coordenação e pela execução das ações do GoPG;
- II – o setor ou unidade responsável pelo tratamento, compartilhamento e gestão dos dados tratados no contexto do GoPG;
- III – quando necessário, pontos focais para um ou mais eixos do GoPG, conforme a estrutura administrativa e as necessidades de implementação da Universidade.

§ 1º A designação prevista no inciso II não transfere à unidade indicada responsabilidade exclusiva pela produção, veracidade, correção, finalidade ou administração técnica dos dados mantidos em fontes, sistemas ou ambientes administrados por outras unidades.

§ 2º As designações deverão observar as competências institucionais existentes e delimitar as atribuições de coordenação, gestão da informação e execução técnica necessárias ao Programa.

CAPÍTULO V

DO REGISTRO DAS OPERAÇÕES DE COMPARTILHAMENTO

Art. 6º. Todo compartilhamento de dados entre a UESB e a CAPES no âmbito do GoPG deverá possuir controle e registro que assegure rastreabilidade, transparência e prestação de contas, contendo, no mínimo:

- I – os dados compartilhados;
- II – a finalidade da transferência;
- III – o fundamento jurídico;
- IV – o prazo de retenção, quando aplicável.

Parágrafo único. Outros elementos necessários à rastreabilidade das operações poderão ser estabelecidos pela regulamentação da CAPES, por norma institucional específica ou por procedimentos técnicos aplicáveis ao serviço de interoperabilidade.

CAPÍTULO VI

DO TRATAMENTO DE DADOS PESSOAIS

Art. 7º. O tratamento de dados pessoais realizado no âmbito do GoPG observará a finalidade pública específica da Avaliação Nacional da Pós-Graduação, da gestão da informação no Sistema Nacional de Pós-Graduação – SNPG e das políticas públicas relacionadas à promoção da ciência e à melhoria da pós-graduação.

§ 1º A UESB e a CAPES, no âmbito das operações de compartilhamento e interoperabilidade do GoPG, atuarão na condição de controladoras conjuntas dos dados pessoais objeto dessas operações, nos termos da regulamentação da CAPES.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 2º A UESB adotará as medidas técnicas e administrativas necessárias ao cumprimento das responsabilidades que lhe competem como controladora conjunta.

§ 3º O tratamento e o compartilhamento de dados pessoais realizados no âmbito do GoPG não dependerão do consentimento do titular quando fundamentados nas bases legais aplicáveis à execução da política pública, sem prejuízo dos deveres de transparência, segurança e garantia dos direitos dos titulares.

§ 4º É vedado o compartilhamento dos dados pessoais tratados no âmbito do GoPG com terceiros estranhos à relação entre a UESB e a CAPES, salvo nas hipóteses expressamente autorizadas por lei.

§ 5º A qualificação prevista no § 1º refere-se à relação entre a UESB e a CAPES no âmbito das operações do GoPG e não altera, por si só, a distribuição interna de competências entre as unidades da Universidade estabelecida no Anexo I.

CAPÍTULO VII

DA INTEROPERABILIDADE TÉCNICA

Art. 8º. A interoperabilidade entre os sistemas da UESB e da CAPES ocorrerá mediante protocolos padronizados de coleta de dados e Interfaces de Programação de Aplicativos – APIs, observados os padrões técnicos, semânticos e de segurança oficialmente estabelecidos pela CAPES.

§ 1º É vedado o acesso direto aos bancos de dados da UESB ou da CAPES para fins de operacionalização da interoperabilidade do GoPG, devendo o intercâmbio de informações ocorrer pelos mecanismos de integração previstos na regulamentação e nas especificações técnicas da CAPES.

§ 2º A UESB poderá utilizar as ferramentas tecnológicas disponibilizadas pela CAPES ou soluções institucionais próprias, desde que atendam aos requisitos técnicos e aos padrões mínimos de tecnologia e segurança oficialmente estabelecidos.

§ 3º A definição dos meios tecnológicos, arquiteturas, configurações, controles de segurança e formas de integração dos ambientes sob gestão da UESB caberá à unidade responsável pela Tecnologia da Informação, observados o Anexo I e os requisitos obrigatórios do GoPG.

CAPÍTULO VIII

DA VERIFICAÇÃO E CORREÇÃO DE DADOS

Art. 9º. A UESB adotará as providências compreendidas em suas competências para possibilitar aos integrantes dos Programas de Pós-Graduação conhecer, conferir e, quando cabível, promover a correção dos dados utilizados no processo de interoperabilidade, inclusive mediante os mecanismos disponibilizados pela CAPES e os sistemas institucionais correspondentes.

Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

§ 1º Identificada inconsistência em informação cuja fonte originária seja administrada pela UESB, sua correção deverá ocorrer na respectiva fonte, observados os procedimentos institucionais aplicáveis.

§ 2º Quando a informação tiver origem em fonte externa, a correção observará os mecanismos e competências próprios da respectiva fonte, cabendo à UESB orientar ou encaminhar a questão apenas quando isso estiver compreendido em suas atribuições.

§ 3º A disponibilização de informações para conferência não altera, por si só, a condição de dado oficial ou consolidado, que será definida segundo os procedimentos e etapas estabelecidos pela CAPES.

CAPÍTULO IX

DA TRANSPARÊNCIA ATIVA

Art. 10. A UESB promoverá transparência ativa sobre as ações de interoperabilidade, o tratamento e o compartilhamento de dados realizados no âmbito do GoPG, em conformidade com a Lei de Acesso à Informação, a LGPD e as normas da CAPES, assegurando informações adequadas sobre finalidades, fontes, categorias de dados e procedimentos institucionais relacionados à interoperabilidade, observadas as hipóteses legais de restrição de acesso.

CAPÍTULO X

DA GESTÃO DE INCIDENTES NO ÂMBITO DO GoPG

Art. 11. Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais compartilhados no âmbito do GoPG, a UESB comunicará imediatamente a ocorrência ao(à) Encarregado(a) pelo Tratamento de Dados Pessoais da CAPES e adotará, no âmbito de suas responsabilidades, as medidas necessárias à contenção, mitigação e prevenção de novas ocorrências, sem prejuízo dos procedimentos gerais de gestão de incidentes previstos no Anexo I, inclusive da comunicação ao(à) Encarregado(a) da UESB.

Parágrafo único. A comunicação à CAPES deverá conter, no mínimo:

- I – descrição da natureza dos dados afetados;
- II – informações sobre os titulares envolvidos;
- III – indicação das medidas adotadas para contenção ou mitigação do incidente;
- IV – riscos relacionados ao incidente.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

CAPÍTULO XI

DA ADESÃO, PERMANÊNCIA E DESVINCULAÇÃO INSTITUCIONAL

Art. 12. A adesão institucional da UESB ao GoPG será formalizada mediante Declaração de Adesão assinada pelo Reitor ou por representante legalmente autorizado, observados os procedimentos e documentos exigidos pela CAPES.

§ 1º A assinatura da Declaração de Adesão implica ciência e aceitação das regras, condições, responsabilidades e procedimentos estabelecidos pela Portaria CAPES nº 158/2023, pela Instrução Normativa GAB/Capes nº 1/2026, com suas alterações posteriores, e pelos atos complementares oficialmente aplicáveis ao Programa.

§ 2º A adesão produzirá efeitos externos a partir da publicação do extrato da Declaração de Adesão no Diário Oficial da União, na forma da regulamentação da CAPES.

Art. 13. A permanência da UESB no GoPG, eventual descredenciamento por descumprimento das obrigações aplicáveis e eventual desvinculação voluntária observarão os procedimentos e efeitos definidos pela regulamentação da CAPES.

Parágrafo único. A manifestação de desvinculação voluntária pela UESB será formalizada pelo Reitor ou por representante legalmente autorizado, sem prejuízo da avaliação institucional dos impactos acadêmicos, administrativos e tecnológicos decorrentes da medida.

CAPÍTULO XII

DOS PROCEDIMENTOS TÉCNICOS, DOS RECURSOS E DAS ATUALIZAÇÕES

Art. 14. Os procedimentos técnicos necessários à implementação da interoperabilidade com o GoPG deverão observar os manuais, guias, modelos de dados, repositórios de metadados, APIs, protocolos, comunicados e demais especificações técnicas e semânticas oficialmente publicados pela CAPES.

Parágrafo único. A atualização dos padrões e especificações técnicas pela CAPES será incorporada aos procedimentos institucionais de interoperabilidade independentemente de alteração desta Resolução, desde que não implique modificação de competência, direito, dever ou obrigação institucional estabelecida em ato normativo superior.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 15. A execução das ações no âmbito do GoPG não implicará transferência de recursos financeiros entre a CAPES e a UESB, cabendo à Universidade custear, com recursos próprios, as despesas relativas às atividades sob sua responsabilidade.

Parágrafo único. Necessidades adicionais de pessoal, infraestrutura, contratação, aquisição ou capacidade tecnológica identificadas durante a implementação serão tratadas pelos processos institucionais competentes e segundo os mecanismos de gestão de riscos e recursos previstos no Anexo I, sem afastar as obrigações assumidas pela UESB perante a CAPES.

CAPÍTULO XIII

DOS CASOS OMISSOS E DA DISTRIBUIÇÃO DE COMPETÊNCIAS

Art. 16. Os casos omissos relacionados à implementação interna deste Anexo serão apreciados pela instância competente conforme a natureza da matéria, observado o disposto no Anexo I.

- I – questões de natureza predominantemente técnica relativas à interoperabilidade, arquitetura, integração, configuração, segurança e operação dos ambientes tecnológicos serão tratadas pela unidade responsável pela Tecnologia da Informação, no âmbito de suas competências;
 - II – questões relacionadas à coordenação institucional do Programa, à gestão acadêmica da pós-graduação e às necessidades funcionais das informações serão tratadas pela PROPI e pelas unidades institucionalmente competentes;
 - III – questões relativas à proteção de dados pessoais observarão as competências do(a) Encarregado(a) e das unidades responsáveis pelos processos e ambientes envolvidos;
 - IV – questões de segurança da informação ou proteção de dados que envolvam competências de múltiplas unidades ou repercussão institucional poderão ser submetidas ao CSIPD, observado o caráter consultivo e de articulação previsto no Anexo I;
 - V – questões que envolvam decisão administrativa, disponibilidade de recursos, conflito de competência ou matéria que exceda a esfera técnica serão encaminhadas à Reitoria ou à autoridade competente.
- § 1º As dúvidas ou situações omissas relativas à interpretação ou aplicação das normas, procedimentos e especificações do GoPG de competência da CAPES serão submetidas à Diretoria de Avaliação da Pós-Graduação – DAV/CAPES, na forma da regulamentação do Programa.
- § 2º Eventual apreciação pelo Conselho Universitário – CONSU limitar-se-á às matérias inseridas em sua competência institucional e não afastará as obrigações



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

decorrentes da regulamentação da CAPES aplicável à participação da UESB no GoPG.

CAPÍTULO XIV

DAS DEFINIÇÕES E DA INTEGRAÇÃO COM O ANEXO I

Art. 17. Para os fins deste Anexo, sem prejuízo das definições constantes do Anexo I, considera-se:

- I – controladoria conjunta: condição atribuída pela regulamentação da CAPES à UESB e à CAPES, no âmbito das operações de compartilhamento e interoperabilidade de dados pessoais do GoPG, com as responsabilidades decorrentes da LGPD e dos atos aplicáveis;
- II – fonte de dados: sistema, repositório, base ou serviço, institucional ou externo, do qual sejam obtidas informações utilizadas nos fluxos do GoPG;
- III – fonte originária: fonte identificada como origem da informação para fins do GoPG e na qual, quando aplicável, deverá ocorrer sua correção ou atualização;
- IV – fonte externa: fonte de dados não administrada diretamente pela UESB utilizada, conforme a regulamentação ou os mecanismos da CAPES, para compor, complementar ou atualizar informações da pós-graduação;
- V – interoperabilidade semântica: capacidade de sistemas distintos trocarem informações preservando significado comum por meio de modelos, metadados, vocabulários, identificadores e demais padrões semânticos definidos para a integração;
- VI – ponto focal: representante designado para articulação e acompanhamento de um ou mais eixos do GoPG, sem criação, por si só, de nova unidade administrativa ou alteração das competências institucionais existentes;
- VII – unidade responsável pela gestão dos dados do GoPG: setor ou unidade formalmente designado pela UESB para coordenar o tratamento, o compartilhamento e a gestão dos dados no contexto do Programa, sem prejuízo das responsabilidades das unidades responsáveis pelas fontes, processos e ambientes tecnológicos;
- VIII – custódia de dados: guarda ou manutenção de dados em ambiente sob responsabilidade de determinada parte, não implicando, por si só, propriedade sobre as informações nem transferência das responsabilidades funcionais ou institucionais relativas à sua finalidade;
- IX – documento técnico oficial da CAPES: guia, manual, modelo, repositório, especificação, comunicado ou outro documento disponibilizado por canal oficial da CAPES para detalhamento da execução do GoPG.



Universidade Estadual do Sudoeste da Bahia – Uesb
Recredenciada pelo Decreto Estadual
Nº 16.825, de 04.07.2016

Art. 18. Aplicam-se subsidiariamente a este Anexo, no que couber, os princípios, definições, regras de segurança da informação, distribuição de competências e referências normativas estabelecidos no Anexo I desta Resolução.

§ 1º Os requisitos específicos estabelecidos pela regulamentação da CAPES para o GoPG prevalecerão, no âmbito exclusivo das atividades do Programa, quando forem mais específicos ou restritivos que as regras institucionais gerais.

§ 2º A aplicação de requisito específico do GoPG não implica sua extensão automática a sistemas, serviços, processos ou atividades institucionais estranhos ao Programa.