



PLANO DE CONTINGÊNCIA DA BIBLIOTECA

Prevenção, resposta, continuidade, recuperação, comunicação e evidências

Brasília, DF – 2026.

Sumário

TÍTULO I DA FINALIDADE, ESCOPO, PREMISSAS E PRINCÍPIOS	3
CAPÍTULO I - DA FINALIDADE E DO ESCOPO.....	3
CAPÍTULO II - DAS PREMISSAS E PRINCÍPIOS	3
TÍTULO II DA GOVERNANÇA E DAS RESPONSABILIDADES.....	4
CAPÍTULO I - DA COORDENAÇÃO DO PLANO.....	4
CAPÍTULO II - DA CADEIA DE ACIONAMENTO.....	4
TÍTULO III DA CLASSIFICAÇÃO E DO CICLO DE RESPOSTA.....	5
CAPÍTULO I - DA CRITICIDADE.....	5
CAPÍTULO II - DO CICLO DE RESPOSTA.....	5
CAPÍTULO III - DOS TEMPOS DE RESPOSTA.....	6
TÍTULO IV DA PREVENÇÃO, PRONTIDÃO E CONTINUIDADE.....	6
CAPÍTULO I - DA PREVENÇÃO TECNOLÓGICA.....	6
CAPÍTULO II - DA PREVENÇÃO CONTRATUAL E BIBLIOGRÁFICA.....	6
CAPÍTULO III - DA PREVENÇÃO FÍSICA E OPERACIONAL	7
TÍTULO V DA COMUNICAÇÃO, ACESSIBILIDADE E PROTEÇÃO DE DADOS	7
CAPÍTULO I - DA COMUNICAÇÃO.....	7
CAPÍTULO II - DA ACESSIBILIDADE	8
CAPÍTULO III - DA PROTEÇÃO DE DADOS E SEGURANÇA.....	8
TÍTULO VI DA RECUPERAÇÃO, TESTES, EVIDÊNCIAS E REVISÃO	8
CAPÍTULO I - DA RECUPERAÇÃO E ANÁLISE POSTERIOR	8
CAPÍTULO II - DOS TESTES E EXERCÍCIOS	9
CAPÍTULO III - DAS EVIDÊNCIAS, REVISÃO E VIGÊNCIA	9
ANEXO I MATRIZ OPERACIONAL DE CENÁRIOS E RESPOSTAS.....	10
ANEXO II CRITÉRIOS DE CRITICIDADE E ESCALONAMENTO	11
ANEXO III MENSAGENS INSTITUCIONAIS DE CONTINGÊNCIA	12
ANEXO IV REPOSITÓRIO MÍNIMO DE EVIDÊNCIAS	12
ANEXO V REFERÊNCIAS NORMATIVAS ESSENCIAIS.....	13

TÍTULO I

DA FINALIDADE, ESCOPO, PREMISSAS E PRINCÍPIOS

CAPÍTULO I - DA FINALIDADE E DO ESCOPO

Art. 1. O Plano de Contingência da Biblioteca Digital estabelece prevenção, resposta, continuidade, recuperação, comunicação, registro e melhoria diante de eventos que afetem o acesso, os serviços, o espaço e os recursos informacionais.

Art. 2. O Plano aplica-se à Minha Biblioteca, demais plataformas, autenticação, portal institucional, conectividade, energia, dez computadores de apoio, recursos de acessibilidade, atendimento, contratos e evidências.

Art. 3. O Plano integra-se aos planos institucionais de tecnologia, segurança da informação, proteção de dados, emergência predial, acessibilidade e continuidade acadêmica.

Art. 4. A Biblioteca possui acervo exclusivamente digital, razão pela qual riscos tecnológicos, contratuais e de acessibilidade recebem tratamento prioritário.

Art. 5. O espaço físico é apoio ao acesso e estudo, não local de guarda de acervo impresso.

Art. 6. O Plano aplica-se durante e fora do expediente, respeitada a disponibilidade dos responsáveis e dos canais de acionamento.

CAPÍTULO II - DAS PREMISSAS E PRINCÍPIOS

Art. 7. A continuidade será planejada sem prometer disponibilidade absoluta ou ininterrupta além das condições contratuais e técnicas.

Art. 8. A resposta priorizará segurança de pessoas, proteção de dados, continuidade acadêmica, acessibilidade, legalidade e comunicação.

Art. 9. Soluções temporárias serão autorizadas, documentadas, proporcionais e encerradas após a recuperação.

Art. 10. Nenhuma contingência autoriza violação de direitos autorais, compartilhamento de credenciais ou uso de sistema não autorizado.

Art. 11. A comunicação será tempestiva, clara, acessível e proporcional ao impacto.

Art. 12. Incidentes serão tratados como fonte de aprendizagem, sem ocultação, subnotificação ou atribuição precipitada de culpa.

Art. 13. A resposta preservará evidências e rastreabilidade desde a identificação até o encerramento.

TÍTULO II

DA GOVERNANÇA E DAS RESPONSABILIDADES

CAPÍTULO I - DA COORDENAÇÃO DO PLANO

Art. 14. O bibliotecário responsável coordena academicamente e tecnicamente este Plano no âmbito da Biblioteca.

Art. 15. A execução é compartilhada entre Biblioteca, TI, Direção-Geral, Direção Acadêmica, Departamento de Regulação, NAI/NAPS, infraestrutura, segurança e fornecedores, conforme a ocorrência.

Art. 16. A Biblioteca identifica impacto acadêmico, aciona responsáveis, orienta usuários, registra evidências e acompanha recuperação.

Art. 17. O TI diagnostica e trata rede, autenticação, equipamentos, segurança, integrações, cópias de segurança e sistemas.

Art. 18. A Direção-Geral decide prioridades, recursos, comunicação institucional ampla, medidas contratuais e continuidade excepcional.

Art. 19. A Direção Acadêmica coordena alternativas pedagógicas, prazos e orientações aos cursos.

Art. 20. Coordenações e NDEs analisam substituição de bibliografia e efeitos sobre PPCs e unidades curriculares.

Art. 21. O NAI/NAPS avalia barreiras e alternativas acessíveis.

Art. 22. Infraestrutura e segurança atuam em energia, interdição, incêndio, evacuação, acesso físico e condições prediais.

Art. 23. Fornecedores atuam conforme contrato, suporte e níveis de serviço aplicáveis.

CAPÍTULO II - DA CADEIA DE ACIONAMENTO

Art. 24. A ocorrência será comunicada primeiro ao responsável funcional mais próximo, sem retardar acionamento emergencial necessário.

Art. 25. Eventos tecnológicos serão registrados no sistema institucional de chamados e comunicados à Biblioteca.

Art. 26. Eventos acadêmicos ou bibliográficos serão comunicados à Biblioteca e à Coordenação afetada.

Art. 27. Eventos de segurança física seguirão protocolos de emergência e orientação da equipe competente.

Art. 28. Eventos de dados pessoais ou segurança cibernética serão imediatamente encaminhados ao TI e à governança de privacidade.

Art. 29. A ausência de um responsável acionará seu substituto funcional ou a autoridade hierarquicamente competente.

Art. 30. A cadeia de acionamento não depende de lista nominal neste documento e permanecerá atualizada nos diretórios institucionais.

TÍTULO III

DA CLASSIFICAÇÃO E DO CICLO DE RESPOSTA

CAPÍTULO I - DA CRITICIDADE

Art. 31. As ocorrências serão classificadas como baixa, média, alta ou crítica.

Art. 32. A classificação considerará segurança, dados, número de usuários, cursos afetados, proximidade de avaliação ou atividade, duração, existência de alternativa e acessibilidade.

Art. 33. Baixa criticidade corresponde a impacto pontual, com alternativa imediata e sem risco relevante.

Art. 34. Média criticidade corresponde a impacto limitado, com degradação do serviço ou necessidade de coordenação entre áreas.

Art. 35. Alta criticidade corresponde a indisponibilidade relevante, múltiplos usuários, atividade acadêmica próxima ou ausência de alternativa adequada.

Art. 36. Criticidade crítica corresponde a risco à segurança, incidente de dados, indisponibilidade ampla e prolongada, perda contratual essencial ou impacto regulatório imediato.

Art. 37. A classificação poderá ser elevada ou reduzida conforme novos fatos.

CAPÍTULO II - DO CICLO DE RESPOSTA

Art. 38. O ciclo de resposta compreenderá:

- I –detecção e confirmação;
- II – registro e classificação;
- III – contenção e proteção;
- IV –diagnóstico e acionamento;
- V – continuidade temporária;
- VI –comunicação e atualizações;
- VII – recuperação e validação;
- VIII – encerramento e análise posterior;
- IX –plano de ação e teste de efetividade.

Art. 39. A confirmação distinguirá falha do usuário, autenticação, rede, equipamento, título, plataforma, contrato ou conteúdo.

Art. 40. O registro conterá data, origem, impacto, classificação, responsáveis, ações, comunicações, evidências e encerramento.

Art. 41. A contenção buscará impedir ampliação do dano sem destruir evidências.

Art. 42. A alternativa temporária será escolhida pela área competente e comunicada aos usuários afetados.

Art. 43. A recuperação somente será declarada após teste funcional e, quando cabível, teste de acessibilidade.

Art. 44. O encerramento registrará causa conhecida ou provável, duração, impacto, providências e prevenção.

CAPÍTULO III - DOS TEMPOS DE RESPOSTA

Art. 45. Ocorrências críticas terão acionamento imediato e atualização periódica enquanto persistirem.

Art. 46. Ocorrências altas terão tratamento prioritário no mesmo período de funcionamento institucional.

Art. 47. Ocorrências médias serão tratadas conforme fila priorizada e impacto acadêmico.

Art. 48. Ocorrências baixas serão programadas sem comprometer continuidade ou segurança.

Art. 49. Os tempos constituem objetivos internos e não substituem níveis de serviço contratuais.

Art. 50. Quando não houver solução no prazo inicialmente estimado, os usuários receberão atualização e orientação alternativa.

TÍTULO IV

DA PREVENÇÃO, PRONTIDÃO E CONTINUIDADE

CAPÍTULO I - DA PREVENÇÃO TECNOLÓGICA

Art. 51. A Biblioteca e o TI realizarão testes periódicos de acesso, autenticação, rede, computadores e recursos assistivos.

Art. 52. Os dez computadores serão inventariados, atualizados, protegidos e submetidos a manutenção preventiva.

Art. 53. A conectividade contará com medidas institucionais de redundância ou alternativa compatível com o risco e a capacidade.

Art. 54. Credenciais administrativas serão restritas e protegidas por controles adequados.

Art. 55. Logs, chamados e relatórios serão preservados segundo a política de segurança e retenção.

Art. 56. Mudanças em integração, portal ou autenticação serão testadas antes de entrar em produção sempre que possível.

CAPÍTULO II - DA PREVENÇÃO CONTRATUAL E BIBLIOGRÁFICA

Art. 57. A Biblioteca manterá controle de vigências, renovações, suporte, alterações de catálogo e condições de acesso.

Art. 58. A revisão semestral identificará títulos incluídos, retirados, alterados ou inacessíveis.

Art. 59. Títulos críticos serão mapeados às unidades curriculares e períodos de oferta.

Art. 60. Riscos de retirada ou não renovação serão comunicados antes do impacto, sempre que previsíveis.

Art. 61. Alternativas bibliográficas serão avaliadas e formalizadas pelo NDE, sem substituição automática.

Art. 62. Bases abertas serão usadas apenas quando legais, qualificadas, estáveis e academicamente adequadas.

CAPÍTULO III - DA PREVENÇÃO FÍSICA E OPERACIONAL

Art. 63. O espaço observará inspeção elétrica, sinalização, acessibilidade, climatização, limpeza, iluminação e rotas de fuga.

Art. 64. Emergências físicas seguirão o plano predial, a orientação da brigada e os serviços públicos competentes.

Art. 65. A interdição do espaço não interromperá o acesso remoto ao acervo, quando a plataforma e a internet do usuário estiverem disponíveis.

Art. 66. A ausência do bibliotecário será coberta por equipe treinada para orientação inicial, registro e escalonamento.

Art. 67. Tutoriais e canais remotos permanecerão disponíveis em formato acessível.

Art. 68. A equipe receberá capacitação e simulação periódicas sobre este Plano.

TÍTULO V

DA COMUNICAÇÃO, ACESSIBILIDADE E PROTEÇÃO DE DADOS

CAPÍTULO I - DA COMUNICAÇÃO

Art. 69. A comunicação informará serviço afetado, início conhecido, impacto, alternativa, canal de suporte e próxima atualização.

Art. 70. Causas não confirmadas não serão apresentadas como definitivas.

Art. 71. A comunicação poderá ocorrer por site, sistema acadêmico, e-mail, ambiente virtual, avisos no campus e canais oficiais.

Art. 72. Eventos amplos ou críticos serão comunicados pela área institucional autorizada, em articulação com Biblioteca e TI.

Art. 73. Docentes e Coordenações receberão orientação específica quando houver impacto sobre unidade curricular ou avaliação.

Art. 74. O encerramento será comunicado aos públicos afetados quando a indisponibilidade tiver sido previamente divulgada.

Art. 75. Mensagens serão preservadas como evidência do incidente.

CAPÍTULO II - DA ACESSIBILIDADE

Art. 76. Comunicações e alternativas deverão ser acessíveis e compatíveis com as necessidades dos usuários afetados.

Art. 77. Falha de recurso assistivo ou ausência de formato acessível será tratada como incidente acadêmico, não como mera solicitação opcional.

Art. 78. O NAI/NAPS apoiará a definição de alternativa individual ou coletiva.

Art. 79. A recuperação incluirá teste de acessibilidade quando a ocorrência afetar tecnologia assistiva ou conteúdo acessível.

Art. 80. A alternativa preservará resultados de aprendizagem, autonomia e privacidade.

CAPÍTULO III - DA PROTEÇÃO DE DADOS E SEGURANÇA

Art. 81. Incidente com dados pessoais seguirá o plano institucional de resposta e será comunicado à governança de privacidade.

Art. 82. A equipe não divulgará dados pessoais, credenciais, logs ou detalhes técnicos que ampliem o risco.

Art. 83. Suspeita de comprometimento de conta poderá motivar bloqueio preventivo e redefinição de credenciais.

Art. 84. Evidências digitais serão preservadas com controle de acesso e integridade.

Art. 85. Comunicações externas sobre incidente de segurança dependerão de autorização institucional competente.

Art. 86. O restabelecimento observará validação de segurança, não apenas retorno aparente do serviço.

TÍTULO VI

DA RECUPERAÇÃO, TESTES, EVIDÊNCIAS E REVISÃO

CAPÍTULO I - DA RECUPERAÇÃO E ANÁLISE POSTERIOR

Art. 87. A recuperação será validada pela área técnica e pela Biblioteca, conforme a natureza do serviço.

Art. 88. A validação verificará acesso, autenticação, conteúdo, desempenho e acessibilidade.

Art. 89. Incidentes altos ou críticos produzirão relatório de análise posterior.

Art. 90. O relatório identificará causa, linha do tempo, impacto, ações, comunicação, evidências, lições e plano de prevenção.

Art. 91. As ações terão responsável, prazo, prioridade e forma de verificação.

Art. 92. Falhas recorrentes serão elevadas à Direção e poderão motivar revisão contratual, tecnológica ou processual.

CAPÍTULO II - DOS TESTES E EXERCÍCIOS

Art. 93. O Plano será testado ao menos semestralmente e antes de avaliação externa relevante.

Art. 94. Os testes incluirão indisponibilidade de plataforma, falha de autenticação, internet, computador, retirada de título e acessibilidade.

Art. 95. O exercício poderá ser de mesa, técnico ou operacional, conforme o risco.

Art. 96. Os resultados serão registrados com participantes, cenário, tempos, falhas e melhorias.

Art. 97. A execução de teste não poderá causar indisponibilidade desnecessária nem violar contratos ou segurança.

Art. 98. Ações corretivas serão verificadas no teste seguinte ou em validação específica.

CAPÍTULO III - DAS EVIDÊNCIAS, REVISÃO E VIGÊNCIA

Art. 99. A Biblioteca manterá incidentes, chamados, mensagens, testes, relatórios, planos de ação e evidências de encerramento.

Art. 100. Os dados serão analisados por tipo, criticidade, duração, recorrência e impacto.

Art. 101. Resultados agregados serão compartilhados com Direção, Coordenações, NDEs e CPA.

Art. 102. O Plano será revisado anualmente ou após incidente crítico, mudança contratual, tecnológica ou institucional relevante.

Art. 103. Casos omissos serão decididos pela Direção-Geral, ouvidas as áreas técnicas.

Art. 104. Este Plano entra em vigor após aprovação pelo CONSU e publicação institucional.

ANEXO I

MATRIZ OPERACIONAL DE CENÁRIOS E RESPOSTAS

OCORRÊNCIA	NÍVEL	LÍDER	AÇÃO IMEDIATA	ALTERNATIVA	COMUNICAÇÃO	ENCERRAMENTO
Minha Biblioteca indisponível	Alta	Biblioteca	Confirmar em rede e dispositivo distintos; abrir chamado ao fornecedor e TI.	Orientar materiais equivalentes já aprovados; ajustar atividade se necessário.	Biblioteca, Coordenações, estudantes afetados.	Teste de acesso e registro do fornecedor.
Falha de autenticação	Alta	TI	Verificar vínculo, integração, lote de usuários e mensagens de erro.	Acesso assistido sem compartilhamento de senha; priorização de turmas afetadas.	Usuários, Biblioteca e Coordenações.	Login validado com perfis de teste.
Internet do campus interrompida	Alta	TI	Acionar conectividade e verificar redundância.	Orientar acesso remoto por conexão própria; remanejar atividade para ambiente conectado.	Comunidade presente no campus.	Teste de navegação nos dez computadores.
Queda de energia	Alta	Infraestrutura	Proteger pessoas e equipamentos; seguir protocolo predial.	Acesso remoto fora do campus; reprogramação de atendimento presencial.	Público campus no e setores afetados.	Energia estabilizada e equipamentos testados.
Falha em computador de apoio	Média	TI	Isolar equipamento, registrar patrimônio e diagnóstico.	Remanejar para estação disponível ou Laboratório de Informática agendado.	Biblioteca e usuários presentes.	Equipamento liberado após teste.
Falha de vários computadores	Alta	TI	Identificar causa comum, rede, atualização ou energia.	Priorizar estações funcionais, remanejar e orientar dispositivos próprios.	Biblioteca, Direção e usuários.	Amostra de estações testada e inventário atualizado.
Retirada de título	Alta	Biblioteca	Mapear PPCs, UCs, turmas e período de oferta.	Alternativa equivalente analisada; orientação docente temporária.	Coordenação, NDE, docentes e estudantes.	Decisão do NDE, matriz e PPC atualizados.
Contrato próximo do término	Alta	Biblioteca/Direção	Inventariar dependências e decisão de renovação.	Plano de migração, contratação ou atualização bibliográfica.	Direção, Coordenações e NDEs.	Contrato renovado ou alternativa implantada.
Site institucional indisponível	Média	TI/Comunicação	Confirmar falha e preservar acesso direto seguro via sistema acadêmico.	Divulgar canal alternativo oficial sem expor chaves.	Comunidade acadêmica.	Site e rotas de acesso testados.

OCORRÊNCIA	NÍVEL	LÍDER	AÇÃO IMEDIATA	ALTERNATIVA	COMUNICAÇÃO	ENCERRAMENTO
Título sem acessibilidade	Alta	Biblioteca/NAI	Testar barreira e registrar necessidade.	Formato ou título equivalente; apoio assistivo autorizado.	Usuário, Coordenação, NDE e fornecedor.	Usuário confirma acesso efetivo.
Suspeita de vazamento ou ataque	Crítica	TI/Privacidade	Conter, preservar evidências, bloquear acessos comprometidos.	Canal seguro alternativo; continuidade apenas após avaliação.	Autoridade competente e públicos definidos pelo plano de incidentes.	Validação de segurança e relatório pós-incidente.
Repositório institucional indisponível	Média	TI/Biblioteca	Confirmar escopo e preservar depósitos.	Suspender novos depósitos e manter arquivos em área institucional autorizada.	Autores e setores afetados.	Integridade, acesso e fila de depósitos validados.
Ausência do bibliotecário	Média	Biblioteca/Direção	Ativar cobertura e registrar demandas técnicas.	Equipe treinada presta orientação inicial e agenda retorno.	Usuários e Coordenações quando necessário.	Demandas respondidas e cobertura registrada.
Interdição do espaço físico	Alta	Direção/Infraestrutura	Isolar área e proteger pessoas.	Acesso remoto; remanejamento para Laboratório de Informática ou sala adequada.	Comunidade acadêmica.	Liberação formal e inspeção do ambiente.
Emergência física	Crítica	Segurança/Infraestrutura	Evacuar e acionar serviços de emergência conforme protocolo.	Suspender atendimento presencial; manter apenas serviços remotos seguros.	Pessoas no campus e gestão.	Liberação da autoridade competente e relatório.

ANEXO II

CRITÉRIOS DE CRITICIDADE E ESCALONAMENTO

NÍVEL	CRITÉRIO	ACIONAMENTO	ATUALIZAÇÃO
Baixa	Impacto pontual, alternativa imediata, sem risco relevante.	Responsável operacional.	No encerramento.
Média	Serviço degradado ou grupo limitado afetado.	Biblioteca e área técnica.	Quando houver mudança relevante.
Alta	Múltiplos usuários, atividade próxima ou alternativa insuficiente.	Gestores das áreas e Direção Acadêmica.	Periódica até recuperação.
Crítica	Segurança, dados, indisponibilidade ampla ou impacto regulatório imediato.	Direção-Geral e governanças de crise.	Contínua, conforme plano institucional.

ANEXO III

MENSAGENS INSTITUCIONAIS DE CONTINGÊNCIA

SITUAÇÃO	TEXTO-BASE
Indisponibilidade inicial	A Biblioteca Digital apresenta indisponibilidade no momento. As equipes responsáveis já foram acionadas. Enquanto o acesso é restabelecido, utilize as orientações acadêmicas divulgadas pela Coordenação e acompanhe os canais oficiais para a próxima atualização.
Acesso alternativo	O acesso principal permanece indisponível. Foi disponibilizada alternativa institucional temporária para as atividades afetadas, conforme orientação do docente ou da Coordenação. Não compartilhe credenciais nem utilize cópias não autorizadas.
Restabelecimento	O acesso à Biblioteca Digital foi restabelecido e validado. Caso ainda encontre dificuldade, registre a ocorrência no canal de suporte da Biblioteca, informando curso, dispositivo, horário e mensagem apresentada.
Barreira de acessibilidade	A Biblioteca recebeu a comunicação de barreira de acessibilidade e acionou o NAI/NAPS, a Coordenação e o fornecedor. Será oferecida alternativa acadêmica acessível, preservados o conteúdo e os resultados de aprendizagem.

ANEXO IV

REPOSITÓRIO MÍNIMO DE EVIDÊNCIAS

EVIDÊNCIA	CONTEÚDO	RESPONSÁVEL PRIMÁRIO
Registro do incidente	Data, impacto, nível, origem, ações, comunicação e encerramento.	Biblioteca
Chamado técnico	Diagnóstico, atendimento, fornecedor, tempos e solução.	TI
Impacto acadêmico	Cursos, UCs, turmas, prazos e alternativas.	Coordenação
Decisão bibliográfica	Análise, ata do NDE, matriz e atualização documental.	NDE/Biblioteca
Acessibilidade	Barreira, recurso, alternativa, teste e retorno do usuário.	NAI/NAPS
Comunicação	Mensagens, públicos, canais e horários.	Comunicação/Biblioteca
Análise posterior	Causa, linha do tempo, lições e ações preventivas.	Líder do incidente
Teste do plano	Cenário, participantes, resultado e melhorias.	Biblioteca/TI

ANEXO V

REFERÊNCIAS NORMATIVAS ESSENCIAIS

- I. Constituição da República Federativa do Brasil de 1988.
- II. Lei nº 9.394, de 20 de dezembro de 1996 – Lei de Diretrizes e Bases da Educação Nacional.
- III. Lei nº 10.861, de 14 de abril de 2004 – Sistema Nacional de Avaliação da Educação Superior.
- IV. Decreto nº 9.235, de 15 de dezembro de 2017, com alterações vigentes.
- V. Lei nº 4.084, de 30 de junho de 1962; Decreto nº 56.725, de 16 de agosto de 1965; e Lei nº 9.674, de 25 de junho de 1998
- VI. profissão de bibliotecário.
- VII. Lei nº 9.610, de 19 de fevereiro de 1998 – direitos autorais.
- VIII. Lei nº 13.146, de 6 de julho de 2015 – Lei Brasileira de Inclusão da Pessoa com Deficiência.
- IX. Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais.
- X. Resolução CFB nº 207/2018 – Código de Ética e Deontologia do Bibliotecário brasileiro.
- XI. Resolução CFB nº 184/2017 – identificação profissional em trabalhos biblioteconômicos.
- XII. Instrumentos de Avaliação de Cursos de Graduação e de Instituições de Educação Superior do Inep vigentes para o ato avaliativo.
- XIII. PDI 2026–2030, Regimento Geral, PPCs e demais normas da Faculdade ARIA.